YAYASAN PRIMA AGUS TEKNIK

Hukum di Era Globalisasi Digital

Dr. Agus Wibowo, M.Kom, M.Si, MM

Hukum di Era Globalisasi Digital

Penulis :
Dr. Agus Wibowo, M.Kom., M.Si., MM.

ISBN : 9 786238 120727

Editor :
Dr. Joseph Teguh Santoso, S.Kom., M.Kom.

Penyunting :
Dr. Mars Caroline Wibowo. S.T., M.Mm.Tech

Desain Sampul dan Tata Letak :
Irdha Yunianto, S.Ds., M.Kom.

Penebit :
Yayasan Prima Agus Teknik Bekerja sama dengan
Universitas Sains & Teknologi Komputer (Universitas STEKOM)

Redaksi :
Jl. Majapahit no 605 Semarang
Telp. (024) 6723456
Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

Distributor Tunggal :
Universitas STEKOM
Jl. Majapahit no 605 Semarang
Telp. (024) 6723456
Fax. 024-6710144
Email : info@stekom.ac.id

KATA PENGANTAR

Puji syukur kehadirat Tuhan Yang Maha Esa atas anugerah dan pertolongan-Nya sehingga penulis dapat menyelesaikan buku yang berjudul "***Hukum di Era Globalisasi Digital***". Buku ini dibuat bertujuan untuk menjadi bahan referensi dan sebagai buku bahan ajar, buku ini dibuat secara semaksimal dan sebaik mungkin agar menjadi manfaat bagi pembaca yang membutuhkan informasi dan pengetahuan mengenai bagaimana Hukum Digital Global.

Istilah "Hukum Digital" merujuk pada serangkaian hukum dan regulasi yang mengatur perilaku dan transaksi di dunia digital yang melibatkan teknologi informasi, internet, dan segala bentuk komunikasi elektronik. Ini mencakup bidang hukum yang berkaitan dengan keamanan siber, privasi data, hak kekayaan intelektual, bisnis elektronik, dan isu-isu hukum lainnya yang berkaitan dengan dunia digital.

Hukum Digital mencerminkan kenyataan bahwa banyak aktivitas manusia, baik itu dalam konteks bisnis, hiburan, atau komunikasi, semakin terhubung dengan teknologi digital dan internet. Karena itu, regulasi ini perlu bersifat lintas batas dan global untuk mengatasi tantangan dan masalah yang muncul di dunia digital yang terus berkembang. Perkembangan dan perubahan hukum ini dapat bervariasi tergantung pada negara atau wilayah, tetapi juga ada upaya untuk mencapai kesepakatan dan standar global dalam beberapa aspek.

Hukum Digital memiliki manfaat signifikan dalam konteks globalisasi dan perkembangan teknologi digital. Keberadaannya membantu menciptakan kerangka kerja hukum yang konsisten dan terkoordinasi di seluruh dunia untuk mengatasi tantangan yang timbul dari penggunaan teknologi informasi dan internet. Manfaatnya melibatkan perlindungan hak individu terkait privasi data dan keamanan siber, memberikan kerangka kerja yang jelas untuk bisnis dan e-commerce lintas batas, serta mendukung penegakan hak kekayaan intelektual secara global.

Dalam buku ini telah mengukir beberapa ciri khusus dari hukum digital. Pertama, hukum digitalitas, khususnya pada skala global lintas batas, sebagian besar merupakan produk dari tatanan privat, yaitu penetapan aturan oleh pihak swasta terutama dalam lingkungan privat di mana ketentuan layanan adalah prima facie "hukum negara". Karakteristik kedua yang terkait erat dengan hukum digitalitas global adalah bahwa hukum ini, sebagian besar, distandarisasi di seluruh yurisdiksi, berdasarkan syarat dan ketentuan standar, dan ditegakkan secara transnasional melalui kode etik.

Buku ini terbagi menjadi 10 bab yang dan terbagi menjadi 5 bagian. Bagian 1 mencakup 2 bab yang akan membahas tentang hak intelektual dan dasar hukum digitalisasi global. Bagian 2 juga terbagi menjadi 2 bab yang akan membahas tentang tata perlindungan privasi data, bagian ke 3 buku ini akan membahas hukum kontrak konsumen. Bagian 4 melanjutkan pembahasan di bagian sebelumnya, akan menerangkan tentang hukum media digital sebagai media publikasi dan promosi. Bagian terakhir buku ini akan menerangkan tentang hukum dan sanksi tindak kejahatan dalam pengunaan data, akhir kata semoga buku ini berguna bagi para pebaca.

Semarang, Desember 2023

Penulis

Dr. Agus Wibowo, M.Kom, M.Si, MM

DAFTAR ISI

Bagian I
Hak Milik Intelektual

BAB I
MENUJU METODOLOGI HUKUM DIGITALISASI

1.1 PENDAHULUAN

Teknologi digital telah membentuk dan terus membentuk dunia. Kehidupan ekonomi, sosial, politik, dan budaya kita bergantung pada cara kita mengatur teknologi-teknologi ini. Digitalisasi juga menantang gagasan dasar kita tentang hukum. Dalam kontribusi ini, kami akan mengkaji bagaimana teknologi digital telah mempengaruhi konstruksi hukum dan kami akan menguraikan kerangka metodologi digitalisasi hukum. Dalam konteks ini *"metodologi"* akan ditafsirkan secara luas dan pragmatis dengan mengacu pada prosedur dan praktik yang digunakan oleh regulator internasional, regional dan nasional, pengadilan dan badan pengambil keputusan lainnya serta aktor hukum swasta seperti pemegang hak dan pengguna informasi yang dilindungi. dalam adopsi, penerapan dan tata kelola aturan hukum informasi.

Tidak diragukan lagi, digitalisasi berdampak pada seluruh bidang hukum dan menantang norma-norma mendasar, asumsi, praktik, dll., antara lain dalam hukum kontrak, hukum administrasi, hukum kesehatan, hukum maritim, hukum konstruksi, dan hukum persaingan. Namun, untuk tujuan proyek menguraikan metodologi hukum digitalisasi, kami berasumsi bahwa tantangan digitalisasi pertama kali muncul dalam undang-undang informasi dan khususnya dalam undang-undang hak cipta. Oleh karena itu, sebagian besar contoh cara mengatasi digitalisasi secara hukum terdapat dalam bidang hukum ini dan dengan demikian memberikan kasus yang paling jelas dalam menilai konsekuensi dari pilihan hukum. Proposisi proyek ini adalah bahwa dengan mempelajari dampak digitalisasi dalam bidang hukum hak cipta, kita dapat menyimpulkan dan mengidentifikasi perubahan metodologi yang mempunyai arti umum.

1.2 CIRI-CIRI HUKUM HAK CIPTA

Hak Cipta adalah kerangka hukum yang melindungi karya kreatif dan intelektual dari penggunaan atau reproduksi tanpa izin. Berikut beberapa ciri umum hukum hak cipta:

1. **Perlindungan terhadap karya asli:** Undang-undang hak cipta memberikan perlindungan otomatis terhadap karya asli yang dinyatakan dalam bentuk nyata. Ini mencakup berbagai karya seperti menulis, musik, seni visual, film dan program komputer.
2. **Hak Milik yang Eksklusif:** Pemegang hak cipta memiliki hak eksklusif untuk mengontrol penggunaan, reproduksi, distribusi, dan pemanfaatan karya ciptanya. Hak ini memberikan kendali penuh kepada pemilik hak cipta atas karya-karya mereka.

3. **Sifat Otomatis dan Langsung:** Hukum hak cipta memberikan perlindungan otomatis sejak karya tersebut diwujudkan dalam bentuk konkret. Pemilik hak cipta tidak perlu mendaftarkan karyanya untuk mendapatkan perlindungan, meskipun pendaftaran dapat memberikan keuntungan tertentu dalam penanganan pelanggaran.
4. **Jangka waktu perlindungan terbatas:** Perlindungan hak cipta tidak bersifat abadi. Setelah jangka waktu tertentu (biasanya seumur hidup pemiliknya dan beberapa tahun lagi), karya tersebut masuk ke dalam domain publik, yaitu. itu tersedia secara gratis untuk semua orang.
5. **Perlindungan internasional:** Sebagian besar negara memiliki sistem hak ciptanya sendiri, namun ada juga perjanjian internasional, seperti Konvensi Berne, yang memberikan perlindungan otomatis di beberapa negara tanpa perlu mendaftarkan ciptaan di setiap negara.
6. **Karya Pilihan:** Undang-undang hak cipta tidak melindungi gagasan atau konsep umum. Hanya ekspresi spesifik dari pemikiran tersebut yang dilindungi. Misalnya, ide sebuah cerita tidak dilindungi, namun penulisan naskah yang mengungkapkan cerita tersebut.
7. **Pengecualian dan penggunaan wajar:** Undang-undang hak cipta juga memuat beberapa pengecualian, seperti penggunaan wajar, yang mengizinkan penggunaan tanpa izin atas suatu ciptaan dalam konteks tertentu, seperti penelitian, pendidikan, dan kritik.
8. **Hak moral dan ekonomi:** hak cipta mencakup hak moral (misalnya hak untuk diakui sebagai pencipta) dan hak milik (misalnya hak untuk menentukan cara penggunaan karya tersebut dan hak untuk memperoleh keuntungan dari penggunaan karya tersebut).
9. **Jawaban Hak Cipta:** Meskipun memperoleh perlindungan hak cipta tidak wajib, namun mengajukan pemberitahuan hak cipta atas suatu karya dapat memberikan informasi penting tentang hak pemilik hak cipta.
10. **Perlindungan Karya Asing:** Undang-undang hak cipta seringkali melindungi karya asing berdasarkan prinsip perlakuan nasional, dimana karya asing diperlakukan sama dengan karya dalam negeri.

Penting untuk dicatat bahwa undang-undang hak cipta mungkin berbeda dari satu negara ke negara lain dan informasi tertentu mungkin berbeda dari satu negara ke negara lain. Selain itu, perkembangan teknologi digital membawa tantangan baru dalam penerapan dan penegakan hukum hak cipta.

Hak kekayaan intelektual (HAKI) memberikan hak eksklusif atas informasi seperti karya asli atau database yang mewakili investasi besar, atau penemuan untuk merangsang kreativitas dan inovasi. HKI mendapat perlindungan seperti jenis hak milik lainnya menurut Piagam Hak Fundamental Uni Eropa (CFREU), Art. Perundang-undangan didasarkan pada keseimbangan kepentingan antara pencipta informasi dan pengguna, dan meskipun eksklusivitas memungkinkan pemegang hak untuk menentukan harga produk atau proses yang memasukkan elemen yang dilindungi di atas biaya marjinal, biaya sosial diharapkan dapat diimbangi dengan peningkatan pendapatan. kesejahteraan konsumen secara keseluruhan.

Hak atas informasi merupakan makhluk hukum perundang-undangan. Sebagai "pulau eksklusivitas di lautan kebebasan", HKI biasanya didasarkan pada hukum positif (konvensi internasional, peraturan regional (UE), dan undang-undang nasional). Ini juga merupakan daya tarik dari CFREU Art: *"Setiap pembatasan terhadap pelaksanaan hak dan kebebasan yang diakui oleh Piagam ini harus diatur oleh hukum"* dan *"tunduk pada prinsip proporsionalitas".*

Meskipun kerja sama hukum internasional di bidang HKI sudah ada sejak Konvensi Paris dan Berne pada tahun 1880-an, undang-undang tersebut telah berkembang secara nasional atau teritorial. "Dasar undang-undang" secara tradisional diterjemahkan ke dalam undang-undang nasional. Bagi Negara-negara Anggota UE, harmonisasi HKI melalui aturan-aturan umum telah mencapai kemajuan besar sejak Petunjuk pertama mengenai perlindungan program komputer diadopsi pada tahun 1991. Saat ini, lebih dari 20 arahan dan peraturan telah dikeluarkan di bidang hak cipta, merek dagang, desain dan paten. Ditambah lagi dengan sejumlah besar keputusan yang diambil oleh Pengadilan Kehakiman Uni Eropa (CJEU) berdasarkan arahan dan peraturan tersebut, dan menjadi jelas bahwa ruang untuk pembuatan peraturan "nasional" sangat dibatasi jika dibandingkan dengan peraturan tradisional. titik awal dari negara nasional yang berdiri sendiri. Selain itu, batasan-batasan penting mengenai ruang gerak bagi pengadilan nasional dan pembuat undang-undang juga mengikuti prinsip-prinsip umum yang dikembangkan oleh CJEU, seperti prinsip-prinsip efisiensi atau proporsionalitas. Namun, meskipun harmonisasi UE telah mengubah perspektif dari "nasional" dan "internasional" menjadi "regional", HKI pada dasarnya masih terbatas pada wilayah masing-masing negara, penegakan hukum sebagian besar masih bersifat nasional dan undang-undang nasional menjadi latar belakang penerapannya. solusi bersama kecuali harmonisasi UE telah terjadi.

1.3 DIGITALISASI PERUNDANG-UNDANGAN

Digitalisasi perundang-undangan mengacu pada penggunaan teknologi digital untuk menyusun, menyimpan, mempublikasikan, dan mengelola undang-undang, peraturan, dan dokumen hukum lainnya. Digitalisasi ini mencakup transformasi dari format tradisional (kertas) ke format digital, memungkinkan akses yang lebih mudah, pencarian yang efisien, dan penyebaran informasi hukum yang lebih cepat. Berikut adalah beberapa aspek digitalisasi perundang-undangan:

1. **Penyusunan dan Pembuatan Hukum:** Dokumen hukum, termasuk undang-undang dan peraturan, dapat disusun dan dibuat menggunakan perangkat lunak khusus. Proses ini mencakup penerapan teknologi untuk mempermudah penulisan, penyusunan, dan peninjauan dokumen hukum.
2. **Penyimpanan Elektronik:** Alih-alih menyimpan dokumen hukum dalam bentuk fisik, digitalisasi memungkinkan penyimpanan elektronik. Ini dapat dilakukan melalui sistem manajemen dokumen atau basis data yang memfasilitasi penyimpanan, pencarian, dan manajemen dokumen secara efisien.

3. **Akses Publik Online:** Digitalisasi memungkinkan publik untuk mengakses undang-undang dan peraturan secara online. Banyak pemerintah telah membangun portal atau situs web resmi yang menyediakan akses mudah ke dokumen hukum.
4. **Pencarian dan Indeksasi:** Sistem pencarian elektronik memungkinkan pencarian cepat dan efisien terhadap teks undang-undang dan peraturan. Indeksasi yang baik mempermudah penemuan informasi hukum yang relevan.
5. **Pembaharuan Otomatis:** Dengan digitalisasi, pembaruan undang-undang dan peraturan dapat dilakukan secara otomatis. Hal ini mengurangi risiko penggunaan informasi hukum yang sudah usang atau tidak akurat.
6. **Kolaborasi dan Konsultasi Publik:** Digitalisasi memfasilitasi proses kolaborasi dalam penyusunan undang-undang dan memungkinkan konsultasi publik yang lebih luas melalui platform online. Pemerintah dapat menerima masukan dari masyarakat sebelum dan selama proses penyusunan undang-undang.
7. **Interoperabilitas Data:** Sistem digital memungkinkan interoperabilitas data antara dokumen hukum dan sistem lainnya. Ini dapat mendukung integrasi data hukum dengan sistem lain seperti basis data kependudukan atau keuangan.
8. **Analisis dan Statistik:** Data hukum dapat dianalisis dengan lebih mudah menggunakan alat analisis data. Ini dapat membantu pemahaman tren hukum, evaluasi kebijakan, dan pembuatan keputusan yang lebih baik.
9. **Keamanan dan Keabsahan:** Sistem digital harus memperhatikan keamanan data dan keabsahan dokumen hukum. Sistem keamanan yang kuat dan tanda tangan digital dapat membantu memastikan integritas dan otentisitas informasi hukum.
10. **Pelaporan dan Transparansi:** Digitalisasi memungkinkan pelaporan yang lebih efisien dan transparansi dalam penggunaan dan implementasi undang-undang. Pemerintah dapat dengan mudah menyajikan informasi kepada publik dan pemangku kepentingan.

Digitalisasi perundang-undangan membawa banyak manfaat dalam meningkatkan aksesibilitas, efisiensi, dan transparansi dalam pengelolaan informasi hukum. Meskipun demikian, perlu juga memperhatikan tantangan terkait keamanan, perlindungan data, dan aksesibilitas bagi semua lapisan masyarakat.

Dimulai pada awal tahun 1990an, UE telah secara aktif membuat undang-undang di bidang HKI dan khususnya di bidang hak cipta. Selama 30 tahun pembuatan undang-undang ini, peraturan khusus mengenai jenis pekerjaan baru yang sebagian besar bersifat digital (program komputer dan database) telah ditambahkan, atau penggunaan baru yang muncul dengan teknologi digital atau telah berubah secara radikal akibat teknologi digital (internet, satelit dan kabel) atau modalitas eksploitasi hak yang dimungkinkan oleh internet (lisensi online dan portabilitas) telah ditangani. Tidak ada arahan yang dicabut, namun lapisan baru telah ditambahkan.

Salah satu tantangan paling penting bagi pembuat undang-undang adalah bagaimana membuat undang-undang yang tahan di masa depan sehingga dapat beradaptasi dengan perubahan yang akan datang. Hal ini pada dasarnya merupakan tugas yang rumit, karena perkembangan teknologi merupakan proses yang dinamis, yang berarti bahwa

kemungkinan-kemungkinan teknologi terus menerus memberikan kemungkinan-kemungkinan dan tantangan-tantangan baru. Ketegangan antara regulasi statis dan teknologi dinamis bersifat sistemik dan tidak dapat dihindari. Bagi undang-undang UE, permasalahan ini diperburuk oleh fakta bahwa undang-undang UE terkenal sulit untuk diubah. Agar arahan atau peraturan dapat diubah dan undang-undang baru dapat diberlakukan, sebagian besar dari 27 Negara Anggota UE harus menyetujuinya.

Namun, kadang-kadang, inisiatif legislatif besar dilakukan di tingkat UE. Salah satu hal yang paling spektakuler tentu saja adalah meningkatnya perlindungan data pribadi yang mencapai puncaknya dengan diadopsinya Peraturan Perlindungan Data Umum (GDPR) pada tahun 2016. GDPR juga mempertimbangkan perkembangan kasus hukum. Yang terpenting, "hak untuk dilupakan" dikembangkan oleh CJEU di Google Spanyol berdasarkan ketentuan dalam Piagam. Prinsip-prinsip ini kini diatur secara eksplisit dalam Pasal GDPR. ("hak untuk menghapus") di mana hak tersebut semakin diperkuat mengingat adanya tantangan khusus di lingkungan online (poin 65). Dengan cara ini, mungkin ada putaran umpan balik (feedback loops) antara peraturan perundang-undangan dan praktik peradilan. Namun sering kali, "perubahan" tidak ditransformasikan ke dalam ketentuan hukum, namun harus diekstrapolasi dari kasus hukum. Oleh karena itu, banyak hal yang bergantung pada kemampuan undang-undang untuk memberikan panduan bagi pengembangan kasus hukum dari CJEU dan pengadilan nasional dan pada saat yang sama memberikan fleksibilitas.

Regulasi Sui Generis atau Adaptasi Aturan yang Ada?

Salah satu tantangan paling mendasar bagi legislator akibat digitalisasi adalah bagaimana melindungi jenis kreasi digital baru apakah akan membuat sistem baru atau memasukkan jenis baru ke dalam sistem yang sudah ada. Perlindungan hukum kekayaan intelektual terhadap program komputer dan basis data merupakan dua contoh utama dari kesulitan-kesulitan ini.

Awalnya, kecenderungannya adalah untuk menggunakan sistem perlindungan jenis baru. Untuk program komputer, WIPO mengusulkan Model Ketentuan tentang Perlindungan Perangkat Lunak Komputer pada tahun 1978. Untuk database, arahan Uni Eropa pada tahun 1996 mengilhami perkembangan serupa. Usulan mengenai program komputer tidak mendapat perhatian internasional, dan pada tahun 1980-an undang-undang hak cipta menjadi model yang disukai. Namun pada akhirnya, diputuskan untuk mengatasi tantangan digitalisasi hak cipta dalam satu instrumen hukum, yaitu. Perjanjian Hak Cipta WIPO (WCT) pada tahun 1996. WCT mewajibkan negara-negara untuk memberikan perlindungan terhadap program komputer dan basis data, terhadap "penyediaan" materi yang dilindungi di internet, dan terhadap langkah-langkah perlindungan teknologi (TPM) dan pengelolaan hak digital (DRM). Juga diperjelas bahwa perlindungan hak cipta mencakup ekspresi dan bukan ide, prosedur, metode operasi, atau konsep matematika. Demikian pula, Perjanjian TRIPS mengatur sistem hak cipta yang komprehensif untuk perlindungan program komputer dan database.

Di tingkat UE, pendekatan terhadap digitalisasi lebih bersifat ad hoc, sehingga menghasilkan gambaran hukum yang terfragmentasi. Berbeda dengan model WCT, UE (saat

ini) mengeluarkan Petunjuk tentang perlindungan hukum program komputer pada tahun 1991 dan Petunjuk tentang perlindungan hukum database pada tahun 1996.

Arahan ini menggambarkan kesulitan pembuatan peraturan sui generis. Istilah *"program komputer"* seperti yang digunakan dalam Petunjuk Program Komputer, misalnya, juga mencakup pekerjaan desain persiapan yang mengarah pada pengembangan program komputer dan mencakup kode sumber dan kode objek. Namun, istilah ini tidak mencakup antarmuka pengguna grafis, yang tidak dapat dilindungi secara khusus oleh hak cipta dalam program komputer. Namun, antarmuka pengguna dapat dilindungi secara terpisah tergantung pada kontennya (gambar atau teks) sesuai dengan aturan yang tidak diselaraskan dalam hak cipta umum. Dalam dengan cara ini, meskipun Petunjuk ini dimaksudkan untuk melindungi *"program komputer"* secara khusus, namun Petunjuk ini tidak memberikan perlindungan penuh untuk program komputer.

Lebih jauh lagi, meskipun Petunjuk Basis Data dan Petunjuk Program Komputer terbatas pada pokok bahasannya saja, keduanya jelas harus menangani beberapa permasalahan dasar yang sama seperti objek perlindungan atau kelelahan. Oleh karena itu, mengenai isi ketentuan substantif, norma-norma dasarnya diharapkan serupa. Namun, terdapat perbedaan penting dan tidak dapat dijelaskan. Misalnya, mengapa Petunjuk Basis Data tidak memuat batasan yang terdapat dalam Petunjuk Program Komputer Seni (dan di WCT) untuk "gagasan dan prinsip"? Haruskah pengadilan melakukan analisis horizontal dan menerapkan pembatasan terhadap basis data dengan analogi? Atau haruskah pengadilan mengandalkan prinsip analisis e contrario? Dalam praktiknya, CJEU mengandalkan WCT dan TRIPS (lihat nanti) untuk menafsirkan Petunjuk Program Komputer, dan dengan cara ini kerangka hukum internasional telah memberikan pelipur lara bagi sistem UE yang terfragmentasi. Namun, seperti yang akan terlihat nanti, sehubungan dengan kelelahan, kurangnya koordinasi antara arahan UE terus menimbulkan masalah.

Perlindungan hukum terhadap program komputer juga menimbulkan kesulitan dalam hukum paten. Konvensi Paten Eropa (EPC) Pasal. Pasal 52 menyatakan bahwa program komputer bukan merupakan penemuan dan oleh karena itu tidak dapat dilindungi berdasarkan Konvensi. Memahami batasan ini, dan khususnya menemukan garis tipis antara *"program komputer"* yang dapat dipatenkan dan program komputer yang tidak dapat dipatenkan, terbukti merupakan hal yang paling sulit dalam praktiknya. Untuk menyelesaikan masalah ini diusulkan untuk mengubah EPC dan mencabut batasan program komputer. Hal ini bukan bertujuan untuk memperluas pokok bahasan yang dapat dipatenkan tetapi untuk mencerminkan perkembangan praktik Dewan Banding EPO yang mengandalkan prinsip-prinsip umum EPC daripada batasan khusus untuk menyaring program komputer yang tidak memiliki hak paten. dampak teknis dari Konvensi ini. Dengan demikian, hasil dari proposal ini akan bergantung pada prinsip-prinsip umum dan bukan pada batasan khusus. Proposal tersebut gagal dan aturan khusus dipatuhi.

Setelah revisi EPC, UE mengusulkan Petunjuk Parlemen dan Dewan Eropa mengenai hak paten atas penemuan yang diimplementasikan dengan komputer. Usulan tersebut berisi peraturan yang sangat rinci mengenai pokok bahasan, syarat-syarat untuk dapat dipatenkan, bentuk-bentuk hak paten, dan bentuk-bentuk hak paten. klaim dan menginstruksikan

Negara-negara Anggota untuk menerapkan ketentuan-ketentuan tersebut melalui undang-undang paten nasional mereka yang sebagian besar tidak diselaraskan. Arahan ini juga pada akhirnya menemui jalan buntu. Untungnya menurut kami demikian. Gagasan untuk mengatur aspek spesifik dan kontroversial dari undang-undang paten melalui ketentuan-ketentuan yang terperinci, dan untuk melakukan hal tersebut lebih lanjut dalam permasalahan kelembagaan yang sudah rumit antara EPC, UE, dan negara-negara nasional pasti akan gagal. Namun, "naluri" dasar para legislator UE untuk menghadapi tantangan digitalisasi melalui peraturan yang spesifik dan terperinci mencerminkan perkembangan hak cipta yang dijelaskan sebelumnya.

Fleksibilitas Perancangan

Petunjuk InfoSoc mulai berlaku pada bulan Juni 2001. Proses yang mengarah pada Petunjuk ini dimulai pada tahun 1990-an dan kemudian menghasilkan usulan pertama dari Komisi pada tahun 1997. Pada saat itulah internet berubah dari yang kurang dikenal. jaringan komputer yang digunakan oleh akademisi, dengan aktor komersial memasuki lokasi. Google didirikan pada tahun 1998 dan Facebook pada tahun 2004. Dengan cara ini, sebagian besar praktik yang kita kaitkan dengan Masyarakat Informasi dan yang menjadi tujuan dari Pedoman ini, tidak benar-benar ada pada saat pedoman tersebut ditetapkan. Petunjuk tersebut dirumuskan.

Meskipun Petunjuk InfoSoc muncul terlalu dini bagi para perumus untuk mengetahui banyak tentang teknologi dan cara-cara komunikasi dan bisnis yang menentukan banyak permasalahan hukum yang harus diselesaikan oleh Petunjuk tersebut, jelas bahwa para perumus sangat tertarik dengan hal ini. sangat sadar bahwa ada sesuatu yang sedang terjadi dan bahwa Petunjuk ini sedang dikembangkan pada periode transformatif untuk penggunaan materi yang dilindungi hak cipta. Dengan demikian, bersamaan dengan menjadi jelas bahwa aturan-aturan dasar yang telah ditetapkan dalam arahan sebelumnya akan tetap berlaku, disebutkan juga bahwa Ketidakpastian hukum mengenai sifat dan tingkat perlindungan perbuatan transmisi berdasarkan permintaan atas karya hak cipta dan materi pokok yang dilindungi oleh hak terkait melalui jaringan harus diatasi dengan memberikan perlindungan yang harmonis di tingkat Komunitas. Harus dijelaskan bahwa semua pemegang hak yang diakui oleh Petunjuk ini harus mempunyai hak eksklusif untuk menyediakan karya hak cipta atau materi pokok lainnya kepada publik melalui transmisi interaktif berdasarkan permintaan.

Ketika dibaca bersamaan dengan pembacaan 20, tampak jelas bahwa para perumus Petunjuk ini menyerukan penerapan alat-alat tradisional secara luas. Dalam menghadapi ketidakpastian hukum mengenai perkembangan teknologi dan hukum, maka hak harus dimaknai secara luas. Hal ini juga merupakan inti dari pernyataan pada bacaan 4: Kerangka hukum yang selaras mengenai hak cipta dan hak-hak terkait, melalui peningkatan kepastian hukum dan sekaligus memberikan perlindungan tingkat tinggi terhadap kekayaan intelektual, akan mendorong investasi besar dalam kreativitas dan inovasi, termasuk infrastruktur jaringan, dan pada gilirannya akan mengarah pada pertumbuhan dan peningkatan hak cipta. daya saing industri Eropa, baik dalam bidang penyediaan konten dan teknologi informasi dan secara umum di berbagai sektor industri dan budaya. Hal ini akan

menjaga lapangan kerja dan mendorong penciptaan lapangan kerja baru. Dilihat dari sudut pandang pemegang hak, interpretasi yang luas terhadap aturan eksklusivitas dengan tujuan untuk memberikan perlindungan tingkat tinggi harus diterapkan.

Dilihat dari sudut pandang pengguna, respons terhadap ketidakpastian ini agak berbeda. Sebagaimana dijelaskan dalam Pasal 32, Petunjuk ini memberikan penjelasan lengkap tentang pengecualian dan pembatasan terhadap hak reproduksi dan hak komunikasi kepada publik. Daftar ini ditemukan di Art. 5(1)—(4). Untuk lebih memperjelas hal ini, Art. 5(5) menyatakan kembali pengujian tiga langkah dan menyatakan bahwa: Pengecualian dan pembatasan yang diatur dalam ayat 1, 2, 3 dan 4 hanya akan diterapkan dalam kasus-kasus khusus tertentu yang tidak bertentangan dengan eksploitasi normal atas ciptaan atau hal lain dan tidak secara tidak wajar mengurangi kepentingan sah dari hak tersebut. pemegang.

Berbeda dengan tes yang dikembangkan dalam Berne Convention Art. 9(2) dan sebagaimana ditemukan dalam TRIPS Art. Petunjuk InfoSoc menggunakan tes sebagai batasan dari batasan dan pengecualian. Efeknya adalah batasan ganda pada batasan dan pengecualian. Batasan penting mengenai ruang gerak bagi pengadilan nasional dan pembuat undang-undang juga mengikuti prinsip-prinsip umum yang dikembangkan oleh CJEU, seperti prinsip-prinsip effet utile atau proporsionalitas. Karena alasan inilah CJEU di Funke Medien menjelaskan bagaimana kebijaksanaan Negara-negara Anggota dalam penerapan pengecualian dan pembatasan yang diatur dalam Arahan InfoSoc harus dilaksanakan dalam batas-batas yang ditentukan oleh hukum UE dan ini berarti bahwa ruang-ruang tersebut tampaknya yang dibiarkan terbuka oleh Petunjuk ini pada kenyataannya sangat dibatasi oleh undang-undang UE. Daftar tertutup mengenai batasan dan pengecualian dalam Petunjuk InfoSoc telah terbukti sangat bermasalah. Yang pertama dan terpenting, daftar ini menjadikan hak cipta tidak fleksibel mengingat adanya perubahan teknologi, dan ketidakmampuan pembatasan dan pengecualian untuk “diperluas” bersamaan dengan eksklusivitas terus-menerus mengabaikan perlindungan demi kepentingan pemegang hak. Untuk mendorong hal yang sama, CJEU dalam beberapa kesempatan telah memperjelas bahwa pembatasan dan pengecualian harus ditafsirkan secara sempit. Secara hukum, strategi pengadilan ini telah membatasi ruang bernapas dari pembatasan dan pengecualian.

Selain itu, dampak dari pembatasan dan pengecualian bergantung pada kemampuan pengguna untuk menggunakan hak pengguna mereka. Dengan cara ini pengguna dan pemegang hak berada dalam kondisi yang sama. Menurut Petunjuk DSM20 Art. 17(7), Negara-negara Anggota harus memastikan bahwa pengguna dapat mengandalkan pengecualian dan batasan. Selain itu, Petunjuk ini “sama sekali tidak akan memengaruhi penggunaan yang sah” dan platform harus memberi tahu pengguna bahwa mereka dapat menggunakan karya di bawah batasan dan pengecualian (Pasal 17(9)). Dengan cara ini, Petunjuk DSM memberikan perlindungan prosedural kepada pengguna. Namun, seperti yang ditunjukkan oleh salah satu dari kami, masih belum jelas bagaimana pengguna harus menegakkan hak-hak mereka berdasarkan Petunjuk tersebut. Yang penting, Petunjuk DSM gagal menentukan konsekuensi hukum dari kegagalan platform dalam memenuhi kewajibannya untuk memastikan pengguna hak. Dengan cara ini pula, sistem hak cipta UE mencerminkan sistem tradisional yang dikenal dalam kerangka kerja internasional dan

khususnya TRIPS, yang selama bertahun-tahun telah meningkatkan penegakan hak-hak pemegang hak namun kurang memperhatikan kepentingan pengguna informasi yang dilindungi. Dengan cara ini, Petunjuk DSM dapat dikritik karena mengambil pandangan sepihak terhadap masalah rendahnya penegakan hak cipta dalam arti bahwa arahan ini bertujuan untuk memperkuat kepentingan pemegang hak namun mengabaikan kepentingan pengguna. Kurangnya perhatian terhadap penegakan hak dan kepentingan pengguna melemahkan dampak pembatasan dan pengecualian.

Penilaian

Jika kita membandingkan pendekatan yang dilakukan legislator UE dengan pendekatan WCT, perbedaannya sangat mencolok. WCT mewakili pendekatan yang komprehensif dan luas terhadap tantangan teknologi. Yang penting, Perjanjian ini, selain memperluas perlindungan, juga menunjukkan bagaimana hak cipta harus memberikan "solusi yang memadai terhadap pertanyaan-pertanyaan yang timbul akibat perkembangan ekonomi, sosial, budaya dan teknologi baru" dan bahwa perhatian harus diberikan untuk mengakui kedua hal tersebut. pentingnya perlindungan hak cipta sebagai insentif bagi karya sastra dan seni" dan untuk menjaga keseimbangan antara hak pencipta dan kepentingan publik yang lebih luas".

Bisa dibilang, UE belum menemukan cara untuk menangani secara legislatif tantangan-tantangan yang timbul dari akuisisi yang ada. Petunjuk DSM yang diadopsi hampir dua dekade setelah Petunjuk InfoSoc dimaksudkan untuk memperbarui perolehan hak cipta UE dan melanjutkan apa yang ditinggalkan InfoSoc. Hal ini juga diadopsi pada masa yang ditandai dengan "Perkembangan teknologi yang pesat [yang] terus mengubah cara kerja dan materi lainnya diciptakan, diproduksi, didistribusikan dan dieksploitasi". Ketika "model bisnis baru dan aktor baru terus bermunculan. Perundang-undangan yang relevan harus mampu menghadapi masa depan agar tidak membatasi perkembangan teknologi" .

Mengikuti tradisi pembuatan undang-undang Uni Eropa di bidang hak cipta, Petunjuk DSM tidak menentang kerangka kerja yang ada. Sebaliknya, peraturan ini mengadaptasi dan melengkapi kerangka kerja hak cipta Uni Eropa yang sudah ada, sambil mempertahankan perlindungan "tingkat tinggi" terhadap hak cipta dan hak-hak terkait. Menariknya, Petunjuk ini mencakup ketentuan-ketentuan penting yang ditujukan untuk pelaksanaan hak cipta baik yang berkaitan dengan pengelolaan kolektif. organisasi dan pemegang hak individu. Bagian 3 terakhir dari Petunjuk ini berisi peraturan baru untuk melindungi pemegang hak individu dalam transaksi kontrak (lihat misalnya Pasal 20 yang mengatur "Mekanisme penyesuaian kontrak" dan Pasal 22 yang mengatur "Hak pencabutan") . Selain itu, Petunjuk ini juga telah mengubah batasan dan pengecualian untuk tujuan khusus kutipan, kritik, ulasan, karikatur, parodi, atau bunga rampai sebagai Hak Pengguna yang tidak dapat dikesampingkan. Aspek-aspek Petunjuk ini mewakili perkembangan penting dan menarik yang menggabungkan aspek hak substantif dan hukum acara. Namun Petunjuk ini tidak banyak membantu meredakan ketegangan yang timbul dari Petunjuk yang mendasarinya.

1.4 MENGADILI DIGITALISASI

Secara umum diakui bahwa CJEU telah memainkan peran penting dalam penyesuaian perolehan undang-undang hak cipta. Sebagaimana terlihat dalam diskusi sebelumnya, hal ini tidak mengherankan. Mengingat kesulitan dalam membuat peraturan baru atau mengubah peraturan yang sudah ada, sebagian besar pengembangan hukum harus berada di tangan Pengadilan. Hal ini sendiri merupakan pengamatan yang penting, dan penanganan pengembangan undang-undang yang dilakukan oleh CJEU merupakan tantangan metodologis yang besar bagi banyak pengadilan nasional, yang juga menimbulkan perdebatan yang lebih luas mengenai legitimasi pengembangan undang-undang UE.

CJEU telah berperan penting dalam mengembangkan undang-undang informasi dalam berbagai cara. Berkenaan dengan hak cipta, Pengadilan ini kurang lebih telah mengembangkan prinsip umum orisinalitas di seluruh Uni Eropa, mendefinisikan ulang hak distribusi dan komunikasi, prinsip kepemilikan hak cipta, dan menafsirkan aturan pembatasan dan pengecualian dalam hak cipta sedemikian rupa sehingga hanya memberikan sedikit ruang bagi variasi nasional. Namun berikut ini, kami fokus pada dua contoh saja: kelelahan online dan hyperlink. Hal ini secara intrinsik terkait dengan digitalisasi namun melibatkan beberapa konsep tradisional hak cipta, yang tidak dirancang berdasarkan arahan UE untuk menghadapi tantangan modern namun solusinya harus ditemukan oleh CJEU, yang dalam kedua kasus tersebut harus "membungkuk untuk memasukkan pasak persegi ke dalam lubang heksagonal.

Kelelahan Online

Asas exhaustion mengatur hubungan antara pemegang hak kekayaan intelektual suatu produk dengan pembeli produk tersebut. Berdasarkan prinsip tersebut, sebagaimana telah dikembangkan dalam undang-undang UE, setelah suatu produk dipasarkan di EEA oleh pemegang hak atau dengan persetujuannya, pemegang hak kehilangan "hak distribusi" dan tidak dapat mengendalikan (melalui HKI) penjualan kembali produk tersebut lebih lanjut; "penjualan (legal) pertama" menghabiskan (sebagian) hak kekayaan intelektual.

Awalnya, prinsip exhaustion dikembangkan di Jerman sekitar tahun 1931 untuk mencegah penegakan hukum atas praktik-praktik penyalahgunaan melalui HKI seperti pemeliharaan harga jual kembali dalam penjualan barang-barang yang dilindungi merek dagang. Belakangan, prinsip ini berfungsi sebagai pembatasan dalam hukum yang bersifat umum. hak distribusi. Dengan cara ini, hasilnya menjadi "paket" undang-undang yang terdiri dari hak eksklusivitas yang luas dan pembatasan yang sesuai. Hak distribusi dan prinsip keletihan dipahami untuk bekerja secara bersamaan dan sebagaimana ditentukan oleh undang-undang Kekayaan Intelektual dan bukan berdasarkan "kehendak para pihak" (kontrak).

Yang penting, mengikuti model legislatif ini, baik eksklusivitas maupun pembatasan adalah hukum undang-undang. Oleh karena itu, tidak terbuka bagi partai untuk mengontrak prinsip tersebut. Dengan kata lain, undang-undang memberikan hak kepada pemegang hak untuk memilih apakah akan memasarkan produknya atau tidak. Setelah keputusan tersebut dibuat, dampak hukum dari pemasaran pada dasarnya telah ditentukan sebelumnya oleh undang-undang dan pembeli produk mempunyai hak berdasarkan hukum untuk menjual

kembali produk tersebut. Dilihat dari perspektif UE, prinsip ini dikembangkan oleh CJEU dalam serangkaian keputusan pada tahun 1970an berdasarkan aturan pergerakan bebas barang dalam Perjanjian EC, dan dengan demikian prinsip tersebut bersifat instrumen. tal dalam mengamankan impor paralel barang-barang yang dilindungi hak kekayaan intelektual antar negara-negara Komisi Eropa (kemudian menjadi EEA). Sejak saat itu, hal ini telah dimasukkan ke dalam undang-undang UE melalui arahan dan batasan, dan sebuah prinsip umum kini ada baik dalam undang-undang hak cipta, desain, dan merek dagang berdasarkan model Jerman dan didorong oleh tujuan utama mengamankan pasar internal.

Pada saat prinsip kelelahan pertama kali dikembangkan dalam hukum Jerman dan diterapkan oleh CJEU dalam kasus-kasus mengenai impor paralel, tidak ada keraguan bahwa prinsip tersebut berkaitan dengan distribusi salinan fisik karya: buku, film, barang bermerek, obat-obatan dll. Ketika ditanya pada tahun 2011 di UsedSoft apakah prinsip kelelahan diterapkan pada program komputer dalam bentuk digital, maka tidak mengherankan jika CJEU dalam penilaiannya pertama-tama menyatakan kembali dasar hukum hak cipta internasional (yaitu WCT), yaitu istilah “salinan” dan “asli serta salinan” yang termasuk dalam hak distribusi dan hak sewa berdasarkan Pasal-pasal tersebut, merujuk secara khusus pada salinan tetap yang dapat diedarkan sebagai benda berwujud.

Referensi pada “salinan tetap” jelas menunjukkan kelelahan dalam bidang transaksi salinan fisik karya seperti buku atau CD yang berisi program komputer yang dilindungi hak cipta. Dengan mengingat titik awal ini, Pengadilan selanjutnya beralih ke aturan kelelahan dalam Petunjuk Program Komputer Seni. 4(2): Penjualan pertama salinan suatu program di Komunitas oleh pemegang hak atau dengan persetujuannya akan menghabiskan hak distribusi salinan tersebut dalam Komunitas, dengan pengecualian hak untuk mengontrol penyewaan lebih lanjut dari program atau salinannya.

Sebagaimana dilihat dari sudut pandang tradisi dan WCT, tampaknya sudah menjadi kesimpulan pasti bahwa Pengadilan tidak akan menganggap pendistribusian salinan melalui pengunduhan berarti kehabisan tenaga karena tidak ada “benda berwujud” yang diedarkan. Namun, sebagaimana diketahui, Pengadilan sampai pada kesimpulan sebaliknya: Dengan memberikan penggunanya hak pengguna yang non-eksklusif dan tidak dapat dialihkan untuk jangka waktu yang tidak terbatas untuk program yang dipermasalahkan, pemegang hak (perusahaan Oracle) sebenarnya telah menjual salinan program kepada pengguna. Dalam kasus seperti itu, jelas Mahkamah, tidak ada bedanya apakah salinan program komputer tersebut disediakan kepada pelanggan oleh pemegang hak yang bersangkutan melalui pengunduhan dari situs web pemegang hak atau melalui media material seperti CD-ROM atau DVD.

Setelah menetapkan bahwa transaksi tersebut secara hukum merupakan penjualan, Pengadilan selanjutnya menjelaskan bahwa pendistribusian ciptaan (unduh dari cloud) yang awalnya merupakan tindakan komunikasi kepada publik diubah menjadi sebuah tindakan distribusi. Disajikan dengan penjualan salinan dan klaim berdasarkan hak distribusi, Pengadilan menyimpulkan bahwa telah terjadi penipisan. Karena transaksi di UsedSoft melibatkan penjualan salinan maka Pengadilan juga dapat mengabaikan pernyataan pada

poin petunjuk InfoSoc bahwa pertanyaan tentang kelelahan tidak muncul dalam hal layanan dan layanan online pada khususnya.

Pada tahun 2018, CJEU ditanyai di Tom Kabinet apakah prinsip UsedSoft diterapkan pada e-book berdasarkan Petunjuk InfoSoc. Kali ini, Pengadilan menolak untuk mengikuti keputusannya di UsedSoft. Atau lebih tepatnya, kasus UsedSoft dikemas secara eksklusif tentang program komputer yang dilindungi oleh Petunjuk Program Komputer. Untuk e-book yang tidak dilindungi berdasarkan Petunjuk Program Komputer namun menurut Petunjuk InfoSoc, Pengadilan menjelaskan bahwa "perubahan" pada UsedSoft dari komunikasi ke publik ke distribusi tidak terjadi. Untuk menjelaskan perbedaan tersebut, Pengadilan menyatakan bahwa tidak seperti Petunjuk Program Komputer, legislator UE tidak bermaksud berdasarkan Petunjuk InfoSoc untuk mengasimilasi salinan karya yang berwujud dan tidak berwujud. Lebih lanjut, Pengadilan menjelaskan bahwa realitas ekonomi berbeda untuk program komputer dan buku. Untuk buku, pasar penjualan e-book bekas akan berdampak serius pada penjualan buku fisik baru, sedangkan pasar perangkat lunak tidak akan banyak terpengaruh oleh penjualan program bekas Dengan demikian, penerapan prinsip kelelahan tidak akan menghasilkan keseimbangan antara kepentingan pencipta dan pengguna skalanya akan menurun.

Dilihat dari sudut pandang hukum, kedua keputusan tersebut sangat sulit untuk diselaraskan. Pertama, dari UsedSoft tentang *"perubahan"* sebenarnya berkaitan dengan Petunjuk InfoSoc (dan tentu saja WCT) yang dipertaruhkan di Tom Kabinet. Pada titik ini, Tom Kabinet nyaris mengesampingkan UsedSoft. Kedua, argumen bahwa pembuat undang-undang seharusnya bermaksud memperlakukan salinan fisik dan elektronik secara berbeda di InfoSoc tetapi tidak dalam Petunjuk Program Komputer merupakan pelanggaran terhadap prinsip dasar hak cipta yang menyatakan bahwa perlindungan bersifat abstrak dan mencakup ciptaan dalam bentuk apa pun. disajikan. Proposisi bahwa Petunjuk InfoSoc juga harus mempertimbangkan tindakan yang dilakukan dalam konteks digital berbeda dari tindakan yang dilakukan di dunia fisik bertentangan dengan prinsip umum netralitas teknologi, yang menurutnya aturan yang sama harus diterapkan secara online dan diterapkan secara offline.

UsedSoft dapat digambarkan sebagai kebijakan yang baik namun memiliki kelemahan dalam hukum. Dilihat dari sudut pandang yang lebih umum, gambaran tersebut menggambarkan kesulitan yang dihadapi Pengadilan ketika harus menerapkan aturan yang dikembangkan untuk produk fisik ke produk digital: Haruskah ia mengikuti "hukum" dengan tegas atau mencoba memasukkan pasak persegi ke dalam lubang bundar?. Pengadilan melakukan keduanya dan gagal dua kali. Efek gabungan dari UsedSoft dan Tom Kabinet adalah dua prinsip kelelahan yang berbeda muncul secara bersamaan: satu untuk program komputer dan satu lagi untuk jenis pekerjaan lainnya. Inkonsistensi seperti ini tidak hanya dilihat dari sudut pandang dogmatis. Hal ini juga menimbulkan ketidakpastian hukum misalnya mengenai karya campuran seperti buku yang berisi program komputer. Namun secara lebih umum, jalur zigzag Pengadilan menggambarkan kesulitan dalam menerapkan prinsip kelelahan dalam lingkungan digital. Sebagaimana dikemukakan oleh Reto Hilty, prinsip kelelahan dirancang untuk menjawab pertanyaan tentang penjualan kembali sebuah

salinan. Namun, untuk program komputer, permasalahan utamanya adalah akses untuk menggunakan program tersebut. Model biner dari prinsip exhaustion (ya/tidak) membuat keputusan apakah terjadi exhaustion atau tidak bergantung pada persyaratan lisensi kontrak antara pemegang hak dan pihak pertama yang menerima lisensi penggunaan tersebut. Dengan demikian, habisnya hanya terjadi jika kontrak tersebut merupakan hak pengguna yang tidak eksklusif dan tidak dapat dialihkan untuk jangka waktu yang tidak terbatas. Hal ini memudahkan pemegang hak untuk membuat kontrak karena kelelahan, misalnya dengan membatasi jangka waktu kontrak. Dengan cara ini, UsedSoft mengilustrasikan pentingnya prinsip kelelahan untuk membantu menarik garis antara hak dan kepentingan pemegang hak dan pengguna pertama dan selanjutnya dari program komputer dan bagaimana dampak dari prinsip kelelahan dapat hilang begitu saja. udara tipis dari perjanjian lisensi perangkat lunak.

Menghubungkan

Ini mengikuti dari InfoSoc Directive Art, bahwa Negara-negara Anggota akan memberi para penulis “hak eksklusif untuk mengizinkan atau melarang komunikasi apa pun tentang karya mereka kepada publik”.

Petunjuk ini didasarkan pada prinsip-prinsip dan aturan-aturan yang telah ditetapkan dalam Petunjuk yang berlaku pada saat diadopsi pada tahun 2001. Daripada membuat peraturan baru, Petunjuk ini “mengembangkan prinsip-prinsip dan peraturan-peraturan tersebut dan menempatkannya dalam konteks masyarakat informasi”. Terkait dengan hak pencipta untuk berkomunikasi dengan publik, lebih lanjut dinyatakan bahwa hak ini harus dipahami dalam arti luas yang mencakup semua komunikasi kepada publik yang tidak hadir di tempat asal komunikasi tersebut. Hak ini harus mencakup segala transmisi atau transmisi ulang suatu Ciptaan kepada publik melalui sarana kabel atau nirkabel, termasuk penyiaran.

Sebagaimana telah dijelaskan, Petunjuk InfoSoc dirancang pada pertengahan tahun 1990an. Pada saat itu, banyak bentuk pemanfaatan “modern” yang dimungkinkan oleh digitalisasi yang saat ini kita anggap sebagai hal yang biasa dan tidak kontroversial, masih belum muncul. Linking merupakan contoh utama dari hal ini. Pada saat Peraturan ini diadopsi, pengadilan nasional dan doktrin hukum mengalami kesulitan untuk menyesuaikan diri dengan paradigma hak cipta. Kesulitan mendasarnya adalah apakah melihat pengaturan hyperlink sebagai suatu tindakan (aktif), yang dengan sendirinya melanggar hak cipta (komunikasi kepada publik atau bahkan hak reproduksi), atau apakah tindakan tersebut pantas untuk dipahami sebagai tindakan kontribusi. Mengingat ketidakpastian ini, maka tidak mengherankan jika legislator UE tidak mengambil tindakan tegas ketika mengadopsi Petunjuk InfoSoc namun membiarkannya untuk kasus hukum di masa depan yang menentukan batasnya. Seperti yang akan ditunjukkan, hal ini pada gilirannya menyebabkan ketidakpastian mendasar dalam jangka waktu yang lama mengenai kondisi hukum yang menjadi bagian utama dari hukum hak cipta modern.

Secara tradisional, pelanggaran hak cipta melibatkan seseorang yang terlibat secara aktif dengan karya tersebut dalam membuat salinan, mendistribusikannya, atau mengkomunikasikan karya tersebut kepada publik baik secara langsung (misalnya pertunjukan) atau tidak langsung (misalnya transmisi berdasarkan permintaan). Bentuk-

bentuk pelanggaran ini mengandaikan adanya tindakan aktif dari para pelanggar itu sendiri. Dengan cara ini, Art melarang tindakan mengkomunikasikan ciptaan tersebut kepada publik.

Tautan berbeda dari skema ini. Orang yang membuat tautan ke materi yang dilindungi (musik, teks, film, dll.) tidak terlibat langsung dengan ciptaan tersebut tetapi hanya menunjukkan kepada calon pengguna jalan menuju ciptaan tersebut dan dengan demikian membuatnya lebih mudah ditemukan. Jika karya yang dirujuk oleh tautan tersebut dihapus, tautan tersebut "mati". Juga tidak ada keraguan bahwa orang yang pertama kali mengunggah karya tersebut dan mereka yang mengunduhnya (baik melalui tautan atau upaya mandiri) melakukan tindakan yang tercakup dalam hak cipta pemegang hak dengan menyediakan karya tersebut dan/atau membuat a salinan (hak reproduksi). Dengan cara ini, analisis hak cipta tradisional dapat melihat bahwa penautan merupakan potensi pelanggaran yang berkontribusi. Karena pelanggaran yang berkontribusi berada (dan masih) di luar hak cipta UE, analisis ini juga tidak akan dikaitkan dengan hukum nasional.

Dua keputusan utama CJEU mengenai penautan adalah Svensson pada tahun 2014 dan GS Media pada tahun 2016. Pada saat Svensson diputuskan, CJEU telah menemukan dalam ITV Broadcasting bahwa komunikasi kepada publik mencakup dua kriteria kumulatif, yaitu, *"tindakan komunikasi"* suatu ciptaan dan komunikasi ciptaan tersebut kepada "publik". Sebelumnya, pada tahun 2006 Pengadilan telah menyatakan dalam SGAE bahwa untuk adanya "tindakan komunikasi", cukuplah sebuah karya tersedia untuk publik sedemikian rupa sehingga orang-orang yang membentuk publik tersebut dapat mengaksesnya, terlepas dari apakah mereka memanfaatkan kesempatan tersebut.49 Ketika Svensson dibawa ke hadapan Pengadilan, hal tersebut telah menetapkan cakupan eksklusivitas yang luas. Namun perlindungan masih bergantung pada perilaku aktif pihak yang diduga pelanggar, yaitu suatu tindakan komunikasi.

Namun di Svensson, Pengadilan menemukan jembatan dari Art, untuk menghubungkan. Kasus ini melibatkan penyediaan hyperlink ke materi yang dilindungi yang telah dibuat (dan tetap) tersedia untuk masyarakat umum oleh pemegang hak (yaitu ke "materi hukum"). Pengadilan menemukan, pertama, bahwa menyediakan tautan yang dapat diklik ke karya-karya yang dilindungi memang "membuat karya-karya tersebut tersedia". Meskipun ada cara tidak langsung dalam menghubungkan karya, hal itu dianggap sebagai sebuah "tindakan". Namun, pada saat yang sama, Pengadilan menemukan bahwa karena materi yang dihubungkan dengan tautan tersebut tersedia secara bebas di situs web lain, tautan tersebut tidak membuat karya tersebut tersedia "untuk umum" (yaitu cabang kedua dari ITV Broadcasting).

Svensson mewakili perluasan jangkauan Seni yang dramatis. Meskipun keterkaitan tidak diperkirakan oleh pembuat undang-undang dan meskipun terdapat kata-kata dalam norma dan penafsiran tradisional, Pengadilan berpendapat bahwa keterkaitan tercakup dalam eksklusivitas. Keputusan tersebut juga menjelaskan alasannya. Jelas bahwa Pengadilan merasa dibenarkan oleh tujuan Petunjuk ini dan tujuan untuk menetapkan perlindungan pada tingkat tinggi dan seruan untuk penafsiran yang luas. Selain itu, dengan menjaga tautan ke materi hukum di luar jangkauan hak cipta, keputusan tersebut memungkinkan pengguna internet untuk terus membuat tautan ke materi yang telah

disediakan oleh pemegang hak cipta. Namun keputusan tersebut tidak memberikan jawaban bagaimana menangani tautan ke materi yang belum tersedia secara bebas untuk umum. Keputusan tersebut jelas menyiratkan bahwa penautan hanya diperbolehkan pada materi yang sudah tersedia secara bebas. Namun dampak dari mempertimbangkan untuk menautkan ke materi lain yang dilindungi hak cipta akan menimbulkan risiko umum bagi siapa pun yang membuat tautan dan juga menimbulkan masalah besar dalam menentukan apakah materi yang ditautkan itu sah atau tidak. Faktor-faktor ini pada gilirannya dapat menyebabkan efek pembekuan pada linking. Selain itu, dengan mengandalkan "publik" sebagai faktor penghubung, Pengadilan membuka jaring yang luas hingga mencakup penggunaan oleh pihak swasta dan komersial. Konsekuensi dari Svensson dapat secara serius membatasi kemungkinan setiap orang untuk menggunakan hyperlink. Karena hyperlink merupakan salah satu teknologi inti internet, hak cipta dapat menghambat kerja seluruh internet seperti yang dikenal dan digunakan pada pertengahan tahun 2000an.

Unsur-unsur ini diuraikan oleh Pengadilan dalam kasus GS Media berikutnya. Dalam kasus ini Pengadilan tidak hanya memperluas alasannya, namun juga mengalihkan perhatiannya pada dampak terhadap pengguna dari cakupan eksklusivitas yang luas. Karena penautan merupakan salah satu teknologi internet yang paling menentukan seperti yang kita kenal, dampak-dampak ini penting untuk diperhitungkan, namun hal ini tidak dilakukan oleh Arahan InfoSoc karena alasan yang sama dengan posisi pemegang hak terkait penautan. telah ditangani. Pada saat perumusan dan penerapan Petunjuk InfoSoc, belum ada seorang pun yang benar-benar memperkirakan dampak digitalisasi terhadap hak cipta dan keseimbangan kepentingan pemegang hak dan pengguna internet.

GS Media prihatin dengan pengaturan hyperlink ke karya yang belum tersedia untuk umum oleh pemegang haknya. Pengadilan pertama kali menjelaskan bahwa alasan tidak dilakukannya komunikasi kepada publik di Svensson adalah karena tidak adanya komunikasi kepada publik baru. Lebih lanjut, Mahkamah beralasan, mengingat hyperlink dan situs web yang dirujuknya memberikan akses terhadap karya yang dilindungi dengan menggunakan sarana teknis yang sama, yaitu internet, maka tautan tersebut harus ditujukan kepada publik baru. Apabila hal tersebut tidak terjadi, terutama karena karya tersebut telah tersedia secara bebas untuk semua pengguna internet di situs web lain dengan izin dari pemegang hak cipta, maka tindakan tersebut tidak dapat dikategorikan sebagai "komunikasi kepada publik", dalam arti Pasal 3(1) [Petunjuk InfoSoc]. Memang benar, segera setelah dan selama karya tersebut tersedia secara bebas di situs web yang hyperlinknya mengizinkan aksesnya, harus dipertimbangkan bahwa, jika pemegang hak cipta dari karya tersebut telah menyetujui komunikasi semacam itu, mereka telah mencakup semua pengguna internet.

Selanjutnya, dan mengutip kekhawatiran yang dikemukakan oleh GS Media, Komisi dan beberapa Negara Anggota, Pengadilan membahas dampak "larangan" terhadap keseimbangan yang ingin dibangun oleh Arahan InfoSoc antara kebebasan tersebut dan kepentingan publik di satu sisi. , dan kepentingan pemegang hak cipta dalam perlindungan efektif atas kekayaan intelektual mereka, di sisi lain. Dalam hal ini, Pengadilan mencatat, internet pada kenyataannya sangat penting bagi kebebasan berekspresi dan informasi, yang dilindungi oleh pasal 11 Piagam, dan bahwa hyperlink berkontribusi terhadap kelancaran

operasionalnya serta pertukaran pendapat dan informasi. dalam jaringan itu ditandai dengan tersedianya sejumlah besar informasi.

Selanjutnya untuk mengatasi permasalahan spesifik yang mungkin ditimbulkan oleh pembatasan hyperlink melalui hak cipta bagi individu yang ingin memposting link tersebut, Pengadilan beralih ke aspek prosedural dari pelanggaran hak cipta, yaitu. bagaimana memastikan apakah situs web yang diharapkan akan mengarahkan tautan tersebut, menyediakan akses ke karya yang dilindungi dan, jika perlu, apakah pemegang hak cipta dari karya tersebut telah menyetujui untuk memasangnya di internet. Untuk mengatasi kekhawatiran tersebut, Pengadilan menggunakan salah satu metode tertua yang ada dalam perangkat hukum pihak mana yang menanggung beban pembuktian? Jika orang yang memasang link tersebut tidak mengejar keuntungan, pengadilan nasional harus berasumsi bahwa dia tidak mengetahui dan tidak dapat mengetahui secara wajar, bahwa karya tersebut telah dipublikasikan di internet tanpa izin dari pemegang hak cipta. Dengan memasukkan niat subjektif dari orang yang memasang tautan tersebut (mengejar keuntungan) dalam analisis, Pengadilan telah memasukkan unsur subjektif ke dalam analisis komunikasi terhadap hak publik yang tidak sesuai dengan hukum hak cipta tradisional.

Seperti yang bisa dilihat, Pengadilan menerapkan sejumlah alat metodologi yang berbeda untuk sampai pada kesimpulan yang mengejutkan dan tidak terduga ini. Pertama, Pengadilan berfokus pada keseluruhan objek dan tujuan umum dari norma seperti "perlindungan pada tingkat tinggi" dan kebutuhan untuk mencapai "keseimbangan antara kepentingan pengguna dan pencipta". Kedua, pengembangan norma memerlukan sejumlah langkah berbeda: pertama Svensson meletakkan dasar, kemudian, melalui serangkaian keputusan lain, GSM Media memberikan rinciannya. Ketiga, Pengadilan bergantung pada prinsip-prinsip umum hak-hak dasar untuk menetapkan parameter keseimbangan kepentingan secara keseluruhan. Keempat, fokus pada aspek prosedural (beban pembuktian).

1.5 PERGESERAN DARI HUKUM SUBSTANTIF KE HUKUM ACARA

Munculnya jaringan digital membuka kemungkinan terjadinya penyalahgunaan dan pelanggaran baru. Perkembangan ini telah menggeser fokus praktis dari hukum substantif ke hukum acara. Di dunia digital, pertanyaan krusialnya bukanlah apakah suatu tindakan online tertentu melanggar hak orang lain, karena seringkali memang demikian. Persoalan pentingnya adalah kemungkinan bahwa kesalahan dapat diperbaiki dan menghasilkan sanksi hukum yang sebenarnya dapat dilaksanakan. Pada dasarnya, permasalahan ini berkaitan dengan cara penegakan hukum, yang sekali lagi bergantung pada upaya hukum yang tersedia dan prosedur hukum yang memfasilitasi kemungkinan diberikannya upaya hukum.

Ada banyak permasalahan dalam penegakan hukum, dan khususnya penegakan hukum lintas batas atas pelanggaran jaringan digital, dan sulit untuk menemukan solusi yang memadai. Wacana hukum modern sangat terkait dengan visi prosedur sebagai instrumen bagi suatu badan tertentu. hukum substantif dan terdapat fokus alami pada hukum substantif karena hukum substantif menyajikan hak dan kesalahan. Secara metodologis, realitas digital dan permasalahan penegakan hukum yang kompleks memerlukan

pertimbangan ulang terhadap perbedaan tradisional antara hukum substantif dan hukum prosedural.

Konsep "hak" dapat digambarkan sebagai merujuk pada lingkup otonomi atau kendali yang dilindungi. Dalam pemahaman ini, karakterisasi "hak" berkaitan dengan derajat kendali atau otonomi yang dimiliki seseorang terhadap suatu hak. barang tertentu. Menurut Alf Ross, salah satu tokoh realisme hukum Skandinavia, konsep hak menandai penegasan diri otonom individu. Posisi akademis ini berakar pada bagian positivisme hukum yang disebut sebagai analitis. positivisme litik yang diasosiasikan dengan orang Inggris Jeremy Bentham dan mungkin khususnya John Austin yang mendefinisikan *"hukum"* sebagai *"perintah yang didukung oleh ancaman"*. Menurut kaum positivis analitis, tatanan hukum tidak mempunyai kekuatan mengikat lebih jauh dari kekuatan yang diwujudkan dalam batasan-batasan eksternal tatanan hukum. Selain itu menurut Hans Kelsen, ancaman tindakan koersif yang dilakukan oleh otoritas publiklah yang membedakan norma hukum dengan norma lainnya.

Jika hak diartikan sebagai kepentingan yang dilindungi oleh penerapan sanksi dan upaya hukum, maka dari sudut pandang teoritis, konsep "hak" tidak mempunyai makna independen. Dari sudut pandang praktis, posisi seperti ini terlalu jauh jangkauannya. Konsep "hak" dalam hukum substantif adalah alat untuk teknik penyajian yang hanya melayani tujuan sistematis. Dengan cara ini, pemilik hak substantif diberikan harapan bahwa jika terjadi pelanggaran terhadap hak tersebut, maka tatanan hukum akan menjadi lebih baik. menyediakan tindakan-tindakan pemaksaan kepada pemegang hak yang sesuai dengan representasi hak substantif. Namun, baik dari segi hukum maupun alasan praktis, penegakan hak merupakan sebuah instrumen yang tumpul dan kesesuaian penuh antara representasi hak substantif dan penegakan hak tidak akan pernah dapat dicapai. Alf Ross memperingatkan untuk tidak menganggap hak-hak substantif sebagai fenomena yang sahih, dan sebagai sesuatu yang berbeda dari penggunaan kekerasan (penghakiman dan pelaksanaan) yang dengannya penggunaan dan penikmatan hak secara faktual dan nyata dapat dilakukan. Jika hukum substantif ditafsirkan sebagai sesuatu yang independen dan terisolasi dari aturan prosedural penegakannya dalam kata-kata Alf Ross: terminologi dan gagasan kami memiliki kemiripan struktural yang cukup besar dengan pemikiran magis primitif mengenai pemanggilan kekuatan supernatural yang pada gilirannya diubah menjadi efek faktual.

Oleh karena itu, hak substantif merupakan sebuah bagian yang harus ditafsirkan sehubungan dengan sanksi dan upaya hukum yang tersedia serta sistem prosedural untuk menentukan keabsahan hak tersebut. Intinya di sini adalah bahwa digitalisasi telah meningkatkan kesenjangan antara harapan sehubungan dengan penegakan hukum yang diciptakan oleh representasi hak substantif dan kemungkinan penegakan hak yang sebenarnya. Ketika penegakan hak akibat digitalisasi dibatasi dalam beberapa hal, maka hak substantif juga dibatasi.

Tentu saja, permasalahan penegakan hukum di dunia digital dapat diatasi di tingkat legislatif, dan hal ini juga terjadi, paling jelas di bidang hukum kekayaan intelektual. Pada tingkat dogmatis, permasalahan penegakan hukum dan konseptualisasi "hak" sebagai sebuah hal yang tidak dapat dielakkan. Refleksi tidak hanya mengenai sanksi dan upaya

hukum yang ada, namun juga kesulitan praktis dalam penegakan hukum menunjukkan adanya gaya penafsiran yang lebih luas terhadap langkah-langkah penegakan hukum. Lebih khusus lagi, gaya penafsiran yang berorientasi pada rekonstruksi *"hak substantif"* ke tingkat pra-digitalisasi. Tantangan digitalisasi dalam hal ini erat kaitannya dengan kesulitan praktis penegakan hukum di dunia digital, dan khususnya pada jaringan digital (kesalahan penegakan hukum). Pertama, barang dan jasa yang dilindungi secara hukum dapat dengan mudah ditiru dengan kualitas yang sempurna dan dapat didistribusikan ke sejumlah besar pelanggar potensial dalam waktu yang sangat singkat. Kedua, sering kali sulit untuk mengidentifikasi dan melacak pelanggar sebenarnya, dan bahkan jika pemegang hak berhasil melakukannya, pelanggar mungkin berada di yurisdiksi yang dalam praktiknya tidak menawarkan ganti rugi hukum kepada pemegang hak. Namun, perlu dipertimbangkan bahwa dalam domain internet tertentu, kesalahan penegakan hukum ditangani oleh platform internet yang menerapkan tindakan untuk menghapus konten, baik melalui pemberitahuan (pemberitahuan dan penghapusan) atau secara otomatis (penegakan algoritmik). Kebijakan yang mendasari dan praktik aktual dari platform internet tersebut dapat mengimbangi atau bahkan membalikkan kesalahan penegakan hukum (over-enforcement).

Contoh sederhana dari pendekatan terhadap kesalahan penegakan hukum berdasarkan apa yang disebut "prinsip pengganda" dapat menggambarkan bagaimana gaya penafsiran yang luas dapat mengatasi tantangan tersebut misalnya, pengunduhan dan streaming ilegal terhadap karya yang dilindungi hak cipta terjadi dalam jumlah yang sangat besar. Biasanya, sulit bagi pemegang hak untuk mengidentifikasi dan melacak orang-orang di balik pengunduhan dan streaming ilegal. Sekalipun hal ini memungkinkan, sumber daya yang dibutuhkan untuk penuntutan biasanya tidak sebanding dengan apa yang dapat diharapkan oleh pemegang hak dalam bentuk putusan jika kasusnya dimenangkan karena kerugian yang ditimbulkan oleh masing-masing pelanggar dalam banyak kasus tidak terlalu penting. Dalam skenario ini, sanksi yang relevan adalah sanksi ganti rugi dan sanksi pidana. Secara umum, alasan di balik kerugian adalah pencegahan dan restitusi, dan alasan di balik sanksi pidana adalah pencegahan. Jika mungkin hanya 5% dari pengunduhan dan streaming ilegal yang terdeteksi dan dituntut dan pemegang hak diberikan ganti rugi atas kerugian ekonomi (pencegahan) dan royalti yang wajar (restitusi) sehubungan dengan pelanggaran aktual dalam kasus tersebut, baik pencegahan maupun restitusi tidak dapat dipulihkan. Begitu pula dengan sanksi pidana dalam bidang pencegahan.

Insentif ekonomi untuk tidak melanggar hak-hak orang lain semakin berkurang jika semakin tinggi kemungkinan kerusakan/denda karena alasan tertentu tidak diterapkan dalam setiap kasus. Prinsip multiplier adalah solusi yang bersifat hukuman yang bertujuan memulihkan pencegahan ketika memberikan sanksi berupa uang. Awalnya, prinsip ini digunakan untuk memperkirakan sanksi sosial berupa uang yang optimal jika terjadi kesalahan penegakan hukum. Sanksi berupa uang optimal yang disesuaikan dengan kesalahan penegakan hukum (T) dihitung dengan rumus sebagai berikut:

$$T = eS$$

dimana (e) adalah pengali yang dihitung sebagai 1/p; (p) karena kemungkinan pelanggaran terdeteksi, pelanggar dapat diidentifikasi dan dilacak serta sanksi berupa uang benar-benar diterapkan. (S) adalah sanksi berupa uang yang akan menjadi sanksi berupa uang yang optimal secara sosial jika tidak ada kesalahan penegakan hukum. Bertentangan dengan pemahaman tradisional tentang prinsip pengganda, metodologi hukum digitalisasi tidak memasukkan dasar pemikiran yang melekat pada sanksi optimal sosial. Dasar pemikiran dari bagian metodologi ini adalah untuk menyesuaikan penegakan hukum di dunia digital agar sesuai dengan penegakan hukum di dunia analog, dan kesalahan penegakan hukum juga terjadi di dunia analog. Oleh karena itu, (S) harus dimodifikasi untuk menunjukkan sanksi berupa uang yang sesuai dengan sanksi berupa uang yang dapat diberlakukan di dunia analog dengan kesalahan penegakan hukum biasa. Oleh karena itu, jika ada kemungkinan 5% bahwa sanksi berupa uang akan diberlakukan jika terjadi pelanggaran di dunia digital, dan 50% kemungkinan bahwa sanksi berupa uang akan diberlakukan di dunia analog, maka penggandanya tidak boleh 20 seperti yang disarankan oleh pemahaman awal tentang prinsip pengganda tetapi hanya 10.

Bisa dibilang, banyak yurisdiksi tidak mengizinkan penerapan prinsip pengganda secara otomatis. Oleh karena itu, permainan angka seperti yang diilustrasikan pada contoh sebelumnya tidaklah menentukan. Intinya adalah untuk mengakui bahwa lebih banyak kesalahan penegakan hukum terjadi di dunia digital dan khususnya di jaringan digital, dan sebagai titik tolak untuk menyarankan bahwa margin kebijaksanaan yang besar dalam penghitungan sanksi berupa uang digunakan untuk mengkompensasi kesalahan penegakan hukum.

1.6 PERGESERAN MENUJU GLOBALISASI

Digitalisasi, dan khususnya jaringan digital, tidak mengenal batas geografis, sehingga menimbulkan komplikasi. Jelasnya, globalisasi tidak diciptakan oleh digitalisasi, namun digitalisasi telah memperkuat dimensi global. Dalam metodologi digitalisasi, globalisasi menyiratkan fokus yang lebih kuat pada norma-norma global dalam perundang-undangan nasional serta penerapan hukum nasional.

Ada dua kecenderungan yang saling terkait yang relevan dalam peralihan menuju globalisasi. Kecenderungan pertama adalah harmonisasi hukum substantif regional atau global dan upaya berkelanjutan untuk menetapkan norma-norma hukum internasional yang memberikan perlindungan minimal. Kecenderungan pertama ini paling jelas ditunjukkan oleh perkembangan di bidang hukum kekayaan intelektual di mana penerapan perjanjian internasional tentang perlindungan minimum sudah ada sejak lebih dari 100 tahun sebelum munculnya digitalisasi (lihat sebelumnya). Alasan diadopsinya perjanjian-perjanjian lama ini justru adalah meningkatnya eksploitasi lintas batas yang menciptakan kebutuhan akan perlindungan di pasar luar negeri. Saat ini, pertukaran barang dan jasa lintas negara yang dilindungi oleh kekayaan intelektual telah meningkat secara signifikan.

Di tingkat legislatif, metodologi hukum digitalisasi mendukung aturan internasional. Namun, ruang lingkup penerapan peraturan internasional memiliki keterbatasan karena adanya komplikasi politik dan perbedaan kebutuhan di antara negara-negara yang terlibat.

Konvensi-konvensi global seperti Perjanjian TRIPS merupakan instrumen hukum yang universal dan cocok untuk kebutuhan ekonomi negara-negara maju di wilayah Utara dibandingkan negara-negara berkembang di Selatan. Sebagai konsekuensinya, pada tingkat tertentu Perlindungan lebih lanjut dari norma-norma global sulit dicapai dan kesenjangan ekonomi antar wilayah geografis yang berbeda menunjukkan bahwa norma-norma regional lebih mungkin untuk berhasil.

Kecenderungan kedua adalah pemupukan silang, yang relevan ketika norma-norma global tidak dapat dicapai. Fertilisasi silang terdiri dari dua jenis: sukarela dan terbimbing. Fertilisasi silang terpandu mengacu pada situasi di mana undang-undang nasional memasukkan unsur-unsur yang menciptakan insentif bagi negara lain untuk mengadopsi undang-undang serupa. Sarana penting dalam fertilisasi silang terpandu adalah klausul timbal balik. Amerika Serikat memberlakukan Undang-Undang Perlindungan Chip Semikonduktor pada tahun 1984 (SCPA 1984) dan membuat perlindungan di AS terhadap chip semikonduktor yang dibuat oleh produsen non-Amerika dengan syarat pengesahan undang-undang serupa di negara produsennya. Sebagai hasil dari SCPA tahun 1984, Petunjuk tentang perlindungan hukum topografi produk semikonduktor disahkan pada akhir tahun 1986 di Uni Eropa. Seperti disebutkan sebelumnya, ketika UE mencoba strategi yang sama yaitu fertilisasi silang terpandu sehubungan dengan perlindungan basis data sui generis, namun gagal. Selain perlindungan hak cipta atas basis data, Petunjuk Basis Data UE tahun 1996 mengatur perlindungan basis data sui generis. Berdasarkan Petunjuk sui generis, perlindungan tersedia bagi produsen basis data yang merupakan warga negara dari Negara Anggota UE atau yang memiliki tempat tinggal atau tempat usaha utama di wilayah UE. Namun, Dewan UE dapat dengan persetujuan memperluas hak sui generis terhadap database yang diproduksi di negara-negara ketiga. Menurut pembukaan Petunjuk ini, hak sui generis hanya berlaku untuk database dari negara-negara ketiga "jika negara-negara ketiga tersebut menawarkan hal serupa. perlindungan terhadap basis data yang dihasilkan oleh warga negara dari suatu Negara Anggota atau orang-orang yang memiliki kebiasaan tinggal di wilayah Komunitas". Klausul timbal balik terutama ditujukan kepada produsen basis data AS dan sejumlah undang-undang tentang perlindungan basis data sui generis disajikan dalam Kongres AS tetapi tidak satupun yang disahkan.

Fertilisasi silang secara sukarela mengacu pada situasi di mana negara mengadopsi kerangka peraturan berdasarkan inspirasi dari yurisdiksi lain. Fertilisasi silang secara sukarela dapat ditafsirkan dalam kerangka metodologi Alan Watson tentang "transplantasi legal" yang mengklaim bahwa perubahan hukum dalam banyak kasus disebabkan oleh peniruan tindakan hukum asing. Alan Watson menggambarkan *"transplantasi hukum"* sebagai gerakan perpindahan suatu peraturan atau sistem hukum dari satu negara ke negara lain dan ia menelusuri fenomena tersebut hingga ke hukum Romawi, yang mempunyai dampak besar pada yurisdiksi-yurisdiksi Eropa yang berbeda. Tidak jelas faktor mendasar apa yang mendorong munculnya transplantasi legal. Watson berpendapat bahwa "aksesibilitas" merupakan faktor penting. Oleh karena itu, langkah-langkah hukum yang mudah ditemukan dan dipahami serta terkait dengan yurisdiksi yang memiliki prestise tinggi kemungkinan besar akan diterapkan ke yurisdiksi lain.

Digitalitas menciptakan permasalahan hukum yang tidak ada di dunia analog. Misalnya, dalam undang-undang data pribadi, hak untuk dilupakan tidak akan menjadi masalah hukum jika tidak ada jaringan digital yang komprehensif. Demikian pula dalam undang-undang hak cipta, habisnya hak atas salinan digital dan hyperlink ke karya yang dilindungi hak cipta hanya terjadi sebagai konflik hukum di dunia digital. Masalah hukum ini dan banyak makhluk digital lainnya biasanya muncul pada waktu yang hampir bersamaan ketika aktivitas bermigrasi ke jaringan digital. Pada umumnya masalah-masalah tersebut tidak dibahas dalam undang-undang, dan semua yurisdiksi pada akhirnya memerlukan peraturan hukum untuk mengatasi masalah-masalah tersebut. Dalam situasi tersebut, mencari solusi hukum di yurisdiksi asing merupakan pendekatan yang praktis dan mungkin juga merupakan pendekatan yang rasional. Salah satu contoh penyerbukan silang secara sukarela di dunia digital adalah ketentuan safe harbour dalam Digital Copyright Millennium Act (DMCA) Amerika Serikat yang dikeluarkan pada tahun 1998. Ketentuan safe harbour ini mengecualikan penyedia layanan internet dan perantara lainnya dari tanggung jawab langsung dan tidak langsung, dan tindakan yang sama juga diberlakukan. diadopsi oleh UE dalam bidang Seni. 12–15 Petunjuk e-Commerce. Peter K. Yu mencirikan ketentuan DMCA yang terkait sebagai pola utama untuk prosedur pemberitahuan dan penghapusan.

Dalam proses peradilan (tingkat dogmatis), pergeseran ke arah globalisasi menunjukkan penerimaan yang lebih besar terhadap kasus hukum dari yurisdiksi asing dan kesediaan pengadilan nasional untuk bergantung pada kasus hukum asing dalam batasan yang ditetapkan oleh undang-undang nasional. Di luar batas-batas tersebut, pemahaman terhadap hukum luar negeri dan perbandingan hukum juga penting, karena lingkungan dunia maya yang tanpa batas memicu sejumlah analisis pilihan hukum untuk menemukan opsi hukum yang memungkinkan. Dengan demikian, sifat konflik lintas batas memungkinkan cakupan yang lebih luas. kemungkinan solusi hukum. Atas dasar ini, Graeme Dinwoodie mengusulkan agar pengadilan memutuskan kasus hak cipta internasional bukan dengan memilih undang-undang yang berlaku, namun dengan merancang solusi yang dapat diterapkan, sehingga: Pengadilan yang dihadapkan pada sengketa hak cipta internasional belum tentu menerapkan undang-undang hak cipta suatu negara terhadap permasalahan yang dipermasalahkan tersebut. Sebaliknya, hal ini akan mempertimbangkan apakah dimensi internasional berdampak pada kebijakan negara lain atau sistem hak cipta internasional, dan mengembangkan (dan menerapkan) aturan substantif hukum hak cipta yang paling efektif dalam menerapkan kebijakan-kebijakan tersebut.

Globalisasi menciptakan dorongan menuju penegakan hukum lintas batas dan dampak peraturan ekstrateritorial. Efek ekstrateritorial dapat menyelesaikan konflik lintas batas dan dapat dimasukkan dalam undang-undang seperti Art, dari Petunjuk DSM. Sesuai dengan Art. 5(3), penggunaan karya dan materi pelajaran lainnya hanya untuk tujuan ilustrasi dalam kegiatan pengajaran digital dan lintas batas akan dianggap hanya terjadi di Negara Anggota di mana lembaga pendidikan tersebut didirikan. Fiksi hukum dalam undang-undang yang sesuai dengan prinsip negara asal, jelas cocok untuk memitigasi masalah globalisasi lintas batas.

Dalam putusan, dampak ekstrateritorial dapat dicapai sampai batas tertentu melalui penafsiran yang luas. Di Glawischnig-Piesczek CJEU mengadakan antara lain bahwa Art. Pasal 15(1) Petunjuk e-Commerce harus ditafsirkan bahwa hal tersebut tidak menghalangi pengadilan suatu Negara Anggota untuk memerintahkan penyedia host untuk menghapus informasi yang tercakup dalam perintah tersebut atau memblokir akses ke informasi tersebut di seluruh dunia dalam jangka waktu yang ditentukan. kerangka hukum internasional yang relevan.

1.7 PERGESERAN MENUJU HUKUM YANG BERBASIS HORIZONTAL

Digitalitas menciptakan cara-cara interaksi baru yang memungkinkan adanya bentuk-bentuk komunikasi, model bisnis, dan lain-lain yang baru. Dalam perkembangan yang sedang berlangsung ini, hukum harus beradaptasi dengan kompleksitas realitas yang semakin meningkat dan bergerak cepat. Netralitas teknologi adalah nilai inti dalam memastikan konsistensi peraturan hukum. Pada dasarnya, netralitas teknologi berarti bahwa peraturan hukum harus berlaku untuk dampak yang sama secara independen dari teknologi dan bahwa peraturan tidak boleh mengharuskan atau mengasumsikan teknologi tertentu. Selain itu, peraturannya harus berwawasan ke depan. Sehubungan dengan digitalitas, netralitas menyiratkan bahwa fenomena analog dan digital harus diatur dengan cara yang sama. Oleh karena itu, netralitas teknologi didasarkan pada prinsip yang lebih umum bahwa undang-undang harus berupaya untuk memastikan bahwa kegiatan yang secara substansial serupa diperlakukan dengan cara yang sama.

Sebagaimana dikemukakan oleh Lionel Bentley, undang-undang yang netral secara teknologi masuk akal setidaknya karena dua alasan. Pertama, dalam banyak kasus, badan legislatif ingin mengatur cara-cara perilaku tertentu, seperti penyebaran ujaran kebencian, dan sarana komunikasi yang tidak relevan. Kedua, alasan untuk mendukung undang-undang yang netral secara teknologi adalah untuk meminimalkan, sebisa mungkin, keadaan di mana undang-undang menjadi usang atau tidak efektif atau penerapannya meragukan ketika teknologi ekspresi atau komunikasi berubah (pembuktian di masa depan). Karena teknologi berkembang pesat, Oleh karena itu, terdapat kecenderungan bahwa peraturan perundang-undangan yang spesifik mengenai teknologi selalu tertinggal dibandingkan dengan teknologi itu sendiri.

Netralitas teknologi tidak boleh disalahartikan dengan arti bahwa aturan yang berlaku pada fenomena analog tanpa pertimbangan lebih lanjut harus diperluas ke fenomena digital serupa karena teknologi baru (digitalitas) dapat mendistorsi keseimbangan kepentingan dan nilai yang dijamin oleh aturan asli di dunia analog. Contohnya adalah hak reproduksi dalam undang-undang hak cipta. Pasal 2 Arahan InfoSoc menetapkan bahwa Negara-negara Anggota harus memberikan hak eksklusif untuk mengizinkan atau melarang reproduksi langsung atau tidak langsung, sementara atau permanen dengan cara apa pun dan dalam bentuk apa pun, secara keseluruhan atau sebagian. Hak reproduksi berlaku untuk penyalinan analog dan digital. Cakupan yang luas dari hak reproduksi yang diselaraskan mengharuskan adanya pengecualian wajib terhadap hak reproduksi dalam Art. 5(1) tentang tindakan reproduksi sementara, yang bersifat sementara atau insidental dan merupakan

bagian integral dan esensial dari suatu proses teknologi. Tindakan reproduksi sementara tersebut, yang tidak relevan dalam kaitannya dengan penyalinan analog, terjadi di, misalnya, prosesor komputer atau di memori komputer dan tidak dapat diamati oleh pengguna namun, bagaimanapun, merupakan prasyarat bagi pengguna untuk mengakses karya tersebut. Pengecualian dalam Art. Pasal 5(1), yang secara de facto hanya berlaku untuk penyalinan digital, harus menjamin keseimbangan kepentingan yang sama antara pemegang hak cipta dan pengguna ciptaan yang dilindungi, tidak peduli apakah reproduksinya dilakukan dalam bentuk digital atau analog. Dapat dikatakan bahwa legislator UE tidak berhasil melakukan hal tersebut karena pemegang hak cipta tampaknya diberikan tingkat perlindungan yang lebih tinggi sehubungan dengan reproduksi digital dibandingkan dengan reproduksi analog.

Contoh ini mengilustrasikan bahwa peraturan yang netral secara teknologi yang menangani permasalahan yang sama mungkin berbeda dalam susunan kata dan isinya, agar dapat mencapai dampak yang sama ketika diterapkan pada teknologi tersebut.85 Sebagai konsekuensinya, menilai netralitas teknologi memerlukan perspektif yang lebih luas yang mencakup tujuan dari kebijakan tersebut. aturan-aturan dan mempertimbangkan bagaimana hukum dapat melindungi kepentingan dan nilai-nilai dengan sebaik-baiknya ketika kepentingan dan nilai-nilai tersebut terancam atau terkena dampak perkembangan teknologi.

Sebagai salah satu elemen dalam metodologi digitalisasi hukum, isu netralitas teknologi sebaiknya ditafsirkan sebagai pergeseran ke arah pengambilan keputusan hukum berdasarkan keseimbangan nilai dan kepentingan yang mendasarinya. Pemahaman seperti ini selaras dengan apa yang disebut oleh Carus Craig sebagai pendekatan ekspansif terhadap netralitas teknologi atau “paralelisme preskriptif” yang menyatakan bahwa kita harus berupaya menerapkan undang-undang pada teknologi baru dengan cara yang bertujuan dan secara konsisten memajukan tujuan normatif undang-undang tersebut.

Pendekatan ini memberikan analisis yang fleksibel. Namun, sisi lain dari fleksibilitas adalah berkurangnya prediktabilitas atau ketidakpastian hukum. Bagaimana menyeimbangkan fleksibilitas dan ketidakpastian hukum harus dikaji dalam kasus-kasus konkrit dan tidak akan dibahas lebih lanjut dalam kontribusi ini. Namun, pendekatan dan faktor-faktor dalam penilaian keseimbangan ini sejalan dengan diskusi ilmiah mengenai aturan versus standar.

Secara umum dan sederhana, tujuan normatif undang-undang kekayaan intelektual dapat digambarkan sebagai membangun keseimbangan yang tepat antara, di satu sisi, kepentingan pencipta dalam mengapropriasi nilai ciptaannya untuk tujuan memberikan insentif bagi ciptaan selanjutnya dan, di sisi lain. di sisi lain, kepentingan orang lain untuk memiliki akses terhadap ciptaan yang bermanfaat. Dengan cara yang sama, alasan di balik undang-undang perlindungan data adalah untuk menciptakan keseimbangan yang tepat antara melindungi integritas pribadi seseorang dan kepentingan orang lain untuk memiliki akses ke data pribadi.

Contoh sebelumnya mengenai kerangka hak reproduksi dan pengecualian untuk tindakan reproduksi sementara dalam Petunjuk InfoSoc menggambarkan bagaimana

legislator UE berupaya untuk mengkalibrasi ulang keseimbangan kepentingan pemegang hak cipta dan pengguna hak cipta.

Konsep netralitas teknologi biasanya diasosiasikan dengan peraturan perundang-undangan, namun konsep ini meluas hingga ke ranah ajudikasi yang memerlukan penafsiran yang bersifat purposif atau teleologis terhadap peraturan perundang-undangan.

Sebagai ilustrasi, dalam Kasus Gabungan C-509/09 dan C-161/10 (eDate Advertising), CJEU mengadopsi penafsiran Seni yang bertujuan dan luas. Peraturan Brussel I89 mengenai yurisdiksi khusus dalam kasus perbuatan melawan hukum lintas batas, yang dibuktikan dengan fakta bahwa perselisihan tersebut berkaitan dengan pelanggaran hak kepribadian secara online. Sesuai dengan Seni. Regulasi, seseorang yang berdomisili di suatu Negara Anggota dapat dituntut di Negara Anggota lain dalam hal-hal yang berkaitan dengan perbuatan melawan hukum di pengadilan di tempat di mana peristiwa yang merugikan itu terjadi atau mungkin terjadi. Dalam kasus hukum Pengadilan sehubungan dengan pelanggaran hak-hak pribadi secara offline, istilah "tempat terjadinya peristiwa yang merugikan" dimaksudkan untuk mencakup baik tempat terjadinya kerusakan (tempat akibat) maupun tempat terjadinya. peristiwa yang menimbulkannya (tempat tindakan). Dalam kasus pencemaran nama baik melalui artikel surat kabar yang didistribusikan di beberapa Negara, aturannya berarti bahwa korban dapat mengajukan tuntutan ganti rugi terhadap penerbitnya di hadapan pengadilan Negara di mana penerbit pencemaran nama baik tersebut berada. publikasi didirikan (tempat tindakan), yang mempunyai yurisdiksi untuk memberikan ganti rugi atas semua kerugian yang disebabkan oleh pencemaran nama baik. Sebagai alternatif, korban dapat mengajukan tuntutan ganti rugi terhadap penerbit di hadapan pengadilan di masing-masing Negara di mana publikasi tersebut didistribusikan dan di mana korban mengklaim telah menderita kerugian terhadap reputasinya (tempat berlakunya), yang mempunyai yurisdiksi untuk mengatur. semata-mata sehubungan dengan kerugian yang ditimbulkan di Negara tempat pengadilan disita. Mengacu pada kriteria Art. 7(2), dalam eDate Advertising Pengadilan menyatakan:

Tampaknya internet mengurangi kegunaan kriteria yang berkaitan dengan distribusi, sejauh cakupan distribusi konten yang ditempatkan secara online pada prinsipnya bersifat universal. Selain itu, pada tingkat teknis, tidak selalu mungkin untuk mengukur distribusi tersebut dengan pasti dan akurat sehubungan dengan Negara Anggota tertentu atau, oleh karena itu, untuk menilai kerugian yang disebabkan secara eksklusif di Negara Anggota tersebut. Kesulitan dalam memberikan pengaruh, dalam konteks internet, pada kriteria yang berkaitan dengan terjadinya kerusakan yang diturunkan dari kontras Shevill dan Lainnya dengan sifat serius dari kerugian yang mungkin diderita oleh pemegang hak kepribadian yang menetapkan bahwa informasi yang merugikan hak tersebut tersedia di seluruh dunia.

Menurut Pengadilan, penafsiran sebelumnya terhadap Art. Dengan demikian, Pasal 7(2) Peraturan Brussel I tidak akan memungkinkan para korban untuk menegakkan hak-hak kepribadian mereka dengan cukup efektif sehubungan dengan pelanggaran internet. Oleh karena itu, Pengadilan berpendapat bahwa kriteria yurisdiksi khusus dalam Art. 7(2) harus diadaptasi sedemikian rupa sehingga seseorang yang mengalami pelanggaran hak kepribadian melalui internet dapat mengajukan tindakan di satu forum sehubungan dengan

semua kerugian yang ditimbulkannya, dan di tempat itulah di mana orang tersebut berada. tersangka korban mempunyai pusat kepentingannya sendiri, yang biasanya sama dengan tempat tinggal korban. Dengan cara ini, Pengadilan dalam kasus pelanggaran online menerapkan aturan baru yang memperluas cakupan yurisdiksi khusus berdasarkan Art. 7(2) untuk memastikan keseimbangan kepentingan yang telah ditetapkan di dunia offline, yang merupakan contoh paralelisme preskriptif dalam peradilan.

1.8 PERUBAHAN METODOLOGI PERUNDANG-UNDANGAN

Pergeseran metodologis dari undang-undang yang ditetapkan negara ke undang-undang kontrak dan peraturan perundang-undangan didorong oleh faktor-faktor yang sama yang mendasari peralihan ke undang-undang yang berbasis horizontal, yaitu tantangan untuk mengatasi kompleksitas dan perlunya memberikan fleksibilitas.

Masuk akal untuk berasumsi bahwa tuntutan hukum di dunia digital sangat heterogen karena banyaknya model bisnis, komunitas pengguna, transaksi, dan lain sebagainya yang berbeda-beda, yang terus-menerus muncul dan karena beragamnya kepentingan yang terlibat dalam fenomena tersebut.

Untuk memenuhi tuntutan tersebut, para pelaku hukum membangun model peraturan swasta. Dalam kasus di mana tidak optimal bagi pelaku hukum untuk bergantung pada undang-undang yang ditetapkan oleh negara, mereka dapat memilih untuk tidak ikut serta dan membentuk peraturan hukum yang bersifat privat, terutama melalui cara kontrak atau dengan kode komputer (misalnya tindakan yang membatasi akses ke situs web, perangkat pemblokiran geografis , dll.). Dalam konteks ini, “undang-undang yang ditetapkan negara” adalah istilah umum untuk undang-undang dan kasus hukum. Kontrak dan peraturan perundang-undangan merupakan respons berbasis efisiensi terhadap hukum perundang-undangan yang sifatnya universal. Ketika peraturan yang ditetapkan secara otoritatif tidak memberikan manfaat terbaik bagi para pihak, maka muncullah pengaturan swasta untuk mendefinisikan kembali posisi hukum dan mengubah keseimbangan antara kepentingan-kepentingan yang berlawanan.

Di sisi lain, kontrak dan khususnya peraturan dapat dikatakan meniadakan dampak dari beberapa perubahan metodologi lainnya. Dengan demikian, pemblokiran geografis dan perizinan teritorial melawan globalisasi. Dengan cara yang sama, dapat dikatakan bahwa pembuatan kontrak dengan tujuan untuk mendefinisikan kembali posisi hukum dan mengubah keseimbangan antara kepentingan-kepentingan yang bertentangan dapat bertentangan dengan hukum yang berbasis horizontal sehingga mengarah pada fragmentasi hukum. Untuk menguraikan keterkaitan antara sektor swasta dan swasta. pengaturan hukum dan undang-undang yang ditetapkan negara, konsep “ruang otonomi” akan diperkenalkan.

Undang-undang yang ditetapkan oleh negara mendefinisikan suatu ruang di mana para pelaku hukum dapat bertindak secara otonom, yang selanjutnya disebut ruang otonomi. Di beberapa wilayah hukum yang disahkan negara dimana perlindungan kebijakan publik hanya memainkan peran kecil, ruang otonominya luas, dan di wilayah hukum yang disahkan negara dimana perlindungan kebijakan publik dominan, ruang otonominya sempit.

Di luar ruang otonomi, pihak swasta tidak dapat membuat kesepakatan bersama atau model peraturan lain yang sah yang menyatakan bahwa seperangkat aturan hukum lain harus berlaku bagi mereka. Di bidang hukum informasi, ruang otonominya sangat luas. Namun, ruang otonomi dibatasi oleh peraturan wajib dan hak-hak yang tidak dapat dicabut, yang terdapat dalam undang-undang kekayaan intelektual, dan persyaratan yang lebih ketat untuk mengakui perjanjian yang sah, yang merupakan prinsip utama dalam undang-undang perlindungan data.

Dalam banyak kasus, tidak disebutkan secara tegas dalam undang-undang apakah suatu peraturan tertentu bersifat wajib atau opsional. Jika demikian, pengadilan harus memutuskan masalah ini. Misalnya, CJEU menyatakan dalam UsedSoft (lihat sebelumnya) bahwa aturan tentang kelelahan dalam Art. Pasal 4(2) Petunjuk Program Komputer bersifat wajib dan karenanya tidak dapat dikontrakkan. Mungkin alasan Pengadilan untuk mempersempit ruang otonomi dalam kasus ini adalah pemahaman bahwa merupakan tujuan kebijakan penting dari legislator UE bahwa salinan program komputer dapat diedarkan secara bebas di dalam UE setelah program tersebut dipasarkan oleh Uni Eropa. pemegang hak cipta.

Dalam metodologi digitalisasi hukum, titik tolaknya adalah para pihak diperbolehkan untuk tidak ikut serta dalam undang-undang yang ditetapkan negara, hanya karena negara/pembuat undang-undang tidak memiliki informasi yang cukup mengenai situasi dan kebutuhan hukum para pelaku hukum yang muncul dalam masa otonomi. ruang, dan kebutuhan hukum para pelaku hukum sangatlah beragam. Peralihan dari undang-undang yang ditetapkan negara ke undang-undang kontrak dan peraturan mendukung beragam model peraturan swasta dan dengan demikian menimbulkan fragmentasi hukum. Namun pergeseran metodologi ini tidak mengganggu tiga pergeseran metodologi lainnya: (1) dari hukum substantif ke hukum acara; (2) menuju globalisasi; dan (3) menuju hukum yang bersifat horizontal, karena yang menentukan ruang otonomi adalah kerangka hukum undang-undang yang ditetapkan negara, dan bukan sebaliknya.

Gagasan mengenai ruang otonomi luas sejalan dengan gagasan kebebasan berkontrak. Seperti halnya kebebasan berkontrak, perluasan ruang otonomi juga mempunyai batasan. Kelompok keterbatasan pertama terdiri dari model peraturan yang melanggar norma moral atau bertentangan dengan tujuan kebijakan penting lainnya. Alasan kedua adalah kegagalan pasar. Kegagalan pasar tradisional adalah terciptanya dampak merugikan terhadap pihak ketiga (eksternalitas), biaya transaksi, informasi asimetris yang memungkinkan pihak yang memiliki informasi terbanyak mendapatkan keuntungan yang tidak adil, dan distribusi kekuatan tawar yang tidak merata. Contoh dari hal terakhir ini adalah ketentuan penggunaan media sosial besar. Pengguna media sosial secara individu pada kenyataannya tidak memiliki kekuatan tawar dan media sosial dapat menentukan ketentuannya. Dalam situasi seperti ini, mungkin ada alasan untuk melakukan penyesuaian ruang otonomi.

Dalam konteks perundang-undangan, pergeseran metodologis dari undang-undang yang ditetapkan negara ke undang-undang kontrak dan peraturan perundang-undangan serta pengakuan terhadap ruang otonomi menyiratkan bahwa pembuat undang-undang

harus bertujuan untuk menciptakan ruang otonomi yang luas dan hanya membatasi ruang tersebut ketika terdapat tujuan kebijakan yang penting atau adanya kegagalan pasar. Selain itu, perubahan ini juga menunjukkan bahwa norma-norma nasional dan internasional tidak boleh dipahami dengan cara yang terlalu kaku namun memberikan ruang untuk "eksperimen" baik oleh pengguna maupun pembuat undang-undang. Hal yang sama juga berlaku dalam proses peradilan, dimana pengadilan dapat berkontribusi pada perluasan dan klarifikasi ruang otonomi dengan mempertahankan model peraturan swasta kecuali jika tujuan kebijakan atau kegagalan pasar menyatakan sebaliknya. Untuk tujuan yang sama, pengadilan juga harus enggan untuk menyatakan bahwa suatu peraturan tertentu bersifat wajib kecuali jika secara tegas dinyatakan demikian dalam undang-undang.

BAB 2
TATA KELOLA KEKAYAAN INTELEKTUAL TRANSNASIONAL DI INTERNET

2.1 PENDAHULUAN

Kekayaan intelektual (KI) adalah topik hukum siber klasik dan contoh utama konflik antara komunikasi online global dan hukum lokal. Sedangkan karya sastra dan seni, merek, dan materi HKI lainnya, pada prinsipnya, dapat diakses oleh khalayak global hampir tanpa biaya melalui Internet, hak kekayaan intelektual (HAKI) bersifat teritorial. Perjanjian HKI internasional memungkinkan untuk memperoleh 190+ HKI lokal, misalnya dalam film atau merek dagang terkenal, namun masing-masing HKI lokal tidak bergantung pada HKI lainnya dan ckupan geografisnya terbatas pada wilayah negara tersebut. yurisdiksi HKI yang memberikannya. Fragmentasi ini juga tunduk pada aturan yurisdiksi internasional dan hukum perdata internasional. HKI yang memerlukan pendaftaran, misalnya paten, hanya dapat diputuskan secara penuh di negara tempat pendaftaran. Pelanggaran hak cipta di berbagai negara bagian dapat diputuskan oleh pengadilan di domisili tergugat, namun pengadilan ini pun terikat untuk menerapkan semua undang-undang kekayaan intelektual di negara bagian yang ingin dilindungi. Karena permohonan dan penerapan lebih dari 190 undang-undang hak cipta tidak mungkin dilakukan oleh kedua belah pihak. dan pengadilan, literatur telah mengusulkan untuk mengurangi jumlah undang-undang yang berlaku terhadap pelanggaran hak cipta online yang umum terjadi menjadi satu, yaitu undang-undang yang paling dekat hubungannya dengan pelanggaran (langsung), dan, mengenai tanggung jawab tidak langsung dari penyedia layanan Internet (ISP), hukum Negara tempat pusat aktivitas bisnis mereka. Namun, usulan untuk mengatasi teritorialitas IP secara online belum disetujui oleh pengadilan atau pembuat undang-undang mana pun.

Oleh karena itu, tata kelola IP online yang benar-benar transnasional memerlukan "aturan lain" di luar undang-undang HKI formal, dan keterlibatan aktor non-negara. Aturan HKI menjadi transnasional ketika diterapkan lintas batas. Minimal, hal ini mempengaruhi dua yurisdiksi IP, paling banyak seluruh Internet dan komunikasi global. Tujuan dari Bab ini adalah untuk mendokumentasikan dan mengklasifikasikan contoh-contoh "undang-undang" HKI transnasional yang berasal dari Eropa Barat dan Amerika Utara, dengan fokus khusus pada jangkauan teritorial dari masing-masing rezim. Opsi-opsi yang tersedia bagi pemegang HKI: Ia dapat melarang atau mengizinkan penggunaan HKI miliknya. Bagian berikut mengulas langkah-langkah penegakan HKI transnasional, dan selanjutnya secara singkat membahas praktik perizinan global dan lokal. Berdasarkan gambaran umum ini, bagian penutup mengidentifikasi tiga lapisan tata kelola kekayaan intelektual di Internet.

2.2 PERINTAH PENGHAPUSAN PENGADILAN

Berdasarkan prinsip teritorial, pengadilan memerintahkan penetapan dan upaya hukum lainnya hanya terkait dengan aktivitas di wilayah hukum Kekayaan Intelektual yang dimohonkan dan diterapkan. Namun dalam praktiknya, pengadilan memerintahkan untuk berhenti dan tidak menyediakan konten tertentu di Internet, meskipun hanya satu undang-undang/HAK nasional yang dipertimbangkan, mempunyai efek ekstrateritorial otomatis karena pengguna Internet di negara lain juga kehilangan kemungkinan untuk mengakses sumbernya, terlepas dari apakah konten tersebut melanggar HKI berdasarkan undang-undang negara ketiga tersebut atau tidak.

Jika tergugat dapat menunjukkan bahwa unggahan yang dimaksud adalah sah berdasarkan undang-undang Kekayaan Intelektual tertentu, maka reaksi yang tepat dari pengadilan sesuai dengan prinsip teritorial adalah dengan secara eksplisit membatasi perintah tersebut hanya pada negara-negara yang hukum Kekayaan Intelektualnya dimohonkan dan dilanggar, dan untuk memerintahkan tergugat untuk melakukan pemblokiran geografis terhadap konten yang dipertaruhkan hanya dari wilayah pelanggaran ini. Misalnya, pengadilan Jerman memerintahkan operator situs web di AS yang menyediakan akses ke karya dalam domain publik berdasarkan hukum AS untuk mencegah pengguna di Jerman mengakses tulisan Thomas Mann dan orang lain yang karyanya masih dilindungi hak cipta berdasarkan hukum Jerman di Jerman. Konflik antara hak merek dagang yang dimiliki secara independen dan sah secara setara dalam tanda yang identik atau serupa (misalnya Merck Germany v. Merck U.S.) juga diselesaikan dengan mewajibkan kedua belah pihak menerapkan tindakan penargetan geografis dan pemblokiran geografis untuk menghindari kebingungan konsumen di pasar tempat masing-masing pemilik merek dagang menikmati eksklusivitas. Contoh tandingan yang membuktikan aturan teritorial adalah konflik yurisdiksi Kanada-AS yang terkenal dalam kasus Google V.

Dalam kasus ini, Mahkamah Agung Kanada secara eksplisit memerintahkan Google, berdasarkan dan sebagai kelanjutan dari undang-undang rahasia dagang Kanada, untuk menghapus indeks situs web tertentu tidak hanya dari Google.ca tetapi juga dari hasil pencariannya di seluruh dunia. Sebagai tindakan balasan, Google memperoleh keputusan dari Pengadilan Distrik A.S. yang menyatakan bahwa tatanan global Kanada tidak dapat diterapkan di A.S. mengingat kekebalan operator mesin pencari berdasarkan hukum A.S. Pada saat yang sama, Google melakukan reteritorialisasi mesin pencarinya. Alih-alih mengizinkan pengguna Internet menghindari penghapusan hasil penelusuran hanya dengan beralih ke domain tingkat atas (TLD) Google lainnya kemungkinan yang menjadi perhatian Mahkamah Agung Kanada dan memicu respons globalnya. Google kini menggunakan teknologi geolokasi yang memastikan bahwa pengguna melihat versi hasil pencarian yang sesuai dengan hukum di tempat di mana pencarian tersebut dilakukan. Perintah pengadilan global Kanada pada akhirnya memperkuat fragmentasi teritorial.

Namun dalam sebagian besar kasus, batas wilayah yang terlampaui dalam perintah penghapusan tidak diperhatikan. Salah satu alasannya adalah tingkat harmonisasi internasional yang cukup maju di bidang kekayaan intelektual. Kasus dimana undang-undang

kekayaan intelektual lokal berbeda dalam arti yang berarti relatif jarang terjadi. Misalnya, bahwa film-film terkini tidak boleh tersedia di Internet tanpa izin terlebih dahulu dari pemegang hak cipta, pada umumnya, merupakan pernyataan hukum yang sah secara universal. Dalam kasus yang jelas seperti ini, praktik perintah penghapusan tanpa batas yang berdampak secara de facto di seluruh dunia juga tampak sah. Namun, dalam kasus-kasus sulit dimana terjadi konflik hukum atau hak kekayaan intelektual, dunia maya dipecah melalui pemblokiran geografis di sepanjang perbatasan dunia nyata antar yurisdiksi kekayaan intelektual.

2.3 TINDAKAN PENEGAKAN PERANTARA

Cara kedua, yang secara praktis jauh lebih penting dalam penegakan HKI transnasional di Internet, berkaitan dengan pengaturan mandiri swasta yang dilakukan oleh perantara.

Peran Utama Perantara

Perantara yang menyediakan layanan komunikasi online telah lama menduduki peran sentral dalam tata kelola Internet pada umumnya dan Penegakan HKI online pada khususnya. Pertama, "[n]tidak ada sesuatu pun yang terjadi secara online tanpa melibatkan satu atau lebih perantara" seperti pendaftar nama domain, penyedia akses dan host, mesin pencari, periklanan, dan layanan pembayaran. Kedua, dan berbeda dengan pembajak anonim Di dunia maya, para perantara adalah target yang layak dalam upaya penegakan hukum yang menjalankan bisnis yang sah sebagai bagian dari perekonomian formal. Ketiga, mereka menawarkan solusi terhadap masalah skala pelanggaran hak cipta dan pelanggaran HKI lainnya secara online, yang jumlahnya sangat banyak sehingga mereka tidak akan pernah bisa melakukan hal tersebut. diadili dalam proses pengadilan negara. Melalui kode etik yang digunakan perantara dalam menjalankan layanannya, mereka dapat menerapkan HKI dalam banyak kasus dalam kasus pencarian Google, miliaran dolar dengan biaya yang relatif kecil. Jawaban atas permasalahan pelanggaran HKI melalui teknologi jaringan digital memang ada "di dalam mesin", dan mesin-mesin ini dikendalikan oleh perantara swasta.

Namun hingga saat ini, perantara online belum dianggap sebagai pelanggar langsung. Bukan perantara yang menyediakan karya berhak cipta kepada publik, menjual produk palsu, atau melanggar HKI, melainkan pelanggan/penggunanya. Oleh karena itu, perantara bertanggung jawab atas pelanggaran pihak ketiga jika hanya secara tidak langsung berdasarkan persyaratan tambahan dan sampai batas tertentu. Standarnya berbeda-beda menurut perantara yang bersangkutan dan antar yurisdiksi IP, namun dilema mendasar dan juga pendekatan peraturan terhadap tanggung jawab perantara adalah sama di seluruh wilayah. Di satu sisi, layanan perantara digunakan dalam pelanggaran HKI, mereka menyadari adanya aktivitas ilegal setidaknya setelah diberi tahu, dan mereka berada dalam posisi untuk melakukan sesuatu untuk mengatasinya. Oleh karena itu, pemegang hak cipta dan pemerintah terus-menerus menekan perantara untuk mengekang setidaknya kasus-kasus pembajakan dan pemalsuan yang jelas. Di sisi lain, perantara memberikan layanan netral yang banyak digunakan untuk tujuan yang sah dan bermanfaat secara sosial.

Akibatnya, perantara telah terlindung dari tingkat tanggung jawab yang setara dengan kewajiban umum untuk memantau layanan mereka atau membuat model bisnis mereka yang sah menjadi tidak mungkin dilakukan.

Misalnya, penyedia host dan mesin pencari harus segera menghapus atau menonaktifkan akses ke konten yang melanggar IP setelah pemberitahuan terkait (pemberitahuan dan penghapusan, NTD). Pada saat yang sama, mereka tidak bertanggung jawab terhadap pemegang HKI sampai mereka diberitahu mengenai suatu pelanggaran atau terhadap pelanggan/pengguna mereka atas niat baik penghapusan positif palsu. Kerangka kerja ini membuka "ruang otonomi", di mana perantara dapat mengembangkan kebijakan HKI yang disesuaikan dengan layanan mereka. Solusi internal seperti itu umumnya akan lebih disukai daripada peraturan eksogen yang berpotensi mengganggu dan diberlakukan oleh pengadilan atau pembuat undang-undang. Dalam hal ini, Dalam mengembangkan kebijakan kekayaan intelektualnya, perantara tidak dipandu oleh tujuan kebijakan publik, namun, sebagai perusahaan swasta, dipandu oleh tujuan memaksimalkan keuntungan. Dalam konteks tanggung jawab IP, hal ini berarti menavigasi secara hemat biaya antara tanggung jawab Scylla dari IP dan Charybdis pelanggan yang tidak puas dengan layanan yang terlalu membatasi. Mengenai cakupan teritorial dari kebijakan Kekayaan Intelektual, skala ekonomi tidak mendukung penerapan standar transnasional yang mencakup seluruh layanan dibandingkan dengan upaya spesifik negara, yang diterapkan melalui teknologi geolokasi yang mahal. Semua aspek ini mendukung munculnya kebijakan Kekayaan Intelektual yang bersifat swasta dan transnasional.

Namun, seperti yang ditunjukkan oleh contoh-contoh berikut ini, negara masih terus melakukan hal tersebut. Dengan mendefinisikan standar tanggung jawab hukum Kekayaan Intelektual, pembuat undang-undang dan pengadilan dapat mempengaruhi isi dan ruang lingkup kebijakan perantara mengenai Kekayaan Intelektual. Selain itu, Komisi Eropa dan pemerintah lainnya telah lama memaksa para perantara untuk menerima kode etik IP yang lebih konkrit.

2.4 TINDAKAN PENEGAKAN PERANTARA DAN DAMPAK TRANSNASIONALNYA

Langkah-langkah penegakan hukum yang dilakukan oleh perantara dan dampak transnasionalnya bervariasi tergantung pada jenis layanan yang diberikan dan cakupan geografis penerapan aturan pengaturan mandiri.

Pendaftaran Nama Domain

Dalam kasus pendaftar nama domain, upaya gabungan dari pemilik merek dagang dan pemerintah menghasilkan rezim global yang sangat awal dan terkenal, yaitu "Kebijakan Penyelesaian Sengketa Nama Domain yang Seragam" (UDRP), yang diadopsi oleh Internet Corporation untuk Assigned Names and Numbers (ICANN) pada tahun 1999, yang masih berlaku hingga saat ini dalam versi aslinya. Munculnya UDRP terikat erat dengan hukum dan kebijakan AS. Setelah menjadi kasus hukum yang diselesaikan yang mendaftarkan merek dagang sebagai merek nama domain untuk dijual kepada pemegang merek dagang yang bersangkutan merupakan pelanggaran merek dagang, badan legislatif AS pada tahun 1999

memperluas perlindungan merek dagang untuk mengatasi masalah “penghuni liar dunia maya” di luar AS. Undang-Undang Perlindungan Konsumen Anticybersquatting (ACPA) mengizinkan tindakan perdata in rem terhadap pendaftar nama domain yang berbasis di A.S. atas penyitaan atau pembatalan nama domain atau pengalihan nama domain dari pemegang nama domain asing ke pemilik masing-masing tanda. Khususnya, undang-undang ini memberikan kekebalan kepada pendaftar nama domain kecuali mereka bertindak dengan itikad buruk atau secara ceroboh mengabaikan tugas mereka berdasarkan undang-undang tersebut.

Pada saat yang sama, privatisasi Internet sedang berjalan lancar. Pada tahun 1998, Departemen Perdagangan AS mengumumkan bahwa Sistem Nama Domain global akan dikendalikan dan dikoordinasikan secara terpusat oleh ICANN, sebuah perusahaan nirlaba di California, namun harus ada persaingan antara pendaftar nama domain yang diakreditasi oleh ICANN. Hal ini, pada gilirannya, menciptakan risiko bahwa cybersquatters non-AS dapat mendaftarkan tanda-tanda yang dilindungi merek dagang kepada pendaftar non-AS di luar jangkauan undang-undang merek dagang AS dan ACPA. Selain itu, Sistem Nama Domain global menyoroti masalah konflik hak merek dagang di Internet. Jika tanda yang sama atau tanda yang sangat mirip dapat dilindungi merek dagang di negara A untuk perusahaan A, dan di negara B untuk perusahaan B, siapa yang berhak menggunakan tanda tersebut di Internet?

Untuk mengatasi masalah penegakan hukum dan koordinasi yang mungkin terjadi, pemerintah AS meminta Organisasi Kekayaan Intelektual Dunia (WIPO) untuk berkonsultasi dengan pemegang merek dagang dan anggota komunitas Internet dengan tujuan untuk mengembangkan rekomendasi untuk “pendekatan seragam dalam menyelesaikan masalah merek dagang/nama domain perselisihan yang melibatkan pembajakan dunia maya (dan bukan konflik antara pemegang merek dagang dengan hak bersaing yang sah)”. Sesuai dengan saran ini, fokus UDRP adalah pada “penghuni liar dunia maya” yang beritikad buruk. Singkatnya, UDRP mengharuskan pendaftar dan pemohon nama domain untuk tunduk pada proses administratif wajib jika pemegang merek menyatakan bahwa (1) nama domain yang terdaftar identik atau mirip dengan merek dagang, (2) pemegang nama domain tidak mempunyai hak atau kepentingan yang sah sehubungan dengan nama domain tersebut, dan (3) nama domain tersebut telah didaftarkan dan digunakan dengan itikad buruk. Jika persyaratan ini terpenuhi, panel UDRP dapat memerintahkan pembatalan nama domain atau pengalihannya kepada pihak yang mengajukan pengadu, yang harus dilakukan oleh pendaftar yang bersangkutan setelah sepuluh hari kerja. Melalui pencantumannya dalam perjanjian pendaftaran seluruh ICANN Sebagai pendaftar yang terakreditasi, UDRP telah menjadi standar hukum global, mengikat semua pemegang TLD umum dan banyak kode negara, terlepas dari domisili pendaftar dan pihak lain yang terlibat. Mayoritas dari ribuan keputusan panel UDRP menguntungkan pemilik merek dagang dan belum menghasilkan peninjauan kembali yang dapat diterima oleh pengadilan negara bagian.

Dari perspektif undang-undang merek dagang tradisional dan fragmentasi teritorialnya, keberhasilan jangka panjang UDRP masih merupakan sebuah kejutan. Pelapor

hanya perlu menunjukkan kepemilikan atas satu merek dagang nasional untuk mendapatkan TLD umum seperti.com, yang berguna untuk kegiatan komersial di seluruh dunia. Dengan demikian, UDRP melengkapi merek dagang nasional yang mempunyai dampak di seluruh dunia. Namun globalisasi merek dagang nasional ini dapat diterima karena UDRP hanya menargetkan kasus-kasus sederhana yang terbatas. Pertama, UDRP hanya peduli dengan nama domain dan bukan konten yang dapat diakses melalui domain tersebut. Kedua, orang yang mendaftarkan domain tersebut tidak boleh mempunyai hak atau kepentingan sah apa pun sehubungan dengan nama tersebut. Perselisihan antara pemegang hak-hak nasional yang sama-sama sah dalam domain yang identik/serupa berada di luar cakupan UDRP dan tetap tunduk pada sistem undang-undang Kekayaan Intelektual yang terfragmentasi secara teritorial. Dan yang ketiga, pendaftaran harus dilakukan dengan "itikad buruk", misalnya, untuk tujuan menjual domain tersebut kepada pelapor atau untuk menghasilkan lalu lintas situs web yang menyesatkan. Tampaknya ada konsensus global yang stabil bahwa "penghuni liar dunia maya" yang beritikad buruk tidak pantas mendapatkan kesabaran. Merek dagang nasional apa pun yang valid sudah cukup untuk mengeluarkannya dari sistem nama domain global.

Kerapuhan dan keterbatasan "konsensus" ini menjadi jelas, ketika pemegang hak cipta Amerika Serikat mencoba untuk melibatkan ICANN dan registrar terakreditasinya dalam skema penegakan hak cipta, yang menurutnya nama domain untuk "situs bajakan" yang diberitahukan akan dibatalkan. Jika rencana ini terwujud, penegakan HKI swasta melalui sistem nama domain, untuk pertama kalinya, akan melampaui tingkat nama domain/merek dagang hingga ke lapisan konten. Setelah program penegakan hak cipta "pemberita tepercaya" antara Motion Picture Association of America dan dua operator pendaftaran untuk TLD generik baru (satu berbasis di AS, satu lagi di Abu Dhabi) diumumkan ke publik, namun para pendaftar dengan cepat membatalkannya. Perjanjian Registri ICANN saat ini dengan registrar TLD generik baru mengharuskan registrar untuk melarang pemegang TLD generik baru terlibat dalam "pembajakan, pelanggaran merek dagang, atau hak cipta memalsukan atau terlibat dalam aktivitas yang bertentangan dengan undang-undang yang berlaku", dan untuk memberikan "(konsisten dengan hukum yang berlaku dan prosedur terkait) atas aktivitas tersebut termasuk penangguhan nama domain". Namun demikian, tidak ada - Sistem penyelesaian sengketa online pengadilan yang sebanding dengan UDRP diterapkan untuk menegakkan arahan ini.

2.5 PENYEDIA AKSES

Melibatkan pendaftar nama domain dalam penegakan hak cipta dan undang-undang terkait konten lainnya memang akan menjadi masalah karena dampak luas dari pembatalan nama domain, yang secara de facto memutus server yang menghosting situs web yang (diduga) melanggar dari Internet. Sebagai perbandingan, perintah pemblokiran yang kurang efektif dan kurang luas jangkauannya terhadap penyedia akses, yang juga dapat diterapkan melalui sistem nama domain, dianggap oleh Pengadilan Hak Asasi Manusia Eropa sebagai "tindakan ekstrem" yang "sengaja mengabaikan perbedaan antara informasi legal dan ilegal

yang mungkin terdapat dalam situs web, dan membuat konten dalam jumlah besar tidak dapat diakses yang belum teridentifikasi sebagai ilegal".

Karena kekhawatiran ini dan peran penyedia akses yang netral dan "sekadar saluran" mengenai konten yang dikirimkan oleh layanan mereka, ISP ini menikmati kekebalan yang luas dan selama beberapa waktu berhasil menghindari keterlibatan dalam penegakan HKI secara online. Posisi pihak luar tersebut termasuk dalam kategori ini Namun, hal ini dipicu oleh munculnya aktivitas berbagi file secara besar-besaran secara peer-to-peer yang tidak sah pada awal tahun 2000an, yang mana pemegang hak cipta tidak dapat secara efektif mengekangnya dengan memburu individu pelanggar anonim. Selain itu, dalam upaya melawan barang palsu yang dijual di Internet , pemegang hak semakin menyoroti penyedia akses sebagai target yang memungkinkan.

Jenis awal skema penegakan hukum swasta yang melibatkan penyedia akses adalah apa yang disebut prosedur "respons bertahap", yang diadopsi oleh penyedia akses dari beberapa negara "secara sukarela" setelah mendapat tekanan kuat dari pemegang hak dan pemerintah. Konsep dari program ini adalah hak cipta pemilik akan melaporkan alamat IP dinamis yang digunakan untuk berbagi file ilegal kepada penyedia akses. Penyedia akses yang pelanggannya telah menggunakan alamat IP pada waktu yang relevan kemudian mengirimkan peringatan kepada pengguna tersebut. Setelah tiga sampai enam peringatan ("teguran"), penyedia akses akan memberikan sanksi kepada pelanggannya dengan membatasi bandwidth atau bahkan dengan memutus sementara pelanggar berulang dari Internet.

Langkah-langkah ini tidak diterima dengan baik oleh masyarakat umum dan sebagian besar telah ditinggalkan. Alih-alih menargetkan pengguna Internet secara individu, jenis tindakan penegakan HKI yang kedua yang melibatkan penyedia akses menjadi lebih menonjol: pemblokiran situs web. Pada tahun 2014, CJEU menyatakan bahwa Negara-negara Anggota UE harus memastikan bahwa pemegang hak cipta dapat mengajukan perintah terhadap penyedia akses untuk melarang mereka mengizinkan pelanggannya mengakses situs web yang melanggar hak cipta jika perintah tersebut tidak menghilangkan akses pengguna Internet ke situs web yang melanggar hak cipta. informasi yang sah. Keputusan ini mendukung kolaborasi antara pemegang hak dan penyedia akses untuk memastikan bahwa semua ISP memblokir situs web tertentu, dan jika konten yang melanggar dipindahkan ke domain lain, halaman baru ini juga akan diblokir.

Jika diterapkan dengan cara-cara ini, pemblokiran situs web dapat menjadi langkah penegakan HKI yang efektif. Namun, jangkauan geografisnya agak terbatas dan jarang bersifat transnasional. Alasannya adalah, berbeda dengan pembatalan domain oleh registrar, pemblokiran situs web oleh penyedia akses tidak berlaku pada satu sumber pelanggaran namun melekat pada penerima yang mencoba mengakses sumber tersebut. Selain itu, hanya pelanggan dari penyedia akses tertentu yang terkena dampak tindakan pemblokiran. Dan karena penyediaan akses ke Internet memerlukan kendali atas infrastruktur fisik, penyedia akses melakukan bisnis dan memiliki pelanggan dalam wilayah yang jelas, biasanya dalam suatu negara. Pemblokiran situs web terjadi di setiap negara,

berdasarkan rezim HKI lokal dibandingkan dengan penyedia akses lokal dan pelanggannya. Dalam hal ini, teritorial HKI sesuai dengan fragmentasi pasar telekomunikasi.

Kedua perantara yang dibahas sebelumnya mempunyai peran yang sangat berbeda di dunia maya. ICANN dan registrar terakreditasinya mengontrol sistem nama domain dasar, sedangkan penyedia akses beroperasi di ujung Internet. Oleh karena itu, cakupan geografis dari tindakan yang diambil oleh para perantara ini berbeda-beda. Pembatalan nama domain berlaku di seluruh Internet dan dengan demikian secara global, pemblokiran situs web oleh penyedia akses hanya memengaruhi pelanggannya (yaitu penduduk negara bagian tertentu). Penyedia host dan operator mesin pencari masih mengendalikan infrastruktur lainnya. Yang pertama dapat secara langsung mengganggu komunikasi yang melanggar HKI dengan mencegah unggahan ex ante, dengan menghapusnya dan memastikan agar tetap tidak diunggah. Sebaliknya, mesin pencari hanya dapat mengurangi kemampuan menemukan sumber ilegal dengan menghapus hasil pencarian; situs web yang melanggar tetap dapat diakses. Kekuatan penyedia host dan mesin pencari untuk mengatur komunikasi online lintas negara dan bahkan mungkin di seluruh dunia juga serupa. Keduanya, secara kasar, terletak di antara pendaftar nama domain dan penyedia akses. Layanan perantara mereka kurang mendasar dibandingkan ICANN namun lebih sentral dibandingkan operasi periferal penyedia akses.

Sejalan dengan itu, kebijakan HKI dari penyedia host dan mesin pencari mungkin, namun belum tentu, mempunyai implikasi transnasional atau bahkan global.60 Dampak teritorial dari tindakan penegakan HKI mereka bergantung pada keadaan teknis, hukum dan ekonomi. Jika undang-undang yang berlaku tidak menentukan cakupan geografis yang diperlukan atau diperbolehkan untuk melakukan penghapusan atau pertanyaan tersebut belum terselesaikan, penyedia host dan mesin pencari hanya mempunyai keputusan individual yang *"otonom"* apakah akan mengadopsi dan menerapkan satu kebijakan IP di seluruh layanan. atau apakah akan mereproduksi fragmentasi wilayah HKI dan undang-undang lainnya dengan membagi layanannya ke dalam versi spesifik negara dengan kebijakan penghapusan/penghapusan HKI yang terpisah. Pada akhirnya, ini adalah keputusan bisnis pribadi yang dapat berubah seiring berjalannya waktu dan biasanya tidak diumumkan secara publik. Salah satu contoh yang telah disebutkan terkait dengan mesin pencari Google, yang mungkin juga berkaitan dengan proses pengadilan yang tertunda di berbagai yurisdiksi, direstrukturisasi sehingga bukan pengguna, dengan memasukkan domain tingkat atas tertentu seperti .ca atau .de, yang menentukan versi hasil pencarian yang ditampilkan, namun Google sendiri melalui teknologi geolokasi. Penyedia host juga terkadang menggunakan domain yang berbeda untuk negara yang berbeda, sedangkan negara lain beroperasi dengan domain .com universal.

Terlepas dari kurangnya transparansi dalam bidang ini, ada beberapa alasan untuk berasumsi bahwa sebagian besar penghapusan HKI oleh penyedia host dan operator mesin pencari mempunyai dampak yang luas dan transnasional. Hal ini tentu terjadi jika layanan yang menghosting situs web membuat situs web tersebut tidak aktif. Kecuali jika penyedia host lain mengambil tindakan, konten tersebut tidak akan dapat diakses oleh semua

pengguna Internet di seluruh dunia. Misalnya, kode etik NTD Belanda mewajibkan penghapusan situs web yang dihosting di Belanda oleh penyedia layanan asal Belanda jika situs tersebut "ternyata ilegal" berdasarkan undang-undang hak cipta Belanda. Setiap elemen dari skema pemesanan pribadi ini terikat dengan Belanda kecuali untuk negara Belanda. dampak penghapusan situs web, yang bersifat global.

Penghapusan platform online dan mesin pencari yang mendominasi pasar juga secara signifikan mengurangi komunikasi online ilegal. Ukuran layanan suatu perusahaan teknologi besar mungkin tidak bersifat global (karena layanan tersebut mungkin tidak tersedia di semua negara, terutama Tiongkok), namun konten yang dihapus dari, misalnya, penelusuran Google secara efektif menghilang dari pandangan publik di banyak negara. Pertimbangan efisiensi biaya umumnya akan mendorong platform online dan operator mesin pencari untuk menerapkan penghapusan IP di seluruh layanan mereka dan juga di seluruh yurisdiksi IP. Oleh karena itu, perusahaan-perusahaan teknologi besar AS telah mengglobalisasi prosedur NTD lokal mereka di semua negara tempat mereka beroperasi. Dalam laporan transparansi, Google menyatakan bahwa formulir webnya untuk pemberitahuan pelanggaran hak cipta konsisten dengan Digital Millennium Copyright Act [U.S.] Digital Millennium Copyright Act (DMCA) dan menyediakan mekanisme yang sederhana dan efisien bagi pemilik hak cipta dari negara/wilayah di seluruh dunia. Facebook juga telah menyatakan niatnya untuk memerangi pelanggaran hak cipta dan merek dagang dengan "program pemberitahuan dan penghapusan global.

Meskipun pernyataan-pernyataan ini hanya menyangkut keseragaman prosedur IP, tidak ada alasan untuk percaya bahwa penghapusan yang diakibatkannya dilaksanakan dengan cara yang terfragmentasi dan spesifik pada suatu negara, misalnya hanya untuk negara tempat pemberitahuan pelanggaran disampaikan. Jika hanya ada satu kebijakan IP, kebijakan tersebut mungkin akan dijalankan secara seragam di seluruh platform. Selain itu, pelanggaran kekayaan intelektual sering juga dianggap sebagai pelanggaran terhadap persyaratan layanan platform, yang, dalam kasus YouTube, "ditegakkan secara konsisten di seluruh dunia, di mana pun konten diunggah. Ketika suatu konten dihapus karena melanggar pedoman kami, maka konten tersebut akan dihapus secara global". Kebijakan yang berulang terhadap pelanggar, seperti yang diterapkan oleh sebagian besar pasar online dan platform konten buatan pengguna (UGC), tentu akan menghasilkan dampak yang luas pada layanan ini. Jika akun pelanggan ditangguhkan sementara atau dihentikan sama sekali, orang tersebut tidak dapat menggunakan platform untuk menyediakan konten yang melanggar HKI di mana pun.

Meskipun cakupan geografisnya tidak disebutkan secara eksplisit, Memorandum of Understanding (MoU) UE "tentang penjualan barang palsu melalui internet", yang disepakati pada tahun 2011 antara semua pasar online besar dan banyak pemegang HKI, menegaskan bahwa pendekatan layanan secara luas terhadap Penegakan HKI. Di satu sisi, MoU mendefinisikan "barang palsu" sebagai "barang fisik tidak asli yang diproduksi tanpa persetujuan Pemilik Hak yang melanggar [merek terdaftar, hak desain atau hak cipta], sesuai dengan Negara Anggota atau Undang-undang UE". Komisi Eropa juga menekankan bahwa

para penandatangan MoU harus mematuhi undang-undang UE dan undang-undang nasional serta melaporkan bahwa platform online prihatin dengan cakupan geografis yang terkadang tidak jelas dari HKI yang diajukan karena telah dilanggar. Di sisi lain, platform penyedia layanan berkomitmen untuk menerapkan prosedur NTD sehingga penawaran yang diberitahukan menjadi tidak tersedia untuk masyarakat umum melalui Platform Internet, yaitu di seluruh layanan. Tindakan pencegahan, tata letak yang tepat tetap berada pada kebijaksanaan penyedia platform, juga harus mencegah barang palsu ditawarkan atau dijual "melalui layanan mereka". Komisi Eropa selanjutnya melaporkan bahwa para penandatangan MoU telah membentuk tim internal khusus yang bertanggung jawab atas penegakan HKI "secara global". Komisi Eropa pada akhirnya berharap dapat memfasilitasi standar juga untuk tingkat internasional.

Sekali lagi sebagai contoh tandingan yang membuktikan aturan penegakan hukum transnasional, ISP sangat menentang kebijakan HKI di seluruh layanan *(global)* ketika menyangkut tindakan di luar prosedur NTD yang sederhana dan tindakan pencegahan yang bersifat diskresioner, atau ketika program-program ini harus dilaksanakan. melampaui pelanggaran hak cipta, merek dagang, dan hak desain yaitu melampaui pembajakan dan pemalsuan). Jika perusahaan teknologi besar menerima kewajiban tambahan seperti itu, mereka hanya akan melakukannya berdasarkan negara per negara.

Misalnya, pada tahun 2007 Google dan Facebook menolak penerapan "Prinsip untuk Layanan Konten Buatan Pengguna", yang mencakup kewajiban penyaringan untuk pasar AS. "Kode Praktik Penelusuran dan Hak Cipta" Inggris tahun 2017 yang mana Google dkk. secara sukarela menyetujui, antara lain, secara otomatis menurunkan "situs web yang melanggar" dalam hasil penelusuran dan mencegah pembuatan saran pelengkapan otomatis yang mengarahkan konsumen ke situs tersebut, secara eksplisit dibatasi pada hasil penelusuran "dikembalikan ke konsumen di Inggris". Konten YouTube Sistem ID, yang digunakan perusahaan untuk mengubah risiko tanggung jawab hak cipta menjadi mesin penghasil uang, juga berfungsi spesifik di suatu negara. Di bawah program ini, pemilik hak cipta terdaftar dapat mengirimkan file video ke YouTube yang kemudian memindai semua unggahan pengguna berdasarkan basis data referensinya. Ketika konten dalam video di YouTube cocok dengan karya di basis data referensi, pemegang hak menerima peringatan dan dapat memutuskan apakah mereka ingin konten tersebut diblokir, dimonetisasi, atau apakah mereka lebih suka melacak statistik penayangan video tersebut. Tindakan-tindakan tersebut dapat bersifat spesifik pada suatu negara; misalnya "sebuah video dapat dimonetisasi di satu negara/wilayah dan diblokir atau dilacak di negara/wilayah lain". Meskipun YouTube mengiklankan sistem NTD+ swasta ini sebagai kesuksesan besar, YouTube secara intensif melobi menentang langkah UE yang mewajibkan penerapan sistem NTD+ ini. Untuk memberikan salah satu contoh terakhir, laporan transparansi yang wajib dibuat oleh YouTube, Facebook, dan platform media sosial besar lainnya berdasarkan Undang-undang Anti-Ujaran Kebencian di Jerman menunjukkan bahwa "Undang-Undang Penegakan Jaringan" ini diterapkan hanya untuk pengguna di Jerman. Jika YouTube dkk. Jika mereka diberitahu mengenai dugaan pelanggaran undang-undang Jerman, mereka akan

menerapkan, sebagai langkah pertama, standar komunitas global mereka. Hanya jika suatu jabatan ditemukan sesuai dengan standar universal ini, barulah, pada langkah kedua, diukur berdasarkan undang-undang Jerman. Jika konten memenuhi standar komunitas namun tidak sesuai dengan hukum Jerman, konten tersebut hanya akan dihapus di Jerman namun tetap dapat diakses di semua negara lainnya.

Layanan Iklan Dan Pembayaran

Pelanggar IP yang bertindak demi keuntungan tidak hanya bergantung pada layanan pendaftar nama domain dan berbagai ISP, namun lebih jauh lagi pada layanan periklanan dan pembayaran. Jika tidak ada iklan yang muncul di situs streaming ilegal dan tidak ada transaksi pembayaran yang dilakukan untuk para pemalsu, para pelaku ini akan segera dipaksa keluar dari bisnis ilegal mereka. Meskipun sangat dipertanyakan apakah pengiklan, penyedia layanan iklan online seperti Google AdSense, dan pemroses pembayaran seperti PayPal secara tidak langsung bertanggung jawab atas pelanggaran kekayaan intelektual yang dilakukan oleh pelanggan/mitra mereka, para perantara ini telah melakukan hal ini pada dekade kedua abad ke-21. menjadi target strategi penegakan hukum kekayaan intelektual yang disebut "follow the money".

Di beberapa negara, asosiasi pemegang hak, pengiklan (pemilik merek) dan penyedia iklan online dan layanan pelacakan konsumen telah menyetujui prosedur yang bertujuan untuk menghindari penempatan iklan di situs web "yang tidak memiliki kegunaan substansial yang sah". Untuk ini Pada akhirnya, pemegang hak, terkadang bekerja sama dengan otoritas publik seperti Unit Kejahatan Kekayaan Intelektual Kepolisian London, menyusun database situs web yang melanggar kekayaan intelektual dan membaginya dengan pengiklan, yang pada gilirannya menginstruksikan perantara online (misalnya Google) untuk mencegah kemunculannya. iklan mereka di outlet-outlet yang masuk daftar hitam ini. Terlepas dari kenyataan bahwa perantara iklan kembali beroperasi dalam skala besar dan oleh karena itu memiliki kepentingan ekonomi untuk menerapkan praktik daftar hitam tersebut di seluruh layanan mereka, kode peraturan mandiri pada poin ini secara eksplisit berlaku di setiap negara. pendekatan negara. Memorandum yang difasilitasi oleh Komisi Eropa "terbatas bagi setiap penandatangan layanan yang disediakan di Negara-Negara yang menjadi Pihak dalam Wilayah Ekonomi Eropa"; kode etik Austria hanya mencakup situs web bajakan yang ditujukan untuk audiens Austria, Prinsip Praktik Baik Inggris berlaku untuk situs web yang menargetkan pengguna Inggris, dan seterusnya. Sikap membatasi terhadap kebijakan kekayaan intelektual dalam konteks periklanan sangat kontras dengan kebijakan di seluruh layanan. dan dengan demikian prosedur NTD "global". Hal ini mungkin mencerminkan kasus hukum yang jauh lebih lemah dalam meminta pertanggungjawaban pengiklan dan perantara iklan atas pelanggaran kekayaan intelektual di situs web pihak ketiga. Meskipun terdapat konsensus global yang menyatakan bahwa penyedia host dan mesin pencari harus menghapus pelanggaran kekayaan intelektual, namun tidak ada kesepakatan mengenai hal tersebut dalam industri periklanan.

Namun kelemahan ini telah diatasi melalui intervensi luar biasa yang dilakukan oleh Organisasi Kekayaan Intelektual Dunia (WIPO). Setelah mendapatkan mandat dari negara-

negara anggotanya, WIPO mengembangkan, dan pada tahun 2019 memulai, platform online "WIPO ALERT", yang berfungsi sebagai pusat global untuk program iklan kekayaan intelektual nasional. Setelah menandatangani surat kesepahaman dengan WIPO, "Berwenang Kontributor" dari 193 negara anggota WIPO mana pun dapat mengunggah daftar URL situs web yang melanggar hak cipta ke database WIPO. Pengiklan, biro iklan dan penyedia layanan teknis mereka dari negara anggota WIPO lainnya dapat mengajukan permohonan untuk menjadi "Pengguna Resmi" WIPO ALERT. Setelah memeriksa "bonafiditas" mereka, mereka dapat mengakses dan secara otomatis menerapkan daftar hitam yang dikumpulkan "dari seluruh dunia". Seperti halnya Komisi Eropa dan otoritas publik lainnya, WIPO menggambarkan perannya sebagai fasilitator netral dalam penegakan hukum yang sah. praktik. WIPO juga secara tegas menunjukkan bahwa mereka tidak menyatakan "bahwa situs tertentu, berdasarkan hukum, telah melanggar hak cipta". Sebaliknya, "situs yang menjadi perhatian" yang masuk dalam daftar hitam didefinisikan sebagai "lokasi online yang secara wajar dicurigai oleh Kontributor Resmi sengaja melanggar atau memfasilitasi pelanggaran hak cipta dan hak terkait, baik di negara tempat pendiriannya atau di tempat lain". Definisi ini terinspirasi oleh Sec. 115A Undang-Undang Hak Cipta Australia, yang mengatur perintah pemblokiran terhadap penyedia akses dengan ketentuan bahwa "tujuan utama dari lokasi online adalah untuk melanggar hak cipta (baik di Australia atau tidak)". WIPO menyatakan bahwa dalam praktiknya hanya "fasilitator pelanggaran hak cipta yang mencolok" yang tercakup dalam database ALERT dan dengan demikian terputus dari aliran pendapatan iklan global.

Target kedua dari pendekatan "ikuti uang" adalah penyedia layanan pembayaran online seperti PayPal dan perusahaan kartu kredit seperti Visa atau Mastercard. Perantara ini sangat kuat karena mereka mampu memantau pedagang yang mencurigakan dan menghubungkan aktivitas mereka di berbagai bank. Meskipun Eropa tampaknya menjadi pusat upaya untuk melibatkan industri periklanan yang sangat terdiversifikasi dan tersebar secara geografis, pemerintah AS telah mendorong dan mendukung inisiatif yang disebut *"RogueBlock®"*, yang diluncurkan pada tahun 2012 dan kini mencakup banyak salah satu penyedia pembayaran terbesar di dunia. RogueBlock® ditengahi oleh International AntiCounterfeiting Coalition (IACC) yang berbasis di Washington, D.C., sebuah organisasi nirlaba yang khusus memerangi pemalsuan dan pembajakan produk, yang keanggotaannya terdiri dari lebih dari 250 perusahaan dan organisasi dari 40+ negara. RogueBlock® menawarkan Anggota IACC mempunyai kemungkinan untuk melaporkan penjual barang palsu atau bajakan secara online langsung ke perusahaan kartu kredit dan jasa keuangan dengan tujuan memfasilitasi tindakan cepat terhadap pedagang tersebut. Menurut IACC, program ini telah menghentikan lebih dari 5.000 akun pedagang dan berdampak pada lebih dari 200.000 situs web. Cakupan geografis dari skema ini bersifat global dalam arti tidak peduli di mana situs web "nakal" tersebut dihosting atau di mana pedagang "nakal" berada. berdomisili. Sebaliknya, RogueBlock® dipicu segera setelah barang yang ditawarkan melalui situs web tidak mematuhi undang-undang kekayaan intelektual baik di negara asal maupun negara tujuan. Setiap transaksi yang tidak sepenuhnya "kepatuhan yurisdiksi ganda" di

tempat asal dan tujuan dianggap ilegal. Pedagang yang terlibat dalam aktivitas ilegal tersebut berisiko terputus dari sistem pembayaran global, meskipun penawaran mereka sah menurut hukum di domisili mereka dan/atau di negara ketiga.

Tiga Perizinan HKI

Alih-alih melarang penggunaan IP yang dilindungi dengan menegakkan hak-haknya, pemegang hak bebas memberikan lisensi dan dengan demikian mengizinkan penggunaannya. Meskipun prinsip teritorialitas mempersulit penegakan hukum kekayaan intelektual transnasional di Internet, kerangka hukum yang ada pada kenyataannya mendukung perizinan online global.

Pertama, peraturan yang mengatur kepemilikan awal HKI pada umumnya seragam di seluruh dunia, sehingga memastikan bahwa orang yang sama, khususnya pencipta suatu ciptaan dan orang yang pertama kali mengajukan paten atau HKI terdaftar lainnya, memperoleh keseluruhan hak milik. HKI nasional. Jika aturan mengenai kepemilikan awal berbeda (penulis versus pemberi kerja/komisaris; orang pertama yang mengajukan versus orang pertama yang menemukan), pihak-pihak yang terlibat memiliki kepentingan yang sama dalam menghindari pemisahan rangkaian kepemilikan awal dan selanjutnya dalam IP yang sama. Oleh karena itu, pengadilan berasumsi bahwa semua hak yang relevan telah secara implisit dialihkan ke satu entitas tunggal. Kedua, pemegang hak global tersebut bebas menggunakan hak teritorial "pribadinya" secara seragam dalam skala global, baik dengan memproduksi dan menjual kekayaan intelektual. -produk yang dilindungi di pasar dunia atau dengan memberikan lisensi di seluruh dunia kepada satu penerima lisensi.

Namun dalam praktiknya, HKI seringkali dimonetisasi berdasarkan negara per negara. Sebuah *"celestial jukebox"* global seperti yang dibayangkan oleh Paul Goldstein pada awal tahun 1990-an, di mana pengguna dapat mengakses konten apa pun dari mana saja dan kapan saja dengan imbalan pembayaran (mikro), belum terwujud. Menurut laporan tahun 2017 oleh the Komisi Eropa untuk e-commerce di UE, hal ini juga berlaku untuk komersialisasi online atas konten yang dilindungi hak cipta di "Pasar Tunggal Digital". Menurut Komisi, "mayoritas konten digital online tampaknya tersedia bagi pengguna secara umum di tingkat nasional, atau untuk wilayah yang mencakup dua hingga empat Negara Anggota, dalam kasus terakhir ketika mereka menggunakan bahasa yang sama". Komisi selanjutnya melaporkan bahwa "70% responden penyedia konten digital membatasi akses ke layanan konten digital online mereka dari Negara Anggota lain". Pemblokiran geografis diterapkan terhadap semua jenis konten digital kecuali produk berita, dan hal ini paling banyak terjadi dalam perjanjian untuk film, olahraga, dan serial TV. Apa yang berlaku untuk Pasar Tunggal UE juga berlaku untuk pasar global. Oleh karena itu, tidak mengherankan jika program ID Konten YouTube memungkinkan pemegang hak dari seluruh dunia untuk mengontrol konten mereka di platform dengan cara yang spesifik untuk setiap negara sehingga "sebuah video dapat dimonetisasi di satu negara/wilayah dan diblokir atau dilacak di negara lain". Shira Perlmutter, yang saat ini menjabat sebagai Chief Policy Officer dan Direktur Urusan Internasional di Kantor Paten dan Merek Dagang A.S. dan mantan eksekutif

kekayaan intelektual tingkat tinggi di industri musik dan film, juga percaya bahwa "teritorialitas akan bertahan di masa mendatang".

Selain sektor musik online, di mana organisasi manajemen kolektif nasional merupakan pemain penting yang berusaha keras untuk melepaskan monopoli nasionalnya, kerangka hukum global, sebagaimana telah dijelaskan, bukanlah alasan utama masih adanya perizinan teritorial dan pemblokiran geografis. Sebaliknya, pemegang hak membagi pasar geografis karena mereka menganggap hal ini sebagai keputusan bisnis yang optimal. Diferensiasi produk dan harga memang merespons perbedaan permintaan dan daya beli lokal sehingga menjanjikan keuntungan maksimal. Pemblokiran geografis untuk mencapai tujuan ini juga didukung oleh undang-undang yang melarang pengelakan langkah-langkah perlindungan teknologi.

Sebaliknya, akses global resmi tidak pernah digabungkan dengan persyaratan pembayaran langsung. Sebaliknya, pemegang hak memberikan akses gratis kepada siapa pun di negara mana pun dan, tergantung kasusnya, dapat mencoba memonetisasi Konten Terbuka miliknya secara tidak langsung, khususnya melalui iklan. Kategori konten yang sering didistribusikan dengan cara ini mencakup berita, tulisan akademis, perangkat lunak, dan berbagai jenis UGC non-profesional. Banyak standar perizinan yang tersedia untuk cara distribusi ini, terutama berbagai lisensi Perangkat Lunak Bebas dan Sumber Terbuka serta lisensi Creative Commons. Jika tidak ada lisensi resmi yang diadopsi, pengadilan menafsirkan ketersediaan gratis atas konten yang dilindungi hak cipta sebagai otorisasi tersirat dari pemegang hak penggunaan kembali Internet yang dapat diperkirakan dan diterima secara umum seperti penyalinan dan penyediaan gambar oleh mesin pencari. Baik lisensi Konten Terbuka formal maupun tersirat mengizinkan penggunaan di semua negara, yaitu secara global. Singkatnya, otorisasi untuk menggunakan IP yang dilindungi di seluruh Internet kurang umum dibandingkan yang diperkirakan. Pasar layanan berbasis biaya masih terfragmentasi secara teritorial. Akses global yang sah secara praktis terbatas pada Konten Terbuka, yang biasanya tidak mencakup karya paling populer dan dalam hal ini bernilai.

Bagian II
Perlindungan/Privasi Data

3
Tata Kelola Undang-Undang Perlindungan Data UE

3.1 PENDAHULUAN

Undang-undang perlindungan data biasanya menetapkan standar dan prosedur yang harus diikuti oleh organisasi dalam perlakuan terhadap data pribadi, serta memberikan hak-hak kepada individu untuk mengakses, memperbaiki, atau menghapus data pribadi mereka. Undang-undang semacam ini juga dapat menetapkan sanksi atau denda bagi pelanggaran terhadap keamanan atau privasi data.

Undang-undang perlindungan data adalah peraturan hukum yang dirancang untuk melindungi informasi pribadi individu dari penyalahgunaan, pengaksesan tidak sah, atau pengolahan yang tidak sah oleh pihak lain. Tujuan utama undang-undang perlindungan data adalah untuk memberikan hak kepada individu atas informasi pribadi mereka dan untuk memberikan panduan kepada organisasi atau entitas yang mengumpulkan, menyimpan, dan mengolah data pribadi.

Undang-undang perlindungan data biasanya mencakup beberapa aspek, termasuk:

1. **Hak Privasi Individu:** Memberikan hak kepada individu untuk mengetahui apa saja informasi pribadi mereka yang dikumpulkan, bagaimana informasi tersebut digunakan, dan untuk memberikan persetujuan sebelum data mereka diproses.
2. **Kewajiban Pihak yang Mengelola Data:** Menetapkan kewajiban bagi organisasi atau entitas yang mengumpulkan data untuk melindungi informasi pribadi, mengambil langkah-langkah keamanan yang sesuai, dan memberikan laporan jika terjadi pelanggaran keamanan data.
3. **Persetujuan Pengguna:** Mengharuskan organisasi untuk memperoleh persetujuan dari individu sebelum mengumpulkan, menyimpan, atau mengolah data pribadi mereka.
4. **Akses dan Koreksi Data:** Memberikan hak kepada individu untuk mengakses data pribadi mereka yang dikumpulkan dan untuk mengoreksi atau menghapus informasi yang tidak akurat.
5. **Pemindahan Data:** Menetapkan aturan terkait pemindahan data pribadi antara entitas atau negara.
6. **Hukuman dan Sanksi:** Menetapkan sanksi atau denda bagi pelanggaran undang-undang perlindungan data untuk mendorong kepatuhan.

Contoh undang-undang perlindungan data yang terkenal termasuk Regulasi Umum Perlindungan Data (GDPR) di Uni Eropa, Undang-Undang Perlindungan Data Pribadi (PIPA) di Korea Selatan, dan Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia. Masing-masing negara atau wilayah dapat memiliki undang-undang sendiri yang mengatur perlindungan data sesuai dengan kebijakan dan norma lokal.

Beberapa contoh undang-undang perlindungan data termasuk Peraturan Umum Perlindungan Data (General Data Protection Regulation/GDPR) di Uni Eropa, California Consumer Privacy Act (CCPA) di Amerika Serikat, dan undang-undang perlindungan data di berbagai negara lainnya yang memiliki fokus serupa untuk melindungi privasi dan keamanan data pribadi.

Undang-undang perlindungan data dapat dianggap sebagai rezim hukum inti dalam penelitian internet dan digitalisasi. Bagaimanapun, hal ini muncul sebagai sebuah bidang pendekatan regulasi yang benar-benar baru terhadap perkembangan teknologi yang belum pernah diketahui sebelumnya—pemrosesan data otomatis dan pengambilan keputusan otomatis. Dengan demikian, hal ini dapat dibandingkan dengan bidang hukum lain yang juga menangani fenomena teknologi baru, misalnya hukum energi atom atau rekayasa genetika.

Namun, yang masih menjadi pertanyaan adalah apakah pengaturan awal dan isi undang-undang perlindungan data masih selaras dengan pendekatan yang berlaku saat ini terhadap peraturan mengenai konsekuensi penggunaan alat, layanan, dan pemrosesan data digital yang diperlukan seiring dengan semakin digitalnya dunia kita. Mungkin, jadi hipotesis di bab berikutnya, mempelajari tentang komputasi di mana-mana, data besar, komputasi awan, pemrosesan volume berkecepatan tinggi, atau kecerdasan buatan telah mengubah pendekatan tentang cara mengontrol pemrosesan data dan pengambilan keputusan otomatis, sehingga kita menemukan sebuah rezim hukum baru.

Hipotesis ini dapat dengan mudah ditegaskan dengan mempertimbangkan retorika ketika, pada tahun 2018, Peraturan Perlindungan Data Umum Eropa (GDPR) mulai berlaku dan Petunjuk Perlindungan Data (DPD) sebelumnya dibatalkan. “Kerangka kerja baru ini ambisius, kompleks dan ketat” dan “radikal”, kerangka ini “menggantikan Petunjuk Perlindungan Data 95/46/EC” dan “ditetapkan untuk memaksa perubahan besar dalam segala hal mulai dari teknologi hingga periklanan, dan obat-obatan hingga perbankan”. Pada saat yang sama, DPD Uni Eropa yang ada saat ini digambarkan sebagai “tidak lagi relevan dengan era digital saat ini”.

Namun, jika kita melihat lebih dekat rezim peraturan perundang-undangan perlindungan data saat ini dibandingkan dengan permulaannya, mungkin kita akan mendapatkan hasil analisis yang lebih berbeda dan dengan demikian membantu untuk lebih memahami dampak digitalitas global. Analisis kali ini berkonsentrasi pada pendekatan Eropa, dengan melihat secara khusus GDPR dan sejauh mana pendekatan tersebut mengatasi fenomena baru dan apakah pendekatan tersebut menafsirkan instrumen dan tujuan baru.

3.2 SEJARAH UNDANG-UNDANG PERLINDUNGAN DATA

Undang-undang perlindungan data telah memenuhi empat tujuan utama sejak awal: Pertama, mereka menemukan pengambilan keputusan otomatis sebagai subjek peraturan baru. Pada tahun 1960an, khususnya administrasi negara, dan juga badan swasta menyadari meningkatnya kebutuhan akan informasi baru di dunia yang semakin kompleks yang memerlukan teknologi informasi baru dan pemrosesan informasi baru untuk mengatasi tantangan-tantangan ini. Perangkat produksi baru, model bisnis kredit dan pinjaman dan

kebutuhan pemasaran di sektor swasta serta permintaan akan tata kelola dan perencanaan di wilayah administratif memerlukan lebih banyak informasi dan penggunaan informasi yang ada dengan lebih baik dan dengan demikian diperlukan cara-cara baru dalam mengatur dan menyusun data. Ketika otomatisasi pemrosesan data diterapkan dimaksudkan untuk membuat data tersedia untuk berbagai tujuan, dengan cepat menjadi jelas bahwa informasi kini tidak memiliki konteks dan karenanya tidak memiliki kendali atas subjek informasi tersebut.

Kedua, berdasarkan pemahaman ini, ketersediaan data dan kemampuan teknis untuk memanfaatkannya menciptakan ketidakseimbangan kekuasaan yang sampai saat itu belum diketahui. Siapa pun yang mempunyai alat untuk mengumpulkan dan menggunakan data yang tersedia, kemudian dapat menggunakan informasi ini untuk mempengaruhi pengambilan keputusan. Sebagai konsekuensinya, individu dapat menjadi objek (yang berpotensi positif) perencanaan swasta dan administratif, tata kelola, serta (yang berpotensi negatif) manipulasi dan kontrol. Oleh karena itu, inti dari perlindungan data adalah mengatur asimetri kekuatan informasi.

Ketiga, perlindungan data memerlukan regulasi pemrosesan data sehingga aturan hukum yang jelas dapat ditegakkan. Hal ini dilatarbelakangi oleh pemahaman bahwa dampak pemrosesan data dapat sangat memberatkan individu dan kepentingan hukum dan masyarakat sehingga hanya tindakan legislatif yang dapat menjamin perlindungan yang tepat. Alat-alat lain, khususnya pengaturan mandiri, misalnya, informasi pribadi industri teknologi tidak akan cukup.

Akhirnya, menjadi jelas bahwa pengolahan data bukanlah tindakan tunggal yang terbatas pada bidang kehidupan tertentu. Sebaliknya, perlindungan data diperlukan untuk mengatasi semua bidang di mana teknologi informasi dan pemrosesan data otomatis berlangsung. Hal ini memerlukan peraturan payung yang mengikat setiap tindakan pemrosesan data.

Instrumen

Untuk mencapai keempat tujuan tersebut, rezim peraturan perlindungan data yang pertama—khususnya di Hessia di Jerman pada tahun 1970 sebagai undang-undang perlindungan data pertama di dunia, dan juga di DPD Eropa pada tahun 1995—mencakup instrumen tertentu untuk mencapainya. Di antara banyak isu yang mungkin diangkat di sini, hanya dua yang akan disebutkan secara khusus:

Pertama, rezim hukum perlindungan data awal ini dipandang dalam tradisi hukum teknologi, sehingga memanfaatkan prinsip dan struktur yang sudah ada di bidang hukum ini. Pengambilan keputusan otomatis dianggap sebagai teknologi baru dengan konsekuensi yang tidak diketahui yang memerlukan regulasi dan pengendalian, serupa dengan energi atom, emisi, atau bahan kimia. Salah satu konsekuensi dari model fungsi hukum teknologi ini mengakibatkan undang-undang perlindungan data bertindak dari sudut pandang preventif. Mereka mengikuti prinsip kehati-hatian sebagaimana dikenal dalam hukum teknologi. Daripada menetapkan aturan baru mengenai tanggung jawab atau tugas kehati-hatian yang diatur dari pendekatan hukum sekunder, mereka berfokus pada pengaturan pemrosesan

data pada tingkat primer. Oleh karena itu, hasil pengolahan data, keputusan yang diambil dari akses dan penggunaan data, biasanya tidak ditangani.

Kedua, kekhawatiran mengenai seringnya penggunaan pengambilan keputusan otomatis muncul pertama kali sehubungan dengan ketersediaan data dan teknologi informasi di tangan Negara. Alasannya dapat dipahami dari ketersediaan dan kecanggihan teknologi informasi dan komunikasi itu sendiri: Pada tahun 1960an dan 1970an, hanya sedikit sekali pelaku yang memiliki kebutuhan dan sumber daya untuk memanfaatkan alat pemrosesan data yang ada. Kita juga tidak boleh lupa bahwa teknologi informasi sering kali didorong oleh dinas rahasia dan tindakan Negara lainnya. Jika negara meningkatkan kekuasaannya terhadap warga negara, maka kesimpulannya adalah, hal ini merupakan situasi yang sangat mengancam hak asasi manusia dan gagasan demokrasi.

Instrumen tambahan lain yang juga memiliki pengaruh dalam perancangan Undang-undang. Undang-undang perlindungan data mencakup peraturan dan ketentuan hukum yang merinci hak, kewajiban, dan tanggung jawab terkait perlindungan data. Beberapa instrumen utama yang sering ditemukan dalam undang-undang perlindungan data meliputi:

1. **Definisi Data Pribadi:** Menetapkan definisi yang jelas tentang apa yang dianggap sebagai "data pribadi." Ini mencakup informasi yang dapat diidentifikasi atau dapat dihubungkan dengan individu tertentu.
2. **Persetujuan Pengguna (Consent):** Menyediakan kerangka kerja untuk mendapatkan persetujuan dari individu sebelum mengumpulkan atau memproses data pribadi mereka. Undang-undang dapat menentukan persyaratan khusus terkait informasi yang harus disertakan dalam permintaan persetujuan.
3. **Hak Individu:** Menetapkan hak-hak individu terkait data pribadi mereka, seperti hak untuk mengakses data, memperbaiki informasi yang tidak akurat, atau bahkan menghapus data dalam beberapa kasus.
4. **Kewajiban Pihak yang Mengelola Data:** Mengatur kewajiban organisasi atau entitas yang mengumpulkan dan memproses data pribadi, termasuk langkah-langkah keamanan yang harus diambil dan tanggung jawab jika terjadi pelanggaran keamanan data.
5. **Pemindahan Data Internasional:** Jika data pribadi dipindahkan melintasi batas negara, instrumen undang-undang biasanya menetapkan persyaratan khusus terkait pemindahan internasional data.
6. **Pemberitahuan Pelanggaran Keamanan Data:** Menyusun ketentuan yang memerlukan organisasi untuk memberi tahu individu dan otoritas pengawas jika terjadi pelanggaran keamanan data yang dapat mengancam privasi.
7. **Penegakan dan Sanksi:** Menetapkan sanksi atau denda untuk pelanggaran undang-undang perlindungan data, untuk mendorong kepatuhan dan memberikan insentif kepada organisasi untuk melindungi data pribadi.
8. **Pengawasan Otoritas:** Menetapkan peran dan tanggung jawab otoritas pengawas yang bertugas mengawasi penerapan undang-undang perlindungan data dan menanggapi pelanggaran.

Contoh instrumen undang-undang perlindungan data yang terkenal termasuk Regulasi Umum Perlindungan Data (GDPR) di Uni Eropa, Undang-Undang Perlindungan Data Pribadi

(PIPA) di Korea Selatan, dan Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia. Instrumen-instrumen ini berfungsi sebagai kerangka kerja hukum untuk melindungi privasi dan keamanan data pribadi individu.

Oleh karena itu, undang-undang perlindungan data pada awalnya terutama mengatur keseimbangan kepentingan publik yang mendukung akses Negara terhadap dan penggunaan data serta hak-hak individu yang menjamin kebebasan dan otonomi individu. Akibatnya, keputusan-keputusan awal yang berpengaruh seperti keputusan sensus Mahkamah Konstitusi Jerman pada tahun 1983 berkonsentrasi pada pembatasan kekuasaan negara dan mengabaikan potensi peralihan kekuasaan ke pihak swasta akibat penggunaan teknologi informasi dan pemrosesan data. Secara keseluruhan, penggunaan teknologi ini oleh pihak swasta kurang ditangani dan tidak terlalu intensif. Akibatnya, kebangkitan internet pada tahun 1990an dan munculnya aktor swasta dalam pemrosesan data termasuk akses luas terhadap layanan pemrosesan data, perangkat keras dan perangkat lunak sering kali diabaikan.

3.3 TANTANGAN UNDANG-UNDANG PERLINDUNGAN TERHADAP DIGITALITAS GLOBAL

Ketika melihat awal mula perlindungan data ini, kita dapat menyimpulkan bahwa tidak banyak perubahan yang terjadi. Semua tujuan undang-undang perlindungan data yang disebutkan sebelumnya masih berlaku. GDPR didasarkan pada tujuan tersebut, dan tampaknya—untuk menjawab pertanyaan umum dalam buku ini—perlindungan data mungkin terbukti menjadi benteng dalam rezim hukum yang belum menerapkan digitalisasi. banyak mengubah pendekatan regulasi yang ada. Hal ini bahkan tampak konsisten dengan temuan bahwa perlindungan data sejak awal ditujukan untuk digitalitas. Oleh karena itu, kita dapat dengan mudah menyatakan bahwa digitalitas global telah melampaui perlindungan data, dan memang demikian adanya.

Namun, ketika melihat lebih dekat pada masing-masing ketentuan GDPR sebagai penerus DPD sebelumnya, kami menemukan beberapa aktivitas sehubungan dengan efek khusus dari digitalisasi. Bagaimanapun, GDPR merupakan reaksi terhadap beberapa pengalaman berdasarkan undang-undang perlindungan data sebelumnya, mengenai ketidakefektifan dan penegakannya yang minimal dan bertentangan. Kita juga dapat menambahkan bahwa GDPR sekarang mencerminkan pemahaman yang lebih baik tentang nilai dan kualitas informasi. Dampak ekonomi dari karakteristiknya sebagai apa yang disebut “kebaikan bersama”, serta pentingnya akumulasi internet, misalnya, di pasar “pemenang mengambil segalanya”.

Globalisasi digital membawa sejumlah manfaat signifikan, tetapi juga menghadirkan beberapa hambatan terkait dengan implementasi Undang-Undang Perlindungan Data (UU PDP) atau regulasi serupa. Beberapa hambatan tersebut melibatkan kompleksitas lingkup globalisasi, ketidaksesuaian regulasi antarnegara, dan tantangan terkait keamanan data. Berikut beberapa hambatan yang mungkin dihadapi:

1. **Perbedaan Ketentuan Hukum Antar Negara:**
    - **Ketidaksesuaian Regulasi:** Setiap negara memiliki regulasi perlindungan data yang berbeda-beda. Ini dapat menyulitkan perusahaan yang beroperasi

secara lintas batas untuk mematuhi semua persyaratan yang berlaku di berbagai yurisdiksi.

- **Ekstrateritorialitas UU:** Beberapa UU PDP bersifat ekstrateritorial, yang berarti mereka berlaku untuk organisasi di luar wilayah negara tersebut jika mereka mengumpulkan atau memproses data warga negara atau penduduk setempat.

2. **Kompleksitas Transaksi Lintas Batas:**
    - **Pemindahan Data Internasional:** Pemindahan data pribadi antar negara dapat melibatkan aturan yang kompleks dan persyaratan tambahan, seperti persetujuan khusus atau perlindungan ekstra terkait keamanan data.
3. **Perlindungan Terhadap Ancaman Keamanan Digital:**
    - **Keamanan Data:** Globalisasi digital dapat meningkatkan risiko keamanan data, termasuk serangan siber dan pelanggaran keamanan data. Menjaga keamanan data menjadi tantangan yang semakin besar dalam lingkungan digital global.
4. **Tantangan Teknologi:**
    - **Teknologi Baru:** Kemajuan teknologi, seperti penggunaan kecerdasan buatan dan analisis data yang canggih, dapat menimbulkan tantangan baru dalam mengelola dan melindungi data pribadi dengan tepat.
5. **Kesesuaian dengan Standar Internasional:**
    - **Ketidaksesuaian Standar Internasional:** Terdapat perbedaan dalam standar perlindungan data internasional. Beberapa negara atau entitas mungkin menghadapi kesulitan dalam mematuhi standar yang berlaku di tingkat global.
6. **Kesulitan Penegakan:**
    - **Penegakan Hukum Antarbatas:** Penegakan hukum melintasi batas menjadi sulit, terutama jika suatu organisasi melanggar regulasi perlindungan data di satu negara, tetapi berbasis di negara lain.
7. **Kesadaran dan Pendidikan:**
    - **Kurangnya Kesadaran:** Tidak semua pengguna dan organisasi memiliki pemahaman yang memadai tentang perlindungan data. Kesadaran yang kurang dapat menyulitkan implementasi dan kepatuhan terhadap UU PDP.

Pengatasi hambatan-hambatan ini memerlukan kerjasama internasional, pengembangan standar global, dan kebijakan yang dapat beradaptasi dengan perubahan cepat dalam lingkungan digital global. Selain itu, penting untuk meningkatkan pemahaman dan kesadaran masyarakat serta meningkatkan kapasitas keamanan siber secara keseluruhan.

Reaksi terhadap defisit penegakan hukum dapat diidentifikasi dalam sejumlah norma GDPR. Selain itu, beberapa temuan di bidang ekonomi (informasi sebagai barang publik; dampak jaringan dari infrastruktur informasi dan platform sosial) jelas telah menjadi landasan beberapa norma (misalnya dalam portabilitas data, Pasal 20 GDPR). Selain itu, kami mengamati reaksi terhadap globalisasi dalam distribusi informasi dan penggunaan teknologi informasi, dan dengan demikian perlunya pengaturan di luar batas negara (misalnya dalam

prinsip pasar Pasal 3 ayat 2 GDPR serta beberapa keputusan CJEU, seperti Google Spanyol, 2014).

Berdasarkan beberapa pernyataan umum mengenai undang-undang perlindungan data awal, analisis berikut akan melihat rezim peraturan yang dominan saat ini dalam perlindungan data, yaitu GDPR. Ketika melihat tujuan dan alat peraturan masing-masing, perbandingan dengan rezim peraturan sebelumnya akan dilakukan.

Tujuan Inti Peraturan

Pernyataan GDPR memberikan sejumlah tujuan. Nomor 2 secara eksplisit menyatakan bahwa Peraturan ini dimaksudkan untuk memberikan kontribusi terhadap pencapaian kebebasan, keamanan dan keadilan serta kesatuan ekonomi, kemajuan ekonomi dan sosial, penguatan dan konvergensi perekonomian dalam pasar internal, dan kesejahteraan individu.

Mengingat banyaknya tujuan yang ingin dicapai, dapat dikatakan bahwa dengan mencoba mencapai semuanya, GDPR akan gagal mencapai satupun tujuan. Namun, jika dilihat lebih dekat, kita dapat mengidentifikasi beberapa prinsip inti yang ingin dicapai oleh GDPR dan memang ada upaya besar yang dilakukan GDPR untuk mencapainya.

Perlindungan Data sebagai Perlindungan Demokrasi

GDPR mengidentifikasi kebutuhan regulasi inti mengenai regulasi pentingnya informasi untuk pembagian kekuasaan dan dengan demikian menghindari asimetri kekuasaan berdasarkan informasi. Agar seseorang dapat melaksanakan kebebasannya, kondisi politik, ekonomi, dan sosial harus ditafsirkan sedemikian rupa agar bisa efektif. Jumlah informasi yang ada tentang seseorang, dan dalam kaitannya dengan hal ini, pengetahuan individu tentang informasi yang ada tentang dirinya, menentukan bagaimana mitra bisnis, pemerintah, atau pihak ketiga akan menilai individu tersebut dan mengambil keputusan tentangnya. Seseorang yang tidak menyadari apa yang diketahui tentang dirinya, kehilangan kemungkinan untuk melindungi dirinya sendiri, untuk memberikan informasi tambahan yang bertentangan atau memperkuat apa yang telah diketahui dan untuk melakukan tawar-menawar yang adil. Individu ini tidak akan bisa menilai reaksi dirinya sendiri dan reaksi pihak lain. Pada akhirnya, karena rasa tidak aman dan ketidakpastian, individu mungkin menahan diri untuk tidak menerapkan kebebasannya jika mereka tidak mampu menilai potensi konsekuensinya. Terminologi yang lebih baru menggambarkan hal ini sebagai “efek mengerikan”: Kebebasan dan kebebasan masih ada, namun penerapan fungsinya terhambat oleh keadaan.

Dampak yang mengerikan tidak hanya berdampak pada individu, tetapi juga masyarakat yang bebas dan demokratis. Mahkamah Konstitusi Jerman menyatakan hal ini sejak awal dalam keputusan sensusnya yang inovatif. Masyarakat demokratis hanya bisa ada jika anggotanya bebas berpartisipasi dan bebas menerapkan kebebasannya. Hal ini merupakan suatu lingkungan di mana individu tidak berada di bawah pengawasan negara atau swasta. Perlindungan data kemudian menjadi tulang

punggung masyarakat demokratis dan menjamin peluang untuk benar-benar melaksanakan hak-hak dasar seseorang.

GDPR tidak secara eksplisit menyatakan hubungan antara perlindungan data dan demokrasi secara terbuka. Namun, hal ini terjalin dengan baik dalam teks dan maksud Regulasi. Dalam pernyataan No. 1, Regulasi melihat landasannya yang paling utama dalam perlindungan Art. 8 Piagam UE dan Pasal. 16 Perjanjian tentang Fungsi Uni Eropa (TFEU). GDPR jelas berhubungan dengan DPD, dan meskipun kadang-kadang menimbulkan polemik, GDPR tidak merombak sistem perlindungan data yang ada secara mendasar, melainkan bertujuan untuk memecahkan masalah yang tidak tercakup dalam Petunjuk sebelumnya. Pernyataan No. 5, 6, dan 7 memperjelas bahwa tujuan GDPR bukanlah untuk melonggarkan kendali DPD dalam pemrosesan data, melainkan untuk melanjutkan, memperkuat, dan memperkuat dampaknya.

Namun yang masih belum diketahui adalah sejauh mana pemahaman mengenai perlindungan data sebagai tulang punggung kebebasan dan demokrasi telah diintensifkan dan langkah-langkah yang diambil untuk melindunginya secara lebih efektif akibat perkembangan dalam skala global dibandingkan dengan DPD. Bagaimanapun juga, digitalitas global berasumsi bahwa terdapat dampak terhadap peraturan yang ada akibat peningkatan dan perluasan penggunaan produk, infrastruktur, dan layanan digital.

Yang jelas terlihat adalah pengaruh beberapa peristiwa spektakuler terhadap dorongan regulasi UE untuk memodernisasi perlindungan data—yang paling terkenal adalah terungkapnya skandal NSA di awal tahun 2013, serta keputusan CJEU di Google Spanyol dan Retensi Data. Namun demikian, peristiwa-peristiwa ini terjadi setelah UE memutuskan untuk mereformasi undang-undang perlindungan data pada tahun 2009. Jadi, peristiwa-peristiwa ini telah memperkuat dorongan bahwa ada kebutuhan untuk melindungi individu, dan skandal NSA, Google Spanyol, dan Retensi Data telah mengilustrasikannya seberapa cepat kekuasaan berpindah ke beberapa pemain di pasar dan ke beberapa negara.

Materi mengenai proses reformasi, yang dimulai sebelum peristiwa-peristiwa ini, memperkuat pemahaman bahwa UE melihat adanya perubahan dalam arah dampak awal dan perlunya bereaksi. Hal ini memberikan informasi bahwa UE memang bereaksi terhadap beberapa perubahan yang disebabkan oleh globalisasi digitalisasi: Komisi Eropa menyebutkan beberapa tantangan transfer data dan efisiensi penegakan hukum yang lebih tinggi. Internasionalisasi transfer data dan pemrosesan data, keberadaan dari beberapa pemain global, khususnya di beberapa bidang digitalisasi, dan kebutuhan untuk melindungi diri dari potensi agresor jelas merupakan salah satu alasan untuk mengambil tindakan.

Asimetri Kekuatan

GDPR juga dipicu dalam perspektif yang lebih umum untuk bereaksi terhadap asimetri kekuasaan berdasarkan informasi. Akses terhadap informasi dan akses terhadap teknologi informasi dan komunikasi memungkinkan personalisasi dan

pengetahuan sistematis tentang individu dan keputusan mereka. Seringkali, pengetahuan dan atribusi tentang seseorang ditafsirkan dengan cara dan dengan hasil yang tidak dapat dihasilkan oleh orang-orang tersebut karena mereka kekurangan sumber daya teknologi dan sumber daya lainnya serta akses terhadap hal tersebut. Sebagai konsekuensinya, entitas mana pun yang mampu mengakses data pribadi dan memanfaatkan data tersebut menerima kekuasaan yang tidak dapat disangkal atas individu tersebut. Namun, individu tersebut tidak dapat mengontrol data yang ada tentang dirinya dan akibatnya tentang penilaian atau keputusan apa pun atas dasar ini. Hal ini terutama berlaku karena keputusan biasanya tidak mengungkapkan informasi apa yang digunakan. Badan ini bisa berupa Negara, atau bisa juga badan swasta.

DPD dan permulaan perlindungan data berfokus khususnya pada Negara dan beberapa aktor swasta karena alasan sumber daya. Pemrosesan data otomatis hanya dapat diakses oleh entitas besar dengan sumber daya yang signifikan dan permintaan pemrosesan informasi yang besar. Namun GDPR memperluas perspektif tersebut. Hal ini secara eksplisit menjadikan ketersediaan teknologi informasi di sektor swasta sebagai fokus karena penyebaran alat dan layanan digital yang belum pernah terjadi sebelumnya dan dengan demikian bereaksi terhadap perkembangan teknologi digital.

Meskipun pemrosesan data Negara dikecualikan sampai batas tertentu karena klausul pembukaan Art. 6 para. 1 menyala. c) dan e) GDPR, dalam Art. 2 para. 2 menyala. c) GDPR sepenuhnya memperluas pemrosesan data pribadi apa pun jika bukan hanya karena alasan pribadi atau rumah tangga. Bahkan tinjauan sekilas terhadap ketentuan GDPR menunjukkan bahwa sebagian besar dampak peraturannya telah mengubah fokus dan kini terutama ditujukan kepada pelaku swasta, misalnya, bab baru mengenai sertifikasi hanya berlaku untuk sektor swasta. Banyak penjelasan yang memperjelas bahwa GDPR berfokus pada pemrosesan data pribadi. Misalnya, situasi kontrak sering disebutkan di mana pemrosesan data dilakukan, atau dalam laporan No. 85, spesifikasi daftar risiko potensial adalah situasi yang biasanya terjadi di sektor swasta.

Namun demikian, GDPR juga terus menangani pemrosesan data Negara, dan pengesahan Petunjuk ini secara paralel untuk tujuan pencegahan, investigasi, deteksi, dan lain-lain. GDPR memberlakukan lebih dari sekadar tindakan hukum sederhana UE melainkan merupakan landasan strategi digital yang mana perlindungan data memainkan peran penting—yang ditujukan baik kepada Negara-negara Anggota maupun entitas swasta.

Oleh karena itu, perhatian terhadap undang-undang perlindungan data harus lebih jelas mengintegrasikan perlindungan data terhadap aktor swasta dan negara; globalitas digital telah membawa UE ke pemahaman yang berbeda sehingga menghasilkan rezim peraturan yang lebih fokus terhadap entitas swasta tanpa mengurangi tindakan terhadap aktor negara.

GDPR sebagai Pemersatu

Pernyataan No. 9 menyebutkan alasan lain dari GDPR: GDPR merupakan reaksi terhadap konsekuensi undang-undang perlindungan data yang terfragmentasi dan penegakan hukum yang terfragmentasi di Uni Eropa. Meskipun pada awalnya peraturan pengolahan data terfokus pada pendekatan nasional dan karenanya merupakan hukum nasional individual, DPD menangani khalayak yang lebih luas. Itu menggunakan klausul pasar interior Seni. Perjanjian Komisi Eropa sebelumnya sebagai argumen untuk menciptakan standar perlindungan data serupa di semua Negara Anggota: Pasar internal untuk informasi (yaitu data pribadi) harus diselaraskan. Karena sejumlah negara di Eropa belum memiliki undang-undang perlindungan data pada saat pengesahan DPD, hal ini berarti adopsi dan pengalihan oleh negara-negara yang telah memiliki standar normatif untuk pengambilan keputusan otomatis dan rezim peraturan baru bagi negara-negara tersebut. Negara-negara yang tidak memiliki standar sama sekali.

Globalisasi, pada saat DPD disahkan, tidak begitu penting. Internet belum ada seperti yang kita kenal saat ini, sehingga transfer data dapat dilakukan, namun dengan hambatan teknologi yang jauh lebih tinggi, dan juga dengan sarana dan penerima yang jauh lebih sedikit seperti yang kita kenal sekarang. Pada tahun 1995, perusahaan informasi yang beroperasi di seluruh dunia, terutama yang berkantor pusat di luar negeri, baru saja mulai berkembang.

Namun GDPR mengakui keadaan yang berubah. Laporan No. 6 secara eksplisit menjelaskan bahwa "skala pengumpulan dan pembagian data pribadi telah meningkat secara signifikan", dan bahwa data pribadi kini tersedia secara global. Oleh karena itu, GDPR menyadari bahwa hampir tidak mungkin untuk mengatur pemrosesan data di tingkat nasional dan bahkan peraturan di tingkat supranasional pun menghadapi kesulitan dalam menetapkan standar dan menegakkannya. Distribusi data melalui internet, layanan yang tersedia secara internasional seperti aplikasi, sistem operasi, perangkat keras dan perangkat lunak termasuk infrastruktur telekomunikasi global, dan ketergantungan pada layanan seluler di banyak bidang kehidupan semuanya terjalin dalam satu kesatuan yang saling berhubungan, seringkali (namun belum tentu demikian) jaringan teknologi informasi yang dapat dioperasikan. Dalam sistem ini, data mengalir secara berkala dan terus menerus disimpan, dibagikan, digabungkan kembali, dan diubah. Sebuah peraturan nasional, bahkan supranasional tentu saja mencapai batas kendali karena langkah-langkah pengolahan data yang berbeda tidak harus dilakukan dalam satu rezim peraturan namun diatur oleh pendekatan hukum yang berbeda. Akibatnya, timbul ketidakpastian besar terutama di kalangan pengawas yang taat hukum mengenai peraturan mana yang mengikat mereka dan tingkat perlindungan data apa yang harus mereka jamin. Seringkali, kewajiban saling bertentangan sehingga menimbulkan pilihan antara Scylla dan Charybdis.

Sebagai reaksi terhadap banyaknya pemrosesan data warga negara Eropa yang dilakukan di luar UE, GDPR memperluas cakupan teritorialnya dibandingkan dengan DPD. Aspek GDPR sebagai pemersatu ini akan dibahas nanti di bab tentang cakupan teritorial. Namun, dampaknya lebih dari sekedar perluasan teritorial: Art. 3 para. 2 GDPR juga

memperjelas bahwa UE menganggap standar hukumnya mengikat di seluruh dunia bagi setiap pengontrol. Kita juga dapat menyimpulkan dari standar transfer data di luar UE bahwa GDPR dianggap sebagai standar emas: Meskipun cukup untuk memiliki standar perlindungan yang memadai berdasarkan Art. 44 dst. GDPR untuk memungkinkan data pribadi diproses di luar UE, CJEU telah menjunjung tinggi dan memperkuat keputusannya mengenai kapan kecukupan dapat diasumsikan dengan secara jelas membatalkan apa yang disebut Perjanjian Safe Harbor dan apa yang disebut Perlindungan Privasi. Keduanya perjanjian adalah dasar transfer data transatlantik yang terhenti karena keputusan ini. Sebagai akibat dari semakin kuatnya rasa percaya diri terhadap undang-undang perlindungan data UE, para pelaku internasional pun bereaksi. Dari sudut pandang pihak luar, GDPR memiliki nilai jual yang unik karena merupakan undang-undang perlindungan data yang paling komprehensif dan melindungi warga negara sejauh ini, serta menawarkan salah satu dari sedikit alat untuk menciptakan persaingan yang setara dalam undang-undang informasi. Oleh karena itu, tidak mengherankan jika minat internasional terhadap GDPR sangat besar, dan cukup banyak negara berpengaruh yang mengambil tindakan politik berdasarkan GDPR. Menyebutkan tiga negara besar—California, Jepang, dan Brasil—yang semuanya telah meloloskan peraturan yang terinspirasi dari GDPR dan sering kali mirip, menggambarkan hal ini dengan meyakinkan. Bahkan negara-negara dengan sedikit kepentingan demokratis namun memiliki kepentingan ekonomi yang tinggi dalam melakukan bisnis dengan UE telah melakukan penyesuaian, meskipun hanya bersifat proforma atau hanya terkait dengan sektor swasta dan bukan sektor publik.

> Pada akhirnya, GDPR sejauh ini—dan prosesnya masih dinamis dan belum selesai—telah memulai kembali proses global untuk meningkatkan kesadaran akan perlindungan data. Hal ini bahkan bisa menjadi pemersatu: Di dalam UE, hal ini memang benar adanya, dan secara global kita harus melihatnya.

3.3 INSTRUMENTAL REGULASI UNDANG-UNDANG

Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia, yang mulai berlaku pada tahun 2020, menjadi landasan hukum yang penting dalam mengatur perlindungan data pribadi di negara ini. UU PDP bertujuan untuk melindungi hak individu terkait penggunaan, pengelolaan, dan perlindungan data pribadi mereka. Berikut beberapa poin utama dari UU PDP di Indonesia:

1. **Definisi Data Pribadi**
   UU PDP mendefinisikan data pribadi sebagai informasi tentang individu yang dapat diidentifikasi, baik secara langsung maupun tidak langsung, yang terkait dengan identitas fisik, psikis, keuangan, kesehatan, orientasi seksual, dan lainnya.
2. **Persetujuan Pengguna**
   UU PDP menegaskan bahwa penggunaan data pribadi memerlukan persetujuan dari pemilik data, kecuali dalam beberapa kasus yang diatur dalam undang-undang.
3. **Hak Individu**

UU PDP memberikan hak kepada individu untuk mengakses, mengoreksi, menghapus, atau membatasi penggunaan data pribadi mereka yang dikumpulkan atau diolah oleh pihak lain.

4. **Kewajiban Pengelola Data**
   UU PDP menetapkan kewajiban bagi pengelola data, termasuk organisasi dan individu, untuk melindungi data pribadi, menerapkan tindakan keamanan, dan memberikan laporan jika terjadi pelanggaran keamanan data.
5. **Pengawasan dan Penegakan**
   UU PDP membentuk Badan Pengawas Perlindungan Data Pribadi (PPDP) yang bertugas mengawasi implementasi UU, memberikan sanksi, serta memberikan bimbingan dan konsultasi terkait perlindungan data pribadi.
6. **Pengalihan Data Internasional**
   UU PDP mengatur pemindahan data pribadi ke luar negeri dengan persyaratan tertentu, termasuk mendapatkan persetujuan dari otoritas yang bersangkutan dan memastikan bahwa negara penerima memiliki tingkat perlindungan yang memadai.
7. **Sanksi**
   UU PDP memberikan sanksi administratif dan pidana bagi pelanggaran terhadap ketentuan perlindungan data pribadi, yang bisa berupa denda, penutupan sementara, atau pencabutan izin usaha.

UU PDP di Indonesia adalah langkah penting dalam menjamin perlindungan data pribadi dan mengatur cara pengelolaan data pribadi oleh entitas yang terlibat. Implementasi yang tepat akan menjadi kunci keberhasilan dalam melindungi privasi individu sambil mendukung pertumbuhan teknologi dan ekonomi digital.

Di Eropa, pendekatan GDPR dibandingkan dengan pendekatan peraturan pertama dalam undang-undang perlindungan data telah berubah. Telah disebutkan bahwa peraturan badan swasta (perusahaan, dll.) telah menjadi faktor penting, sementara peraturan negara masih menonjol namun karena kekhasan hukum kompetensi UE, peraturan tersebut tidak begitu menonjol. Perlindungan terhadap kepribadian dan otonomi sebagai tulang punggung demokrasi kini sebagian telah diatur dalam peraturan lain, seperti undang-undang media atau peraturan mengenai ujaran kebencian. Meskipun demikian, perlindungan data masih tetap menjadi alat penting untuk melindungi kebebasan-kebebasan inti ini.

Bab ini akan menggambarkan perubahan dalam dua instrumen peraturan utama: Bab ini menunjukkan bahwa prinsip kehati-hatian dalam beberapa hal dirumuskan ulang menjadi pendekatan berbasis risiko. GDPR juga memperkenalkan pendekatan perlindungan konsumen secara lebih terbuka dan menggunakan undang-undang perlindungan data sebagai alat dan sarana baru untuk mengendalikan pasar yang adil dan perdagangan yang adil.

Prinsip Kehati-hatian versus Pendekatan Berbasis Risiko dan Konsep Netralitas Teknologi

Rezim hukum perlindungan data awal mengikuti pendekatan berbasis hukum teknologi (yaitu prinsip kehati-hatian dan instrumen lain seperti kontrol negara oleh pihak berwenang). Mereka menganut gagasan bahwa segala jenis perlindungan data dapat menimbulkan risiko. Pernyataan Mahkamah Konstitusi Jerman dalam keputusan sensus tahun 1983 yang inovatif adalah sebagai berikut: “Tidak ada data yang tidak relevan”. Oleh

karena itu, DPD menyatakan bahwa segala jenis pengolahan data memerlukan pembenaran; jika tidak, hal itu dianggap ilegal dan tidak memiliki dasar yang sah. Pendekatan ini sering digambarkan dengan menggunakan pendekatan standar hukum dan ketertiban dari hukum administrasi, konsep prinsip pelarangan dengan syarat izin: Suatu kegiatan swasta dilarang, tetapi Negara dapat mengizinkannya. hal ini dilakukan atas dasar sah demi kepentingan hukum tertentu yang lebih unggul, di antaranya kebebasan dan kebebasan individu.

Namun perlu dicatat bahwa penafsiran ini mempunyai beberapa kelemahan sejak awal: Pertama, badan-badan swasta, yang juga ditangani oleh DPD, bertindak berdasarkan prinsip kebebasan. Berbeda dengan Negara, mereka tidak memerlukan pembenaran atas tindakan apa pun, namun justru sebaliknya: Negara harus membenarkan pelanggaran terhadap hak-hak dasar entitas swasta yang jelas-jelas merupakan rezim hukum dan ketertiban. Prinsip pelarangan seperti itu hanya akan mudah diterapkan jika hanya ditujukan kepada Negara, karena hal ini terikat oleh aturan hukum. Oleh karena itu, Negara memerlukan dasar hukum untuk membatasi kebebasan warga negara (yaitu setiap pelanggaran terhadap hak asasi manusia). Namun bagi entitas swasta dan perorangan, prinsip umum pelarangan permintaan izin dari otoritas negara akan dianggap sebagai gangguan besar terhadap kebebasan dasar mereka. Argumen pragmatis yang menentang penafsiran tersebut adalah bahwa DPD tidak pernah mencantumkan prosedur perizinan yang aktif dan lengkap. Hal ini akan mengurangi aktivitas pemrosesan data seminimal mungkin, dan tidak ada rezim hukum perlindungan data yang ada pada masa awal (dan juga saat ini) yang menginginkan hal ini.

Namun benar bahwa persyaratan pembenaran yang baru yang ditetapkan oleh DPD mengubah pendekatan umum terhadap pengolahan data. Kini, badan-badan swasta dan negara-negara harus mengendalikan kegiatan-kegiatan mereka dan melakukan tes terlebih dahulu (ex ante) untuk mengetahui apakah pengolahan data mereka legal menurut DPD dan apakah proses transposisi menjadi undang-undang dilakukan oleh negara-negara anggota. Karena penerapan DPD bersifat luas (“data pribadi apa pun”), hal ini berarti diperlukan upaya besar dari pihak pengolah data. Perlunya tindakan preventif ini semakin diperparah dengan fakta bahwa DPD tidak membedakan jenis pengolahan data tertentu atau memberikan keistimewaan terhadap pengolahan data tertentu. Sebaliknya, “netralitas teknologi” adalah strategi peraturan yang dinyatakan: DPD dirancang agar dapat diterapkan pada pemrosesan data apa pun secara umum, karena kemungkinan laten dari rekombinasi data merupakan ancaman terus-menerus terhadap data apa pun.

GDPR secara umum menjunjung pendekatan ini namun tidak menerapkan pendekatan ini seketat DPD. Sebaliknya, GDPR telah memasukkan sejumlah ketentuan yang berasumsi bahwa ada jenis pemrosesan data tertentu yang dapat dianggap lebih berisiko dibandingkan dengan DPD. orang lain sehubungan dengan konsep perlindungan data. Di sini, pendekatan yang lebih berbasis risiko dapat diidentifikasi, meskipun pendekatan tersebut belum sepenuhnya diambil alih dalam GDPR. Sebagai konsekuensinya, akan ada perkembangan di tahun-tahun mendatang di mana operasi yang lebih berisiko akan

dikendalikan dan diatur lebih lanjut sementara jenis-jenis lainnya pemrosesan data tidak akan mendapatkan banyak perhatian dari pengontrol dan otoritas pengawas.

Salah satu ketentuan yang menggambarkan pendekatan berbasis risiko tambahan dapat ditemukan dalam Art. GDPR, yang disebut dengan "penilaian dampak perlindungan data". Pasal 35 memperkenalkan sebuah instrumen untuk peringatan dini, yang mana pengontrol diharuskan menilai risiko suatu pemrosesan data dan sebagai konsekuensinya secara proaktif melakukan tindakan untuk mengurangi risiko tersebut. Pengendali mungkin juga harus berkonsultasi dengan otoritas pengawas. Pasal 35 ayat. 3 GDPR menyebutkan sejumlah jenis pemrosesan data yang dianggap berisiko tinggi, di antaranya pembuatan profil (lit. a)) atau pemrosesan data sehubungan dengan kategori data khusus (lit. b)). Pasal 35 ayat. 4 GDPR juga mewajibkan otoritas pengawas menerbitkan daftar jenis pemrosesan data yang termasuk dalam kewajiban menjalani Art. 35 Penilaian risiko GDPR. Pihak berwenang juga diaktifkan oleh Art. 35 ayat. 5 GDPR akan menerbitkan daftar jenis pemrosesan yang setara dan tidak dianggap berisiko dalam pengertian Seni. 35 ayat. 1 GDPR. Daftar ini tidak hanya merinci kewajiban pengontrol sehubungan dengan aktivitas yang terdaftar, namun juga berfungsi sebagai contoh untuk interpretasi jenis pemrosesan lain yang tidak terdaftar.

Definisi hukum atas jenis pemrosesan data berisiko tertentu, serta kemungkinan untuk mendefinisikan aktivitas sebagai tidak berisiko, menyimpang dari prinsip awal yang menyatakan bahwa keadaan ringkaslah yang menghasilkan risiko terhadap kebebasan dan kebebasan individu, dan dengan demikian data apa pun. pemrosesan harus dinilai secara individual. Di bawah Seni. Namun GDPR, pengontrol yang tepat, tujuan yang ringkas, dan teknologi pemrosesan data yang spesifik kini hanya menjadi penting setelah ambang batas penilaian risiko telah dilakukan.

UU Perlindungan Data sebagai UU Perlindungan Konsumen dan Persaingan Sehat

Undang-Undang Perlindungan Data (UU PDP) sering kali dianggap sebagai salah satu aspek dari perlindungan konsumen, terutama karena fokusnya pada melindungi data pribadi individu. Perlindungan konsumen dan perlindungan data pribadi memiliki hubungan erat, dan keberadaan UU PDP dapat dianggap sebagai upaya untuk memberikan perlindungan lebih lanjut terhadap hak-hak konsumen. Berikut adalah beberapa cara di mana UU PDP dapat dianggap sebagai bagian dari kerangka perlindungan konsumen:

1. Privasi dan Kontrol Individu:

- UU PDP memberikan hak-hak kepada individu untuk melindungi privasi mereka dan mengendalikan bagaimana data pribadi mereka dikumpulkan, disimpan, dan digunakan. Ini sejalan dengan hak konsumen untuk memiliki kendali atas informasi pribadi mereka.

2. Persetujuan Pengguna:

- Prinsip persetujuan pengguna dalam UU PDP mencerminkan konsep persetujuan informasi dari konsumen. Pengguna memiliki hak untuk mengetahui dan memberikan izin terhadap pengumpulan dan penggunaan data pribadi mereka.

3. Hak Akses dan Koreksi:

- UU PDP memberikan hak kepada individu untuk mengakses informasi yang dikumpulkan tentang mereka dan memberikan kesempatan untuk mengoreksi atau menghapus informasi yang tidak akurat. Ini mencerminkan hak konsumen untuk memahami dan mengendalikan informasi yang berkaitan dengan mereka.

4. Transparansi:

- UU PDP mendorong transparansi dalam praktik pengelolaan data pribadi. Konsep ini mencocokkan dengan prinsip perlindungan konsumen untuk memberikan informasi yang jelas dan dapat dimengerti kepada konsumen.

5. Perlindungan Terhadap Penyalahgunaan Data:

- Melalui ketentuan-ketentuannya, UU PDP bertujuan untuk mencegah penyalahgunaan data pribadi, sehingga melindungi konsumen dari risiko potensial seperti pencurian identitas atau penggunaan data yang tidak sah.

6. Sanksi dan Penegakan:

- UU PDP menyertakan sanksi dan penegakan hukum untuk melindungi hak-hak individu. Ini dapat mencakup denda dan tindakan hukum yang dapat diambil terhadap pelanggaran, yang dapat membantu melindungi konsumen dari praktik yang tidak etis.

Dengan demikian, UU PDP dapat dipandang sebagai instrumen perlindungan konsumen yang melibatkan aspek-aspek khusus terkait privasi dan pengelolaan data pribadi. Dalam era digital, di mana pengumpulan dan penggunaan data semakin meluas, perlindungan data pribadi menjadi semakin penting dalam menjaga hak-hak konsumen.

Perubahan pada pendekatan peraturan inti juga dapat diidentifikasi sehubungan dengan rezim peraturan dan tujuan peraturan undang-undang perlindungan data UE. DPD pada awalnya merupakan alat pengaturan teknologi yang bertujuan untuk mengendalikan teknologi yang sedang berkembang. Prinsip ini menggunakan instrumen-instrumen yang khas, dengan prinsip kehati-hatian yang paling menonjol, antara lain dengan menetapkan rezim peraturan ex ante dan otoritas pengawas. Pengendali diwajibkan untuk menguji aktivitas pemrosesan data mereka sebelum melaksanakannya: Pada tingkat dasar, pengontrol mempunyai kewajiban untuk membatasi aktivitas mereka. GDPR adalah inti dari pemahaman ini. DPD tidak membedakan kelompok aktor yang berbeda selain antara pengendali data (termasuk pengolah data) dan subjek data. Subyek data sendiri dianggap terjebak dalam asimetri kekuatan informasi dibandingkan dengan pengontrol data. Keadaan khusus di mana hal ini terjadi asimetri kekuasaan yang muncul bukanlah bagian dari rancangan peraturan.

Hal ini berbeda dengan GDPR—setidaknya beberapa ketentuan mengidentifikasi berbagai subkelompok situasi yang layak dilindungi. Unsur-unsur undang-undang perlindungan konsumen dan undang-undang persaingan telah diperkenalkan, yang paling menonjol dalam ketentuan Art. 20 GDPR mengenai hak atas portabilitas data. Mayoritas arahan UE saat ini mendefinisikan konsumen sebagai “orang perorangan yang bertindak untuk tujuan di luar perdagangan, bisnis, dan profesinya”. Undang-undang perlindungan konsumen membahas masalah mendasar, sebagian besar dalam situasi kontrak: Konsumen sering kali berada dalam situasi di mana mereka tidak melakukan tawar-menawar secara

setara, terutama dengan perusahaan dan industri besar dalam transaksi bisnis. Transaksi-transaksi ini biasanya menyangkut kehidupan pribadi mereka, namun pada dasarnya mereka dirugikan. Oleh karena itu, undang-undang perlindungan konsumen bertujuan untuk melindungi konsumen dari risiko dan ancaman serius yang tidak dapat mereka atasi sebagai individu; dalam memberdayakan mereka untuk membuat pilihan berdasarkan informasi yang akurat, jelas dan konsisten; dan terakhir, meningkatkan kesejahteraan mereka dan secara efektif melindungi keselamatan serta kepentingan ekonomi mereka. UE memiliki tradisi lama dalam melindungi kepentingan konsumen.

Meskipun GDPR tidak secara eksplisit menyebutkan "konsumen" sebagai subkelompok subjek data, tujuan inti dari perlindungan data untuk mengatasi asimetri kekuatan informasi dan undang-undang perlindungan konsumen untuk melawan asimetri kekuatan di pasar pada dasarnya saling terkait erat. Hal ini berlaku meskipun undang-undang perlindungan data tidak menjadikan dampak ekonomi sebagai titik awal seperti halnya undang-undang perlindungan konsumen. Oleh karena itu, penerapan undang-undang perlindungan data lebih luas karena memperhitungkan dampak asimetri kekuatan informasi pada semua jenis keputusan. Namun demikian, beberapa instrumen undang-undang perlindungan data dapat diamati serupa dalam undang-undang perlindungan konsumen, khususnya memperkuat kontrol organisasi terhadap kondisi, membantu konsumen/subjek data untuk membuat pilihan yang lebih baik dan secara efektif memperjuangkan hak-hak mereka terhadap praktik tidak adil. Oleh karena itu, tidak mengherankan jika otoritas pengawas telah mengidentifikasi hubungan antara perlindungan data dan perlindungan konsumen sebelum berlakunya GDPR.

"Efek lock-in" menciptakan hambatan terhadap persaingan yang efektif; hal ini menciptakan beban yang tinggi pada masuknya pasar. Sebagai tindakan balasan, Art. 20 GDPR secara aktif menghubungkan undang-undang perlindungan data dengan undang-undang persaingan usaha. Pembahasan mengenai hubungan antara kedua rezim peraturan hukum tersebut—setidaknya di Jerman dan Eropa—sejauh ini lebih banyak dibahas dari sisi hukum persaingan usaha. Yang paling menonjol, masalah ini diangkat oleh Kantor Kartel Federal (Bundeskartellamt), otoritas persaingan tertinggi di Jerman: Dalam keputusan melawan Facebook, mereka menggunakan dampak undang-undang perlindungan data sebagai argumen inti untuk aturan yang melarang praktik perusahaan dalam menggabungkan kembali pengguna. data dari berbagai sumber di dalam dan di luar grup perusahaan. Undang-undang perlindungan data yang bertujuan untuk memberikan perlindungan paling efektif terhadap hak-hak subjek data tidak menghalangi perlindungan tambahan dari rezim hukum lainnya. Pernyataan 146 GDPR dengan demikian menyatakan bahwa tanggung jawab perlindungan data ada "tanpa mengurangi klaim atas kerusakan apa pun yang berasal dari pelanggaran aturan lain dalam undang-undang Persatuan atau Negara Anggota".

Perluasan rezim peraturan yang mengarah pada perlindungan konsumen tambahan dapat diidentifikasi sebagai reaksi terhadap digitalitas global: Perusahaan IT yang beroperasi

secara internasional telah memperbesar asimetri kekuasaan tidak hanya terhadap subjek data secara umum, namun juga dalam hubungan konsumen pada khususnya.

3.4 PERATURAN ISI

Setelah menguraikan prinsip-prinsip umum, pendekatan peraturan, dan tujuan inti GDPR sejauh ini, dapat dikatakan bahwa undang-undang perlindungan data UE yang baru telah memperluas konsep perlindungan data dalam kondisi global. Peninjauan lebih lanjut terhadap tindakan-tindakan tertentu dalam masing-masing ketentuan GDPR akan menunjukkan reaksi lebih lanjut secara rinci.

Defisit Penegakan

Salah satu dorongan dari pihak UE untuk mereformasi rezim peraturan perlindungan data yang ada adalah keinginan untuk menegakkan status hukum yang lebih harmonis, bahkan mungkin terpadu, terhadap status hukum yang ada dibandingkan dengan DPD. Seiring berjalannya waktu , menjadi jelas bahwa, khususnya, mekanisme penegakan hukum yang diberikan oleh DPD dan transposisi menjadi undang-undang oleh Negara-negara Anggota tidak cukup untuk melaksanakan ketentuan yang melindungi data pribadi secara efektif.

Ada banyak alasan untuk hal ini. Tidak jelas tugas, kompetensi dan wewenang apa yang dimiliki oleh otoritas pengawas. Beberapa pihak dan negara yang terlibat berpandangan bahwa DPD tidak memberikan kewenangan kepada pengawas untuk menetapkan peraturan tertentu dan menegakkannya; Negara-negara Anggota lainnya telah memiliki kompetensi dan wewenang yang luas. Hal ini, serta tradisi, pemahaman dan penafsiran yang berbeda, menyebabkan perbedaan penilaian dan keputusan otoritas pengawas di Negara-negara Anggota mengenai jenis pemrosesan data yang serupa atau bahkan sama. Hal ini menciptakan ketidakpastian dan mengurangi efektivitas penegakan hukum. Dampak ini semakin intensif di tingkat internasional karena dampak “belanja hukum perlindungan data”, khususnya oleh perusahaan-perusahaan besar dan beroperasi secara internasional dalam rangka mencari interpretasi minimal dari Negara Anggota terhadap DPD. Khususnya, perusahaan-perusahaan informasi internasional yang besar telah mendorong penegakan hukum dan kerja sama antar otoritas pengawas hingga batasnya. Mereka telah merancang struktur perusahaan dan teknis untuk menghindari penerapan DPD atau hanya pemrosesan data terbatas yang berada di bawah rezim Negara Anggota dan yurisdiksi DPD.

Fakta terakhir ini khususnya terkait langsung dengan dampak digitalitas global: Karena sebagian besar layanan digital ditawarkan secara internasional dan perusahaan-perusahaan terpenting berkantor pusat di luar UE, defisit penegakan hukum juga merupakan akibat langsung dari globalisasi, yang sebagian besar merupakan dampak dari digitalisasi global. sistem digitalisasi berbasis internet. Hal ini juga terkait langsung dengan penerapan undang-undang perlindungan data DPD dan Negara Anggota.

Selain itu, pelanggaran terhadap undang-undang DPD dan Negara Anggota sering kali sulit dikenai sanksi. Misalnya, di Jerman, tanggung jawab atas pelanggaran undang-undang perlindungan data pada kenyataannya tidak ada, karena undang-undang Jerman pada

umumnya hanya memperbolehkan pemulihan atas kerugian material dan oleh karena itu biasanya tidak memberikan ganti rugi yang efektif kepada subjek data atas pelanggaran hak kepribadian atau informasi. Kemungkinan untuk mengenakan denda sering kali dibatasi di Negara-negara Anggota. Oleh karena itu, undang-undang sekunder sering kali tidak mempunyai pengaruh yang mengatur untuk secara efektif memberikan sanksi kepada pelanggar.

Sebagai reaksi terhadap masalah hukum ini, GDPR melakukan upaya reformasi yang besar untuk memberikan penegakan hukum yang efektif. Efisiensi otoritas pengawas telah diperkuat dan kompetensi serta wewenang mereka telah dinyatakan dengan jelas dalam daftar Art. 55 dan seterusnya. GDPR. Untuk menyatukan penilaian jenis pemrosesan data, Dewan Perlindungan Data Eropa (EDPB) meresmikan gagasan Art. 29 Kelompok Kerja di bawah DPD. Mekanisme konsistensi, Art. 63 dan seterusnya, bersamaan dengan pembentukan badan pengawas yang terkemuka, menetapkan suatu prosedur yang memungkinkan pengambilan keputusan yang mengikat antar lembaga yang berbeda dan dalam beberapa hal bahkan bersifat wajib.

Untuk mendeteksi pelanggaran perlindungan data secara efektif, hak subjek data telah diperluas dibandingkan dengan DPD, dan dalam Art. 12 dan seterusnya. Hak informasi GDPR telah dijelaskan dengan lebih tepat. Kerugian, termasuk kerugian non-materiil, kini secara eksplisit diatur dalam Art. 82 ayat. 1 GDPR. Juga, Art. 80 GDPR baru menyediakan representasi subjek data dalam prosedur penegakan hukum yang mirip dengan tindakan perwakilan.

Perlu juga dicatat bahwa kewajiban terkait penegakan hukum juga diperkuat dengan kewajiban untuk menunjukkan legalitas sebagaimana tercantum dalam Pasal baru. 24 ayat. 1 GDPR: Hal ini mengharuskan setiap pengontrol untuk mendokumentasikan dengan benar bahwa setiap pemrosesan dilakukan sesuai dengan GDPR. Dengan demikian, bahkan potensi masalah prosedural pun dapat diatasi.

Ruang Lingkup Teritorial

Ruang lingkup teritorial dalam Undang-Undang Perlindungan Data Pribadi (UU PDP) mengatur wilayah geografis atau cakupan hukum di mana undang-undang tersebut berlaku dan di mana organisasi atau entitas yang mengelola data pribadi wajib mematuhi regulasinya. Berikut adalah beberapa prinsip umum dalam ruang lingkup teritorial UU PDP:

1. **Domisili Pengelola Data:**
    - Biasanya, UU PDP akan berlaku untuk organisasi atau entitas yang berdomisili atau beroperasi di wilayah yurisdiksi yang mengeluarkan undang-undang tersebut. Artinya, jika suatu organisasi memiliki keterkaitan dengan wilayah tersebut, baik berupa kantor cabang, pusat data, atau operasi bisnis lainnya, maka UU PDP dapat diterapkan.
2. **Pengumpulan Data di Wilayah Tersebut:**
    - Jika suatu organisasi, meskipun berdomisili di luar yurisdiksi tertentu, mengumpulkan data dari individu yang berada di wilayah tersebut, maka UU PDP dapat berlaku untuk organisasi tersebut. Hal ini menunjukkan ekstrateritorialitas undang-undang perlindungan data.

3. **Pemindahan Data Internasional:**
    - UU PDP sering kali mengatur pemindahan data pribadi ke luar negeri. Hal ini dapat mencakup persyaratan khusus atau persetujuan yang diperlukan untuk mentransfer data ke negara atau wilayah tertentu.
4. **Pengaruh Globalisasi Digital:**
    - Dalam era globalisasi digital, beberapa UU PDP mungkin memiliki ketentuan yang mengakui pengaruh global dan melibatkan organisasi yang, meskipun tidak berdomisili di dalam yurisdiksi tersebut, tetapi memiliki dampak signifikan pada individu yang berada di wilayah tersebut.
5. **Penentuan Residensi Data Subyek:**
    - Beberapa undang-undang mungkin juga mempertimbangkan tempat tinggal atau kediaman data subyek sebagai faktor yang menentukan dalam menerapkan UU PDP. Jika data subyek berada di dalam yurisdiksi tertentu, maka UU PDP di wilayah tersebut dapat berlaku.

Penting untuk dicatat bahwa setiap undang-undang perlindungan data memiliki ketentuan tersendiri terkait ruang lingkup teritorialnya. Prinsip-prinsip tersebut dapat bervariasi antara negara dan wilayah, dan organisasi yang beroperasi secara global perlu memahami dan mematuhi ketentuan-ketentuan dari berbagai yurisdiksi yang relevan. Selain itu, implementasi UU PDP juga dapat melibatkan kerjasama internasional dan upaya bersama untuk mengatasi tantangan perlindungan data pribadi di era digital global.

Salah satu aspek penting dari masalah kurangnya penegakan hukum yang ketat dan dapat diperkirakan adalah pembatasan sebagian besar cakupan teritorial undang-undang perlindungan data di UE. DPD menganut prinsip teritorialitas, yaitu setiap—tetapi hanya satu-satunya—pemrosesan data yang terjadi di UE diatur berdasarkan undang-undang UE. Prinsip ini juga dibarengi dengan prinsip pendirian, yaitu setiap pengolahan data yang dilakukan dalam rangka kegiatan suatu pendirian di UE harus bertindak sesuai dengan DPD dan transposisi menjadi undang-undang oleh Negara Anggota.

Namun, hal ini terbukti menjadi masalah dalam semua kasus ketika subjek data menawarkan datanya kepada pengawas di luar UE yang tidak mempunyai kantor di UE. Oleh karena itu, banyak pengawas internasional yang mendirikan perusahaan di dalam UE sebagai tempat melakukan aktivitas pemasaran dan bisnis, namun pemrosesan data inti dilakukan di luar UE. Dengan pendekatan ini, banyak perusahaan internasional dapat menghindari dampak regulasi dari undang-undang perlindungan data UE.

GDPR bereaksi terhadap perkembangan ini dengan mengabaikan prinsip teritorial dan memilih apa yang disebut “aturan pasar”, Art. 3 para. 2 GDPR. Aturan pasar membuat undang-undang UE berlaku bagi siapa pun yang menawarkan barang atau jasa kepada individu di UE—terlepas dari kewajiban keuangan atau kontrak yang terlibat—atau memantau perilaku orang-orang di UE. Dengan demikian, teritorialitas maupun pendirian tidak bersifat wajib, sehingga hubungan material dengan UE dalam pemrosesan tidak lagi diperlukan.

Perubahan ini sangat penting mengingat dampak digitalitas global, dan hal ini terjadi karena dua alasan. Alasan pertama adalah alasan yang jelas: GDPR, berbeda dengan DPD,

kini berlaku untuk pemrosesan data apa pun yang menangani individu di UE sehingga menyimpang dari prinsip teritorial sebelumnya. Kini tidak perlu lagi membuktikan pemrosesan data di UE untuk meminta perlindungan dari GDPR.

Aspek kedua yang diungkapkan oleh Seni baru ini. 3 para. 2 GDPR merupakan perkembangan luar biasa dalam penanganan barang dan layanan digital. Dengan menerapkan prinsip pasar, pembuat undang-undang menyejajarkan penerapan undang-undang UE sehubungan dengan barang dan jasa virtual serta dampaknya dengan barang dan jasa non-virtual. Keduanya kini mengikuti peraturan hukum bahwa apa pun—produk material maupun layanan virtual—yang masuk ke UE harus mematuhi standar UE: Mobil AS harus memenuhi semua persyaratan peraturan produk dan keselamatan UE; hal serupa kini terjadi pada layanan online apa pun yang ditawarkan kepada seseorang di UE.

Oleh karena itu, kita dapat mengamati adanya pergeseran di pihak UE untuk tidak hanya menguasai pasarnya sendiri namun juga bereaksi terhadap perusahaan-perusahaan internasional yang telah berhasil menaklukkan wilayah layanan dan barang digital—sebuah aspek yang tidak menjadi komitmen UE dalam hal ini.

GDPR secara aktif berupaya untuk mengatasi defisit penegakan hukum yang timbul pada masa DPD. Seperti yang diilustrasikan, sejumlah alat telah dipilih untuk tidak hanya merumuskan standar material namun juga untuk memastikan bahwa standar tersebut mengikat dan ditegakkan. Namun, ada satu aspek yang tidak ditangani oleh GDPR dan dengan demikian terus mengikuti arahan DPD adalah "penegakan penegakan hukum" (yaitu bagaimana memastikan bahwa tindakan apa pun yang wajib diambil oleh pengontrol benar-benar dilakukan. Selain itu, instrumen mengenai cara menegakkan sanksi dalam bentuk apa pun masih kurang, terutama denda dan ganti rugi.

Di sini, GDPR terus bergantung pada ketentuan hukum umum (yaitu hak akses dan informasi, dll.), hukum prosedur dan penegakan hukum internasional secara umum dan Negara Anggota, serta tempat penegakan hukum yang telah ditetapkan (yaitu pengadilan dan kemudian lembaga penegakan hukum). Namun hal ini berarti bahwa instrumen GDPR mana pun, yang memerlukan penegakan atau kontrol lebih lanjut, juga akan mengalami kesulitan yang sama seperti yang terjadi di bidang hukum lainnya. Hukum internasionallah yang mengatur sejauh mana entitas yang beroperasi secara internasional dapat dipaksa untuk mematuhi peraturan di UE.

3.5 REGULASI INTERNET

Januari 2022, di Indonesia, regulasi internet terkait dengan berbagai aspek, termasuk keamanan, privasi, dan konten, diatur oleh beberapa undang-undang dan peraturan pemerintah. Berikut adalah beberapa regulasi internet utama di Indonesia:

1. **Undang-Undang Informasi dan Transaksi Elektronik (UU ITE):**
    - UU ITE (Undang-Undang Nomor 19 Tahun 2016) merupakan regulasi yang mengatur berbagai aspek terkait transaksi elektronik, termasuk keamanan dan privasi data. UU ini juga mencakup ketentuan-ketentuan terkait dengan tindakan kriminal yang melibatkan penggunaan teknologi informasi.
2. **Peraturan Pemerintah Pengganti UU ITE (Perppu ITE):**

- Perppu ITE merupakan peraturan pemerintah yang dikeluarkan untuk merevisi beberapa pasal dalam UU ITE. Perppu ITE telah mengalami beberapa kali revisi dan menjadi sorotan karena dituduh dapat mengancam kebebasan berbicara.

3. **Peraturan Menteri Komunikasi dan Informatika (Permennkominfo):**
    - Beberapa Permennkominfo dikeluarkan untuk mengatur aspek-aspek tertentu dalam penggunaan internet. Misalnya, Permennkominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik mengatur perlindungan data pribadi di Indonesia.
4. **Undang-Undang Perlindungan Anak:**
    - Undang-Undang Nomor 35 Tahun 2014 tentang Perlindungan Anak mencakup ketentuan terkait dengan perlindungan anak di internet dan penggunaan teknologi informasi yang melibatkan anak-anak.
5. **Undang-Undang Hak Cipta:**
    - Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta mengatur hak dan kewajiban terkait dengan konten digital dan perlindungan hak cipta di dunia maya.
6. **Ketentuan Mengenai Konten Pornografi:**
    - Ada ketentuan-ketentuan khusus yang mengatur konten pornografi di internet. Hal ini termasuk dalam UU ITE dan peraturan terpisah yang mengatur larangan dan sanksi terhadap konten pornografi.
7. **Pengawasan oleh Badan Regulasi Telekomunikasi Indonesia (BRTI) dan Kementerian Komunikasi dan Informatika (Kominfo):**
    - BRTI dan Kominfo memiliki peran dalam mengawasi dan mengatur penggunaan internet di Indonesia. Mereka memiliki kewenangan untuk memantau dan mengambil tindakan terhadap konten yang dianggap melanggar regulasi.

Penting untuk diingat bahwa regulasi di bidang internet dapat berubah seiring waktu, dan perubahan dapat terjadi setelah tanggal pengetahuan saya pada Januari 2022. Oleh karena itu, untuk informasi yang paling akurat dan terkini, disarankan untuk merujuk pada dokumen resmi dan sumber informasi yang dikeluarkan oleh pemerintah Indonesia.

Hanya akan disinggung secara singkat bahwa GDPR juga tidak menangani internet dan masalah spesifiknya terkait perlindungan data secara eksplisit. Banyaknya perangkat peraturan baru yang jelas merupakan reaksi terhadap perkembangan internet dan keberadaannya di mana-mana. Namun, pendekatan yang netral terhadap teknologi dalam Peraturan ini mungkin paling baik dilihat dari penolakan untuk menyatakan peraturan konten tertentu.

Betapa sulitnya mencapai pemahaman bersama dalam hal ini dapat dilihat dari perdebatan yang belum selesai mengenai Peraturan ePrivasi baru, yang dimaksudkan untuk menyediakan peraturan khusus internet berdasarkan GDPR. Meskipun banyak upaya yang dilakukan oleh beberapa presiden di UE, sejauh ini belum ada kompromi yang tercapai. Jadi, GDPR tetap menjadi inti perlindungan data tanpa membahas kekhususan regulasi internet. Di sini, digitalitas global telah hadir dalam teori, namun tidak dalam praktik.

Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia memberikan sanksi untuk pelanggaran penggunaan data guna mendorong kepatuhan terhadap aturan-aturan perlindungan data pribadi. Beberapa sanksi yang dapat diberikan menurut UU PDP Indonesia termasuk:

1. **Sanksi Administratif:**
    - Denda administratif dapat diberikan kepada pelaku usaha yang melanggar ketentuan UU PDP. Besaran denda ini dapat bervariasi tergantung pada jenis pelanggaran yang dilakukan.
2. **Penutupan Sementara:**
    - Otoritas Pengawas Perlindungan Data Pribadi (PPDP) memiliki kewenangan untuk memberikan sanksi penutupan sementara terhadap pelaku usaha yang melanggar UU PDP.
3. **Pencabutan Izin Usaha:**
    - Jika pelaku usaha tidak mematuhi ketentuan UU PDP secara berulang, PPDP dapat mencabut izin usahanya.
4. **Pemberitahuan Pelanggaran Keamanan Data:**
    - Jika terjadi pelanggaran keamanan data yang dapat membahayakan privasi individu, pelaku usaha wajib memberikan pemberitahuan kepada otoritas dan individu yang terkena dampak.
5. **Penuntutan Pidana:**
    - UU PDP memberikan dasar hukum bagi penegakan pidana dalam kasus pelanggaran yang serius. Ini dapat mencakup hukuman pidana bagi pelaku usaha atau individu yang sengaja atau kelalaian melanggar ketentuan UU PDP.

Sanksi ini dimaksudkan untuk memberikan insentif kepada organisasi dan individu untuk mematuhi ketentuan perlindungan data pribadi, serta untuk memberikan perlindungan yang lebih baik terhadap privasi individu. Otoritas pengawas, seperti PPDP, memiliki peran penting dalam mengawasi implementasi UU PDP dan memberikan sanksi jika ditemukan pelanggaran.

Penting untuk diingat bahwa sanksi yang diberlakukan dapat bervariasi tergantung pada tingkat pelanggaran, dampaknya terhadap privasi individu, dan faktor-faktor lain yang relevan. Oleh karena itu, kepatuhan terhadap UU PDP dan peraturan perlindungan data pribadi lainnya menjadi hal yang krusial bagi organisasi dan entitas yang mengelola data pribadi.

3.6 KESIMPULAN DAN PANDANGAN

Kesimpulan dari analisis pertama dan singkat ini, yang dibatasi pada beberapa gagasan dan instrumen umum dalam undang-undang perlindungan data UE, adalah sebagai berikut: Undang-undang perlindungan data belum berubah menjadi undang-undang “baru” seiring dengan meningkatnya digitalitas global. Sebaliknya, kita dapat melihat bidang ini sebagai bidang hukum yang dinamis dan telah menyesuaikan diri dengan perkembangan selama 30 tahun terakhir dan khususnya dengan meningkatnya operasi internasional di bidang teknologi informasi. Namun, kedaulatan dan hukum internasional mempunyai

dampak buruknya: UE telah memperluas pendekatan hukum substantifnya dan penegakan hukum secara langsung melalui beberapa instrumen, namun bukan “penegakan penegakan hukum” yang sebenarnya. Secara keseluruhan, undang-undang perlindungan data masih merupakan undang-undang informasi paling komprehensif yang pernah ada—dan GDPR, mengikuti jejak DPD, merupakan alat yang ampuh untuk mengatur digitalitas juga dalam skala global. Hal ini terjadi karena karakter modelnya, yang mulai diselaraskan oleh banyak negara di seluruh dunia ketika mengintensifkan upaya perlindungan data mereka sendiri.

BAB 4
PRIVASI DATA DAN MASYARAKAT SEBAGAI KOMODITAS

4.1 PENDAHULUAN

Mencapai konsensus global mengenai cara terbaik untuk melindungi data pribadi akan menjadi upaya yang sangat sulit jika Amerika Serikat ingin memainkan peran penting dalam proyek ini untuk memajukan digitalitas global. Seperti yang akan dijelaskan dalam ba b ini, alasannya adalah karena faktor hukum dan budaya. Undang-undang AS, di tingkat federal, tidak memberikan perlindungan hukum yang kuat terhadap penentuan nasib sendiri berdasarkan informasi dan hanya menawarkan perlindungan konstitusional terbatas terhadap informasi pribadi yang bersifat rahasia.

Keadaan hukum ini, pada gilirannya, mencerminkan fakta budaya yang lebih luas di AS, sebagian besar warga negara tidak terlalu peduli dalam melakukan kontrol atas informasi pribadi mereka (termasuk bagaimana informasi tersebut dikumpulkan, disimpan, dan dikomodifikasi). Di Sebaliknya di Eropa, masyarakat awam sangat khawatir mengenai penerapan otonomi dan kontrol atas data pribadi mereka dan baik politisi maupun birokrat telah menanggapi kekhawatiran yang meluas dan mendalam mengenai privasi informasi. Undang-undang AS saat ini tidak menerapkan generalisasi apa pun. perlindungan data pribadi di tingkat federal. Sejauh data pribadi mendapat perlindungan hukum di tingkat federal, perlindungan ini, paling banter, tidak lengkap dan tersebar.

Bahkan ada yang bisa mengatakan bahwa perlindungan data pribadi di AS seperti keju Swiss karena perlindungan tersebut penuh dengan “lubang” atau kesenjangan dalam cakupannya. Seperti yang dijelaskan oleh Profesor Daniel Solove, seorang pakar hukum privasi Amerika yang terkemuka, “undang-undang privasi federal membentuk peraturan yang rumit dan memiliki kesenjangan dan kelalaian yang signifikan.” Undang-undang privasi juga sebagian besar bersifat reaktif dibandingkan proaktif di AS. Daripada berpikir secara holistik tentang apa yang dibutuhkan oleh kebijakan privasi yang masuk akal di tingkat nasional, Kongres cenderung menggunakan kewenangan Klausul Perdagangan6 untuk melindungi privasi dalam konteks yang sangat spesifik seringkali setelah undang-undang tersebut disahkan. tidak adanya privasi data dalam konteks tertentu, seperti yang berkaitan dengan rekaman video rental seseorang atau data SIM, menjadi wacana nasional.8 Hasilnya adalah kebijakan yang tidak harmonis dan tidak koheren dengan subjeknya. diatur atau keterkaitan peraturan perundang-undangan yang satu dengan yang lain. Terlebih lagi, pendekatan bunga rampai ini tidak terlalu efektif dalam mengamankan data pribadi. Seperti yang dikeluhkan Profesor Colin Bennett, “mungkin terdapat banyak undang-undang, namun tidak banyak perlindungan.”

Permasalahan hukum dan budaya yang perlu diatasi agar AS dapat berpartisipasi dalam pengembangan hukum privasi data global bahkan lebih luas dan lebih mengakar dibandingkan ketidakpedulian sosial terhadap penentuan nasib sendiri berdasarkan informasi. Konstitusi AS, yang mencakup jaminan kebebasan berpendapat yang ditafsirkan

secara luas, akan menimbulkan hambatan besar terhadap penerapan dan penegakan batasan pengumpulan, penyimpanan, dan penggunaan data pribadi yang dimiliki oleh entitas seperti Facebook, Google, dan Twitter. Bahkan jika permasalahan ekonomi politik dapat diatasi dengan sukses, yang menyebabkan Kongres memberlakukan undang-undang privasi federal yang komprehensif yang menyerupai Peraturan Perlindungan Data Umum (GDPR) Uni Eropa, terdapat risiko serius bahwa pengadilan federal akan membatalkan undang-undang federal yang baru tentang Amandemen Pertama dasar (baik seluruhnya atau sebagian besar).

Pada tahun 2011, dalam kasus tidak jelas yang melibatkan undang-undang privasi Vermont, Mahkamah Agung memutuskan bahwa pembatasan penjualan praktik resep dokter untuk tujuan pemasaran merupakan peraturan pidato berbasis konten yang tidak konstitusional. Dengan kata lain, di AS, pengumpulan, penyimpanan, dan eksploitasi komersial atas data pribadi merupakan suatu bentuk "percakapan". Oleh karena itu, peraturan privasi mungkin akan tunduk pada pengawasan hukum yang sangat ketat dan dapat dianggap inkonstitusional karena undang-undang terlalu membatasi kebebasan berpendapat dengan melarang penambang data "berbicara" (yaitu mendistribusikan ulang data yang mereka kumpulkan dan simpan).

Tentu saja, Amerika Serikat, seperti Jerman, adalah negara federal. Pemerintahan negara bagian mempunyai wewenang polisi umum untuk mengatur guna melindungi kesehatan, keselamatan, kesejahteraan, dan moral penduduknya. Kekuasaan polisi umum ini dapat mencakup adopsi, misalnya tingkat negara bagian, perlindungan privasi yang komprehensif. Namun hingga saat ini, hanya satu negara bagian, California, yang telah mengadopsi undang-undang negara bagian yang cakupan cakupannya sebanding dengan GDPR. California sering menjadi pemimpin nasional misalnya dalam mengatasi polusi udara. Oleh karena itu, kita mungkin berharap negara-negara lain akan mengikuti jejak California dan mengadopsi undang-undang perlindungan data yang komprehensif. Namun pendekatan ini juga akan menghasilkan undang-undang perlindungan data pribadi yang menyerupai keju Swiss yang penuh dengan lubang namun karena alasan yang berbeda dari alasan yang menjelaskan mengapa undang-undang dan peraturan privasi federal saat ini merupakan tambal sulam yang tidak koheren.

Undang-undang negara bagian akan mengatur perlindungan data hanya dalam wilayah negara bagian itu sendiri; hak privasi akan sangat bervariasi ketika seseorang melintasi batas negara. Selain itu, pengadilan federal pada umumnya memutuskan bahwa negara bagian tidak boleh menerapkan peraturan mereka secara ekstrateritorial terhadap aktivitas yang terjadi di negara bagian lain. Dengan demikian, California tidak dapat mewajibkan perusahaan yang beroperasi bahkan di negara bagian tetangga untuk mematuhi peraturan privasi California. Selama negara bagian mana pun menerapkan undang-undang privasi yang kurang protektif dibandingkan California, bisnis yang mengumpulkan, menyimpan, dan menjual data pribadi akan memilih untuk bergabung dalam yurisdiksi tersebut dan memelihara server mereka di sana. Ada juga kemungkinan hal tersebut terjadi karena CCPA akan melakukan hal tersebut. mempengaruhi praktik dan peraturan yang

mengatur pengumpulan, penyimpanan, dan transfer data secara luas, hal ini mungkin tidak valid atas dasar federalisme karena melanggar aspek tidak aktif dari Klausul Perdagangan.

Jalur hukum lain yang sah juga tersedia bagi platform media sosial yang dominan untuk melemahkan keefektifan undang-undang privasi data pribadi negara terutama termasuk klausul pilihan hukum dalam perjanjian persyaratan layanan (TOS) ditambah dengan arbitrase wajib atas setiap perselisihan yang timbul berdasarkan TOS. Penyedia layanan dapat menyatakan bahwa undang-undang di negara yang kurang melindungi privasi akan mengatur penggunaan layanannya dan berdasarkan Undang-Undang Arbitrase Federal, mengharuskan setiap perselisihan harus diselesaikan melalui arbitrase, bukan litigasi perdata. Klausul pilihan hukum yang dipadukan dengan arbitrase dapat secara efektif membatalkan undang-undang privasi negara bagian (seperti California) seperti halnya ketentuan-ketentuan ini secara efektif membatalkan banyak undang-undang hak-hak sipil dan perburuhan negara bagian.

Bahkan sehubungan dengan undang-undang negara bagian yang secara efektif melindungi data pribadi di dalam batas negara bagian, Konstitusi federal, dan Amandemen Pertama, akan membatasi kemampuan pemerintah negara bagian untuk membatasi tindakan yang dilakukan oleh entitas yang mengumpulkan, menganalisis, menambang, dan memanipulasi data pribadi. Karena pengumpulan, penyimpanan, dan manipulasi data semuanya merupakan “ucapan” untuk tujuan Amandemen Pertama, undang-undang negara bagian yang membatasi atau melarang pengumpulan dan penggunaan data pribadi berpotensi menghadapi tantangan konstitusional yang serius. Singkatnya, budaya umum yang tampaknya acuh tak acuh terhadap privasi data pribadi sehubungan dengan lembaga non-pemerintah, dikombinasikan dengan sistem hukum yang lebih berpihak pada pengumpul data, akan mempersulit AS untuk mengadopsi dan menegakkan kebijakan privasi data pribadi. standar privasi hukum global setidaknya jika standar tersebut serupa dengan yang ditetapkan dalam GDPR. Hal ini tidak berarti bahwa data pribadi tidak terlindungi sama sekali di AS. Amerika Serikat bukannya tanpa perlindungan federal atas data pribadi. Beberapa undang-undang federal yang sangat spesifik memberikan perlindungan undang-undang yang relatif sempit terhadap jenis data tertentu, seperti informasi kredit pribadi seseorang (Fair Credit Reporting Act), riwayat kesehatan (Kesehatan). Undang-Undang Portabilitas dan Akuntabilitas Asuransi), dan catatan siswa (Undang-undang Hak Pendidikan Keluarga dan Privasi).

Memang benar, undang-undang federal yang disebut Undang-Undang Perlindungan Privasi Video tahun 1988 (VIPPA) mewajibkan perusahaan untuk menyewa kaset VCR (jika masih ada) dan DVD untuk memperlakukan catatan yang terkait dengan peminjaman tersebut sebagai rahasia dan melarang pelepasan catatan tersebut kepada pihak ketiga tanpa persetujuan tegas dari orang yang terkait dengan catatan tersebut. Meskipun ditulis dengan mempertimbangkan teknologi era 1980-an yang sangat spesifik kaset video pengadilan federal telah menafsirkan VPPA secara kreatif dan luas untuk mencapai format baru dalam mendistribusikan konten audio-visual (termasuk rekaman sewa untuk layanan

streaming seperti Netflix dan Hulu, tapi mungkin anehnya masih mengecualikan buku fisik kuno).

Akan cukup adil, dan sepenuhnya akurat, untuk menggambarkan peraturan privasi data federal di AS sebagai sesuatu yang bersifat tambal sulam. Perlindungan hukum ada sehubungan dengan jenis data pribadi yang sangat spesifik; peraturan perlindungan data pribadi yang komprehensif tidak bisa melakukan hal tersebut. Oleh karena itu, keberadaan undang-undang privasi umum di beberapa negara bagian (terutama termasuk California) tidak boleh dianggap sebagai bukti bahwa sebagian besar penduduk AS menikmati perlindungan data pribadi komprehensif yang sebanding dengan perlindungan yang diberikan berdasarkan GDPR. Faktanya, meskipun beberapa negara bagian mengadopsi peraturan privasi komprehensif yang membatasi pengumpulan dan redistribusi data pribadi, gambaran keseluruhan pemerintahan tingkat federal saat ini suram dan prospek reformasi serius sangat tidak pasti.

4.2 UNDANG-UNDANG PERLINDUNGAN DATA PRIBADI

Privasi dan kebebasan berpendapat berada dalam ketegangan satu sama lain. Sejauh undang-undang privasi membatasi atau melarang penyebaran informasi, hal ini menghambat pelaksanaan kebebasan berbicara (serta kebebasan pers). Lebih dari yurisdiksi lainnya, Amerika Serikat menyampaikan perlindungan yang luas dan mendalam terhadap kebebasan berpendapat. Perlu juga dicatat bahwa pengadilan federal mendefinisikan pidato dengan cakupan yang luar biasa mencakup pengumpulan, penyimpanan, dan transfer data. Motif pembicara untuk menyebarkan informasi umumnya tidak mempengaruhi status dilindunginya; motif yang buruk, seperti menyebabkan rasa malu atau penghinaan, tidak akan membuat ujaran yang bersifat transgresif sosial tidak terlindungi. Bahkan, ujaran palsu yang disengaja pun mendapat perlindungan yang kuat berdasarkan Amandemen Pertama. Mahkamah Agung Amerika Serikat menyatakan bahwa penggunaan data termasuk pengumpulan, penyimpanan, dan manipulasi data merupakan suatu bentuk “ucapan” untuk tujuan penerapan Amandemen Pertama. Sehubungan dengan data apa pun yang berkaitan dengan pejabat publik, tokoh masyarakat, atau masalah yang menjadi perhatian publik, undang-undang privasi dapat dibatalkan secara hukum karena membebani “ucapan” terkait dengan proses pertimbangan demokratis. Baik diadopsi oleh pemerintah federal atau negara bagian, perlindungan privasi data harus bersifat netral dari sudut pandang dan konten, serta dibatasi secara sempit untuk menghindari pelanggaran kebebasan berpendapat (yang, di Amerika Serikat, tidak seperti di sebagian besar negara lain, mencakup perlindungan yang sangat kuat terhadap pidato komersial). Oleh karena itu, Amandemen Pertama akan sangat mempersulit upaya apa pun untuk menyelaraskan peraturan privasi di AS dengan peraturan di UE dan negara lain.

Ada batasan konstitusional terhadap undang-undang privasi informasi yang tidak melibatkan pejabat publik, tokoh masyarakat, atau masalah yang menjadi perhatian publik tetapi merupakan fungsi dari Klausul Perdagangan dan federalisme. Kongres dapat secara konstitusional mengatur aktivitas ekonomi atau komersial apa pun yang, jika digabungkan

dalam perekonomian nasional, akan berdampak besar pada perdagangan antar negara bagian. Kongres telah mengatur, misalnya, penjualan data surat izin mengemudi secara komersial dan Mahkamah Agung telah menguatkan undang-undang ini karena tidak hanya diterapkan pada pihak swasta, namun juga pada pemerintah negara bagian yang memiliki dan ingin menjual data surat izin mengemudi.

Namun, kekuasaan regulasi federal bagaikan pedang bermata dua. Berdasarkan Klausul Supremasi Konstitusi, undang-undang federal yang mengatur pokok bahasan tertentu akan mendahului undang-undang negara bagian yang mengatur pokok bahasan yang sama. Oleh karena itu, jika Kongres memberlakukan undang-undang privasi data umum yang relatif lemah, undang-undang tersebut kemungkinan besar akan mendahului penerapan undang-undang negara bagian yang lebih ketat (seperti CCPA California). Sekalipun kepatuhan terhadap undang-undang federal dan negara bagian secara teori dimungkinkan, undang-undang federal memiliki efek preemptive jika cara yang digunakan berbeda dengan yang digunakan dalam undang-undang negara bagian. Dengan kata lain, terdapat konflik dalam cara yang digunakan untuk mencapai tujuan yang sama. Tujuan kebijakan akan mengarahkan pengadilan peninjau untuk menemukan tindakan pencegahan konflik yang tersirat dalam undang-undang negara bagian. Lebih khusus lagi, jika Kongres ingin mendahului CCPA California, Kongres dapat melakukannya dengan memberlakukan undang-undang privasi federal yang lebih lemah yang mengatur privasi data pribadi.

Amandemen Pertama mempersulit pengamanan data pribadi karena pengumpulan, penyimpanan, dan penjualan data merupakan “pidato” di Amerika Serikat. Namun hal ini tidak berarti bahwa setiap dan seluruh undang-undang privasi akan berdiri di atas es yang tipis secara konstitusional. Perlindungan privasi terbatas yang ada dalam undang-undang federal belum, dan kemungkinan besar tidak akan, dibatalkan berdasarkan Amandemen Pertama. Namun, jika pemerintah federal atau negara bagian mengadopsi sesuatu yang serupa dengan hak untuk dilupakan, yang memerlukan mesin pencari untuk mendeindeks informasi yang masuk dalam cakupan luas “masalah yang menjadi perhatian publik” di AS, undang-undang seperti itu akan menghadapi kemungkinan besar pembatalan yudisial atas dasar Amandemen Pertama. Namun di sisi lain, undang-undang yang membatasi pengumpulan dan pendistribusian ulang data pribadi yang tidak berkaitan dengan pejabat publik, tokoh masyarakat, atau hal-hal yang menjadi perhatian publik tidak akan menimbulkan permasalahan Amandemen Pertama yang sama.

4.3 PERLINDUNGAN PRIVASI HUKUM FEDERAL

Meskipun akan ada Amandemen Pertama, dan komunitas politik yang umumnya acuh tak acuh terhadap privasi informasi, sejumlah undang-undang federal ada dan melindungi privasi informasi dalam beberapa konteks berbeda, termasuk mengenai catatan akademik siswa, catatan medis, catatan keuangan dan perbankan, dan, anehnya, rekaman persewaan kaset video. Undang-undang ini menghindari masalah konstitusional karena tidak mengatur informasi yang berhubungan dengan pejabat publik, tokoh masyarakat, atau masalah yang menjadi perhatian publik.

Ketika informasi hanya berkaitan dengan masalah yang menjadi perhatian pribadi, Amandemen Pertama biasanya tidak akan memberikan hambatan terhadap undang-undang yang melindungi informasi dari pengungkapan. Undang-Undang Hak Pendidikan dan Privasi Keluarga (FERPA) melindungi catatan akademik siswa dan mencegah lembaga pendidikan negeri dan swasta mengungkapkan catatan akademik siswa. Undang-undang ini dimaksudkan untuk melindungi siswa dari pengungkapan catatan pendidikan mereka tanpa izin. Hal ini mencakup hal-hal biasa seperti prestasi akademis (nilai) dan juga catatan kedisiplinan (untuk pelanggaran atau ketidakjujuran akademis). Sejalan dengan itu, Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan tahun 1996 (HIPPA) memberlakukan pembatasan pada pembuatan, pemeliharaan , dan penyebaran rekam medis pribadi.

Fair Credit Report Act of 1970 (FCRA) melarang pengungkapan informasi keuangan pribadi secara paksa termasuk riwayat kredit seseorang. Seperti GDPR, FCRA juga mewajibkan perusahaan yang menyimpan catatan keuangan pribadi untuk menghapus atau mengoreksi informasi yang salah ketika informasi tersebut harus menjadi perhatian lembaga pelaporan kredit. FCRA juga memuat “hak untuk dilupakan”. Setelah jangka waktu tertentu (umumnya tujuh tahun tetapi sepuluh tahun dalam kasus permohonan kebangkrutan), informasi riwayat kredit yang buruk harus dihapus dari laporan kredit seseorang. Kewajiban untuk menghapus informasi kredit yang merugikan yang sebenarnya, namun bertanggal, termasuk yang tidak benar. pembayaran hutang dan bahkan mengajukan kebangkrutan pribadi.

Beberapa undang-undang privasi federal memiliki cakupan yang sangat sempit dan merupakan produk dari pelanggaran privasi informasi yang sangat nyata sehingga menimbulkan kemarahan publik. Selama sidang pengukuhan Robert Bork untuk mendapatkan kursi di Mahkamah Agung Amerika Serikat, penentang pencalonan tersebut memperoleh rekaman penyewaan kaset video Bork dan mempublikasikan informasi ini ke publik. Undang-Undang Perlindungan Privasi Video tahun 1985 mewakili tanggapan Kongres terhadap peristiwa ini dan melindungi terhadap pengungkapan, tanpa persetujuan, catatan peminjaman audio-visual seseorang. Secara total, ada sekitar dua puluh undang-undang privasi federal yang saat ini berlaku, dan mencakup ketentuan-ketentuan dalam Undang-undang Kebijakan Komunikasi Kabel tahun 1984, Undang-Undang Penipuan dan Penyalahgunaan Komputer tahun 1986, Undang-undang Hak Cipta Milenium Digital, Undang-undang Privasi Komunikasi Elektronik tahun 1986, dan Undang-Undang Privasi tahun 1974.

Masing-masing undang-undang ini berdampak membatasi pengungkapan informasi pribadi tanpa persetujuan tertulis sebelumnya. Akankah tantangan Amandemen Pertama terhadap satu atau lebih undang-undang ini berhasil? Mungkin tidak. Mahkamah Agung telah memperjelas bahwa Amandemen Pertama membatasi perlindungan hukum yang diberikan undang-undang negara bagian terhadap reputasi dan martabat pribadi. Dimulai dengan New York Times Co. v. Sullivan, Mahkamah Agung memutuskan bahwa Amandemen Pertama melindungi pernyataan palsu sekalipun mengenai pejabat publik untuk memastikan

bahwa debat publik mengenai hal-hal yang menjadi perhatian publik “tanpa hambatan, kuat, dan terbuka lebar.” Dalam serangkaian kasus berikutnya, para Hakim memperluas aturan ini untuk mencakup tokoh masyarakat dan bahkan tokoh swasta yang terlibat dalam permasalahan yang menjadi perhatian publik. Namun, meskipun Mahkamah Agung terus memperluas standar Sullivan, untuk mencakup gugatan privasi seperti intrusi terhadap pengasingan, mereka dengan tegas menyatakan bahwa baik pemerintah federal maupun negara bagian dapat melindungi informasi yang hanya berkaitan dengan masalah pribadi dari pengungkapan yang tidak disengaja.

Preseden utama, Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc. , melibatkan laporan kredit yang salah yang merusak kemampuan perusahaan untuk memperoleh kredit. Penerbitnya, Dun & Bradstreet, mengklaim bahwa Amandemen Pertama memberikan perlindungan terhadap tanggung jawab atas pelaporan yang keliru, namun tidak bersalah, mengenai kelayakan kredit Greenmoss Builders. Mahkamah Agung dengan tegas menolak klaim Dun & Bradstreet, dengan menyatakan bahwa “pernyataan mengenai masalah-masalah yang semata-mata merupakan urusan pribadi tidak terlalu menjadi perhatian dalam Amandemen Pertama” dan, oleh karena itu, “mengingat berkurangnya nilai konstitusional dari pembicaraan yang tidak melibatkan masalah apa pun.” merupakan hal yang menjadi perhatian publik, kami berpendapat bahwa kepentingan negara cukup mendukung pemberian ganti rugi yang diduga dan bersifat hukuman bahkan jika tidak ada bukti 'kebencian yang sebenarnya'. Jadi, jika undang-undang federal atau negara bagian mengatur pengungkapan informasi jika informasi tersebut tidak berkaitan bagi pejabat publik, tokoh masyarakat, atau masalah yang menjadi perhatian publik, Amandemen Pertama tidak akan berdampak besar dan undang-undang tersebut tidak boleh dibatalkan secara hukum karena melanggar hak berpendapat dan pers.

Undang-undang federal yang melindungi privasi dalam keadaan tertentu berkaitan dengan catatan pribadi dan bukan aktivitas seperti kebiasaan menjelajahi web atau pembelian di internet. Kita bahkan bisa menganggap catatan tersebut merupakan semacam milik pribadi, dengan undang-undang privasi federal yang memberikan kepemilikan, dalam bentuk kendali, kepada orang yang bersangkutan. Bagaimana dengan informasi yang lebih umum seperti geolokasi data atau kebiasaan berselancar web? Bisakah undang-undang federal melindungi terhadap transfer informasi semacam itu secara tidak sukarela tanpa persetujuan tegas dari orang tersebut? Keputusan Sorrell, yang telah dibahas sebelumnya, menunjukkan bahwa perlindungan privasi yang ditargetkan yang hanya membatasi jenis penggunaan data pribadi tertentu dapat menimbulkan masalah Amandemen Pertama. Seorang pasien dapat dikatakan harus menikmati kendali atas data resep dokternya bahkan jika data tersebut disimpan oleh apotek atau perusahaan asuransi kesehatan. Namun, Mahkamah Agung menyatakan bahwa larangan penjualan informasi tersebut untuk tujuan pemasaran merupakan pembatasan berdasarkan konten yang memicu pengawasan hukum yang ketat. Salah satu perbedaan yang mungkin terjadi antara undang-undang Vermont dan undang-undang privasi federal adalah bahwa undang-undang Vermont sangat bertarget dan melindungi privasi dengan cara yang sangat terbatas; undang-undang privasi federal yang

sedikit demi sedikit umumnya berlaku dan melarang pengungkapan informasi kepada pihak ketiga secara kategoris (bukan hanya untuk pembicara tertentu atau tujuan tertentu). Oleh karena itu, dalam hal ini, mereka tidak "berbasis pembicara" karena perlindungan privasi akan berlaku terlepas dari orang atau entitas yang ingin mendistribusikan informasi tersebut dan tidak "berbasis konten" karena perlindungan tersebut berlaku terlepas dari alasan yang tepat bagi pemegangnya. data pribadi ingin melepaskannya kepada pihak ketiga tanpa persetujuan sebelumnya dari orang yang terkait. Namun di sisi lain, undang-undang privasi yang mencakup pengecualian untuk tujuan penegakan hukum atau penelitian medis akan menimbulkan peningkatan risiko pembatalan hukum. Sederhananya, perlindungan selektif terhadap kepentingan privasi berimplikasi pada Amandemen Pertama karena Sorrell memperlakukan perlindungan privasi selektif sebagai bentuk diskriminasi konten.

4.4 HAK PRIVASI DATA KONSTITUSIONAL DAN HAK KONSTITUSIONAL

Meskipun ada persepsi luas bahwa tidak ada hak konstitusional atas penentuan nasib sendiri berdasarkan informasi, hal ini sebenarnya tidak terjadi. Terlebih lagi, Mahkamah Agung Amerika Serikat mengakui hak atas privasi informasi bahkan sebelum Kasus Sensus yang (pantas) dikeluarkan oleh Mahkamah Konstitusi Federal Jerman. Seperti yang akan dijelaskan pada bagian ini, perbedaan utama antara AS dan Eropa Barat bukanlah pada adanya kepentingan yang dilindungi konstitusi dalam hal penentuan nasib sendiri berdasarkan informasi, namun lebih pada cakupan hak tersebut. Di UE, di Dewan Eropa, dan di yurisdiksi domestik seperti Jerman, pemerintah mempunyai kewajiban tidak hanya untuk menghormati hak-hak konstitusional, termasuk hak privasi, namun juga kewajiban untuk menjamin hak-hak ini secara lebih umum dalam masyarakat. Sebaliknya di AS, hak konstitusional hanya berlaku terhadap pemerintah dan tidak menimbulkan kewajiban untuk mengatur aktor non-negara guna menjamin hak-hak dasar masyarakat secara lebih luas.

Faktanya, hak atas privasi informasi sebenarnya ada di bawah Konstitusi AS. Mahkamah Agung pertama kali mengakui kepentingan tersebut pada tahun 1977. Dalam Whalen v. Roe, Mahkamah Agung menolak tantangan konstitusional terhadap undang-undang negara bagian New York, Controlled Substances Act, yang mewajibkan dokter untuk melaporkan resep obat penghilang rasa sakit yang membuat ketagihan (yang merupakan obat terlarang). pasar ada) ke Departemen Kesehatan Negara Bagian New York. Undang-undang tersebut memberlakukan persyaratan pelaporan informasi mengenai dokter yang meresepkan obat dan menciptakan program di pemerintahan negara bagian untuk menyimpan, menganalisis, dan melacak resep obat pereda nyeri yang berpotensi menimbulkan kecanduan.

Baik dokter maupun pasien berkeberatan karena pengumpulan dan penyimpanan informasi medis pribadi sensitif yang dilakukan oleh New York dapat dan akan mengakibatkan pelanggaran privasi jika lembaga negara gagal menyimpan informasi tersebut dengan benar dan menjamin kerahasiaannya. Untuk menghindari kemungkinan ini, para penggugat berpendapat bahwa negara tidak boleh mengumpulkan dan menyimpan

informasi ini. Mereka menegaskan bahwa hak privasi yang melindungi otonomi reproduksi harus diperluas hingga mencakup informasi medis pribadi yang bersifat rahasia.

Argumen tersebut sepenuhnya masuk akal. Mahkamah Agung mengakui hak umum atas privasi dalam keputusannya yang penting pada tahun 1965 dalam kasus Griswold v. Connecticut. Griswold membatalkan undang-undang negara bagian Connecticut yang melarang pasangan menikah mencari, memperoleh, dan menggunakan alat kontrasepsi untuk tujuan pengendalian kelahiran. Beberapa tahun kemudian, pada tahun 1972, pengadilan memperluas kepentingan otonomi reproduksi ini kepada pasangan yang belum menikah. Mungkin yang paling terkenal, pada tahun 1973, Mahkamah Agung memperluas hak privasi Griswold hingga mencakup keputusan untuk mencari dan melakukan aborsi non-terapeutik. Oleh karena itu, pada tahun 1977, konsep hak privasi konstitusional, sebagai salah satu aspek kebebasan yang dilindungi berdasarkan Klausul Proses Hukum dari Amandemen Kelima dan Amandemen Keempat Belas, telah memiliki dasar yang kuat dalam kasus hukum yang ada.

Di Whalen, para Hakim dengan suara bulat menolak tantangan konstitusional terhadap undang-undang negara bagian New York karena undang-undang tersebut memajukan tujuan penting pemerintah (mengurangi penyalahgunaan obat pereda nyeri yang diresepkan) dan berisi perlindungan yang memadai terhadap pelepasan data medis pribadi yang disengaja atau tidak disengaja (catatan tersebut disimpan dengan aman dan akses terhadap catatan tersebut sangat dibatasi). Namun demikian, Hakim John Paul Stevens, yang menulis surat untuk pengadilan, mengakui bahwa Konstitusi melindungi kepentingan privasi dalam catatan medis pribadi. Ia menekankan bahwa bukannya tidak menyadari adanya ancaman terhadap privasi yang tersirat dalam akumulasi informasi pribadi dalam jumlah besar di bank data yang terkomputerisasi atau arsip pemerintah berukuran besar lainnya. Namun ia menjelaskan, mengakui bahwa dalam beberapa keadaan, kewajiban tersebut dapat dikatakan berakar pada Konstitusi, namun skema perundang-undangan di New York, dan penerapan prosedur administratifnya, merupakan bukti adanya kepedulian dan perlindungan terhadap kepentingan individu terhadap privasi.

Oleh karena itu, kepentingan privasi konstitusional dalam menghindari pengungkapan data pribadi yang tidak beralasan ada di bawah Konstitusi AS tetapi dengan ketentuan bahwa program pemerintah yang mengumpulkan dan menyimpan data memiliki tujuan yang sah, dan memiliki perlindungan substantif dan prosedural yang memadai untuk menghindari pengungkapan data yang tidak beralasan. data pribadi, program pendataan pemerintah bersifat konstitusional. Kasus-kasus berikutnya, terutama termasuk NASA v. Nelson, yang diputuskan oleh Mahkamah Agung pada tahun 2011, telah menegaskan prinsip umum bahwa ketika pemerintah memiliki informasi pribadi yang bersifat rahasia, harus ada perlindungan yang memadai untuk melindungi dari pengungkapan yang tidak disengaja kepada pihak ketiga. Oleh karena itu, undang-undang AS mencerminkan undang-undang CJEU berdasarkan keputusan-keputusan seperti Digital Rights Ireland dan Tele2Sverge. Memang benar bahwa Mahkamah Agung belum membatalkan undang-undang federal atau negara bagian karena melanggar kepentingan seseorang dalam privasi informasi, namun

pemerintah harus memastikan bahwa ketika mengumpulkan dan menyimpan data pribadi yang bersifat rahasia, pengungkapan data hanya dapat dilakukan untuk kepentingan sah pemerintah, dan catatan-catatan ini harus disimpan dengan aman dengan akses yang dikontrol secara ketat dan hati-hati untuk menghindari pengungkapan yang tidak beralasan.

Mengingat hak konstitusional atas privasi informasi ada di Amerika Serikat, orang mungkin bertanya mengapa tidak ada undang-undang privasi federal yang umum. Di Eropa Barat, pemerintah mempunyai kewajiban tidak hanya untuk menahan diri dari pelanggaran hak-hak konstitusional, seperti Pasal 779 dan 880 Piagam Eropa dan Pasal 8 Konvensi Eropa, namun juga kewajiban umum untuk menjamin kepentingan-kepentingan ini secara lebih luas dalam masyarakat. Kewajiban untuk melindungi hak-hak dasar dari pembatasan yang dilakukan oleh pihak swasta berarti bahwa di Eropa, pemerintah mempunyai kewajiban tegas untuk memberlakukan dan menegakkan undang-undang privasi data yang membatasi aktor non-pemerintah (termasuk orang dan perusahaan lain).

Namun di AS, hak konstitusional hanya bertentangan dengan negara itu sendiri bukan bertentangan dengan lembaga non-pemerintah. Berdasarkan doktrin tindakan negara, hak konstitusional akan berlaku bagi entitas swasta hanya jika mereka memenuhi salah satu dari empat tes untuk tindakan negara. Doktrin dampak sekunder, atau Drittwirkung (penerapan aturan konstitusi pada lembaga non-pemerintah), merupakan hal yang lumrah dalam yurisprudensi CJEU, ECtHR, dan dalam yurisprudensi domestik mahkamah konstitusi di negara-negara seperti Republik Federal Jerman tetapi hal ini tidak penting di AS.Di AS, ada kemungkinan untuk menantang aturan-aturan hukum swasta berdasarkan teori bahwa pemerintah menetapkan dan menegakkan aturan-aturan ini, dan aturan-aturan tersebut harus konsisten dengan batasan-batasan konstitusi. Namun, Konstitusi dan Bill of Rights tidak memiliki penerapan langsung atau tidak langsung terhadap peraturan-peraturan tersebut. perusahaan swasta seperti McDonald's atau Marriott; pemerintah tidak mempunyai kewajiban untuk menjamin kepentingan konstitusional secara luas dalam masyarakat umum. Oleh karena itu, meskipun Mahkamah Agung mengakui adanya kepentingan privasi dalam data pribadi yang bersifat rahasia dan merugikan pemerintah, tidak ada hak umum atas penentuan nasib sendiri berdasarkan informasi, seperti yang diakui oleh Mahkamah Konstitusi Federal dalam Kasus Sensus86 atau CJEU di Google Spanyol berdasarkan Konstitusi AS sehubungan dengan aktor non-negara. Agar entitas non-pemerintah dapat diatur, Kongres perlu membuat undang-undang.Singkatnya, Konstitusi AS memang melindungi hak penentuan nasib sendiri berdasarkan informasi.

Kepentingan ini merupakan salah satu aspek hak privasi dan juga berimplikasi pada perlindungan Amandemen Pertama terhadap pernyataan yang dipaksakan. Namun, hak-hak ini hanya mengikat negara itu sendiri dan tidak mempunyai penerapan langsung atau tidak langsung kepada lembaga non-pemerintah. Agar hak privasi informasi dapat diterapkan pada lembaga non-pemerintah, termasuk orang dan perusahaan lain, undang-undang positif, di tingkat federal, negara bagian, atau lokal harus diberlakukan. Terlebih lagi, keputusan badan legislatif untuk memberlakukan atau tidak memberlakukan undang-undang tersebut sepenuhnya bersifat diskresi.

4.5 PERLINDUNGAN DATA PRIBADI UMUM TERHADAP ENTITAS NON-PEMERINTAH?

Meskipun hak konstitusional tidak bertentangan dengan individu atau badan swasta, dan meskipun Amandemen Pertama mempersulit pengaturan privasi, pemerintah pusat masih bisa memberlakukan dan menegakkan undang-undang privasi yang lebih umum dibandingkan yang ada saat ini. Pertanyaan yang muncul adalah: Mengapa AS tidak memiliki perlindungan yang lebih luas terhadap data pribadi dibandingkan perusahaan seperti Facebook, Google, dan Twitter?. Tentu saja ada banyak faktor yang berperan, namun permasalahan terbesarnya berkaitan dengan kurangnya kepedulian terhadap perlindungan data pribadi dalam masyarakat kontemporer di AS. Sebagian besar penduduk AS tidak peduli terhadap pengumpulan dan penggunaan data pribadi mereka oleh perusahaan swasta dan mereka sedemikian rupa sehingga sebagian besar orang Eropa mungkin akan menganggapnya mengejutkan, berbahaya, atau mungkin keduanya. Selain itu, beberapa akademisi hukum terkemuka di AS berpendapat bahwa kekuatan pasar, jika dibiarkan beroperasi secara bebas dan berjalan dengan sendirinya, akan cukup melindungi kepentingan individu dalam privasi data. Di AS, banyak orang termasuk warga negara biasa, tetapi juga pejabat pemerintah dan badan hukum akademisi sebagian besar tidak peduli dengan ancaman terhadap penentuan nasib sendiri berdasarkan informasi yang diberikan oleh perusahaan media sosial, penyedia mesin pencari, dan perusahaan swasta nirlaba lainnya yang mengumpulkan, menyimpan, dan menambang data pribadi demi privasi.

Sebagian permasalahannya berkaitan dengan metodologi common law sebagai sarana untuk mengatasi permasalahan hukum. Meskipun AS, baik di tingkat federal maupun negara bagian, sangat bergantung pada peraturan perundang-undangan, atau “kode”, sebagian besar reformasi hukum di AS terjadi di tingkat negara bagian secara interstisial. Semua kecuali satu negara bagian AS menggunakan metode pembuatan peraturan common law, yang berarti bahwa pengadilan memiliki tanggung jawab utama untuk membuat dan menegakkan peraturan hukum perdata yang berarti hukum kontrak, properti, dan perbuatan melawan hukum.

Common law membentuk peraturan-peraturan baru, atau memodifikasi peraturan-peraturan yang sudah ada, berdasarkan retrospektif. Ketika litigasi bergerak maju dari pengadilan ke pengadilan banding, para pihak mungkin berargumentasi bahwa peraturan-peraturan hukum yang ada harus diterapkan sebagaimana peraturan-peraturan yang berlaku saat ini atau mereka dapat melakukan hal yang sama. mendukung modifikasi atau pencabutan aturan-aturan common law yang sudah ada. Metodologi common law bersifat melihat ke belakang, bukan melihat ke depan. Metodologi ini tidak terlalu mengantisipasi masalah, melainkan bereaksi terhadap masalah tersebut setelah masalah tersebut muncul. Hukum perdata cenderung lebih berwawasan ke depan dan berusaha menangkal permasalahan sebelum terwujud dalam masyarakat. Kode Napoléon (Kode Sipil Perancis), KUH Perdata Jerman, dan bahkan GDPR sangat berwawasan ke depan dan proaktif, dibandingkan melihat ke belakang dan reaktif. Dalam tradisi hukum perdata, pembuat undang-undang, hakim, dan akademisi hukum bekerja untuk memperbarui undang-undang secara berkelanjutan dengan cara yang mengantisipasi dan memenuhi kebutuhan

masyarakat yang terus berkembang. Tujuannya bukan sekadar untuk memperbaiki kesalahan setelah kesalahan tersebut terjadi. idealnya, hukum perdata akan mencegah dan mencegah terjadinya kerugian.

Dalam beberapa hal, metode hukum perdata mencerminkan keyakinan yang lebih besar terhadap kemampuan pemerintah untuk mempelajari permasalahan dan mencapai kesimpulan yang benar. Ketika suatu sistem hukum mengadopsi peraturan sebelum adanya perubahan sosial, ilmu pengetahuan, atau teknologi, terdapat risiko melakukan kesalahan. Pendekatan interstisial yang lebih konservatif secara teori seharusnya menghindari keputusan yang tidak tepat sasaran. Namun, di sisi lain, pendekatan seperti ini harus dibayar mahal terkadang permasalahan baru memerlukan gambaran besar dan pemikiran yang sistematis dan bukan sekadar mengutak-atik masalah yang ada.

Seperti yang telah dijelaskan sebelumnya, di AS, berdasarkan undang-undang federal, perlindungan data pribadi terdiri dari serangkaian undang-undang yang tidak terkait, yang diadopsi pada berbagai waktu, sering kali sebagai respons terhadap kekurangan yang dirasakan dalam lanskap hukum yang ada. AS tidak pernah menciptakan rezim perlindungan data komprehensif yang menangani penentuan nasib sendiri secara informasional secara sistematis dan komprehensif. Sebaliknya, ketika permasalahan muncul, Kongres telah mengambil langkah-langkah tersendiri untuk mengatasi permasalahan tersebut tetapi hanya permasalahan tersebut saja. Dalam mempertimbangkan pergerakan menuju rezim digitalitas global untuk perlindungan data pribadi, perbedaan dalam peraturan yang berwawasan ke depan dan ke belakang akan menimbulkan permasalahan yang sangat sulit. Secara umum, pendekatan AS lebih memilih peraturan yang minimal dan reaktif serta memberikan kepercayaan yang besar pada pelaku pasar swasta untuk berperilaku bertanggung jawab. Kita tahu, dari contoh kegagalan dalam menghormati privasi data pribadi, kita tahu bahwa pasar swasta yang tidak diatur dalam data pribadi tidak akan bisa berbuat apa-apa. mengatur dirinya sendiri secara efektif atau andal. Kita juga tahu bahwa konsumen individu, yang dihadapkan pada penyedia layanan monopoli atas platform media sosial dan mesin pencari, tidak memiliki daya tawar yang berarti dengan perusahaan seperti Facebook, Google, Twitter, dan YouTube. Terlepas dari fakta-fakta yang sudah diketahui umum ini, sistem hukum AS cenderung memandang sangat skeptis terhadap intervensi pemerintah di pasar swasta (termasuk pasar informasi). Penduduk AS cenderung memandang pemerintah dengan rasa tidak percaya dan menaruh kepercayaan yang lebih besar, secara lebih refleks, pada perusahaan swasta yang mencari keuntungan.

Perbedaan budaya yang lebih besar ini akan menghambat kemampuan AS untuk mencapai kesepakatan luas dengan Eropa dan seluruh dunia mengenai standar transnasional yang sesuai mengenai perlindungan data pribadi. Sejujurnya, tidak mengherankan jika CJEU telah memutuskan bahwa standar perlindungan data pribadi AS, yang tercermin dalam apa yang disebut perjanjian “Perlindungan Privasi”, tidak setara secara material dengan standar Eropa, dan oleh karena itu tidak cukup untuk memenuhi persyaratan perjanjian yang sah secara hukum yang akan mengizinkan perusahaan AS mengumpulkan, menyimpan, dan memperdagangkan data pribadi penduduk UE. Seperti perjanjian Safe Harbor yang

mendahuluinya, Perlindungan Privasi tidak melakukan apa pun untuk memastikan bahwa data pribadi penduduk UE aman dari penyimpanan dan pengintaian pemerintah AS situasi yang menurut CJEU pada dasarnya tidak dapat diselaraskan dengan Pasal 7 dan 8 Perjanjian ini. Piagam Eropa. Seperti keputusan CJEU sebelumnya (Schrems I) yang menyatakan bahwa perlindungan AS yang tercantum dalam perjanjian Safe Harbor tidak memadai secara hukum, Schrems II menegaskan kembali bahwa CJEU tidak akan melepaskan hak penduduk UE atas informasi mandiri. penentuan kapan perusahaan seperti Facebook atau Instagram menyimpan datanya di AS (bukan di UE).

Perlindungan yang tampaknya setara dengan GDPR berdasarkan perjanjian Perlindungan Privasi melibatkan ketergantungan pada pejabat tingkat rendah Departemen Luar Negeri *(ombudsman)*, yang tidak memiliki wewenang untuk benar-benar mencari database badan intelijen yang relevan dan tidak memiliki wewenang untuk meminta penghapusan informasi pribadi. Data atau bahkan kemampuan untuk membatasi akses badan keamanan nasional AS terhadap data tersebut. Untuk mengetahui bahwa sekadar pantomim privasi untuk mengatasi pelanggaran privasi data penduduk UE di AS memberikan perlindungan yang sepenuhnya setara dengan GDPR, diperlukan tindakan yudisial yang bersifat kebutaan yang disengaja, sebuah fiksi hukum yang sama sekali tidak masuk akal, atau mungkin tindakan yang sangat tidak masuk akal. keduanya. Pemerintah AS melakukan pengawasan yang luas dan menyeluruh terhadap komunikasi elektronik dengan cara yang benar-benar tidak transparan dan tidak memiliki pengawasan hukum yang berarti. Kita mengetahui hal ini dari pengungkapan Edward Snowden yang sangat meresahkan namun belum terselesaikan. Perlindungan Privasi tidak memberikan jaminan apa pun yang berarti bahwa data pribadi yang berkaitan dengan penduduk UE akan sama amannya di AS seperti halnya di wilayah UE berdasarkan GDPR. CJEU sepenuhnya benar dalam mencapai kesimpulan ini dalam Schrems II. Ketika klaim Schrems di masa depan diajukan dan diputuskan, kelemahan dan sifat tidak lengkap dari ketentuan perlindungan data pribadi AS akan semakin sulit untuk diabaikan begitu saja. Perusahaan-perusahaan AS yang ingin melakukan bisnis di UE mungkin harus menerapkan protokol dan prosedur untuk menghindari ekspor data tersebut ke AS guna menghindari tanggung jawab berdasarkan GDPR dan rezim privasi domestik.

4.6 DIGITALITAS GLOBAL DAN PERLINDUNGAN DATA PRIBADI

Beberapa tahun yang lalu, Frank Easterbrook, mantan profesor hukum Universitas Chicago dan saat ini menjadi hakim federal yang bertugas di Pengadilan Banding AS untuk Seventh Circuit, menulis artikel tinjauan hukum yang sangat berpengaruh tentang bagaimana teknologi dapat memicu perubahan hukum. Berjudul “Ruang Siber dan Hukum Kuda,” artikel tersebut berpendapat bahwa internet tidak akan menghadirkan masalah atau tantangan hukum baru yang serius. Klaim utamanya adalah bahwa segala upaya untuk menciptakan rezim hukum khusus untuk internet, seperti “hukum kuda” yang bersifat hipotetis, akan “menjadi dangkal dan kehilangan prinsip-prinsip pemersatu.” Dalam pandangannya, hal tersebut akan jauh lebih baik. untuk mempertimbangkan permasalahan

yang ditimbulkan oleh dunia maya “dalam konteks aturan yang lebih luas” yang melibatkan kontrak, properti, dan perbuatan melawan hukum. Meskipun dampak teknologi baru terhadap hubungan sosial, hukum, dan budaya yang ada sudah mulai teratasi, yang terbaik adalah melakukan hal ini. karena “jika Anda tidak tahu apa yang terbaik, biarkan orang membuat pengaturannya sendiri.” Sebaliknya, Easterbrook berpendapat bahwa biasanya akan lebih bijaksana jika “terus melakukan apa yang telah Anda lakukan.

Hampir seperempat abad kemudian, menjadi jelas bahwa internet memang menciptakan masalah yang memerlukan tanggapan hukum yang tepat sasaran. Saat ini, informasi melintasi batas-batas negara dalam sekejap secara harfiah secepat cahaya melalui kabel serat optik dan transfer informasi secara instan menciptakan dampak sosial yang serius di tempat-tempat yang jauh dari sumber informasi. Untuk membingkai permasalahan ini dalam istilah hukum dan ekonomi, transnasional Arus informasi menciptakan eksternalitas yang membebankan biaya pada orang-orang di yurisdiksi yang jauh dari server yang menyimpan informasi. Dan, ketika penyebaran informasi ini menimbulkan kerugian di suatu yurisdiksi, pembuat kebijakan akan berupaya untuk mengatasi dampak buruk tersebut. Sama seperti permasalahan seperti polusi dan emisi karbon yang memerlukan pendekatan global, kerugian sosial yang disebabkan oleh pengumpulan dan redistribusi data pribadi juga memerlukan pendekatan transnasional. pendekatan ini agar efektif. Jelas terdapat kebutuhan akan digitalitas global walaupun prospek untuk mencapai kesepakatan mengenai cara menyelaraskan privasi informasi dan kebebasan berpendapat masih sangat tidak pasti.

Permasalahan konflik hukum yang terkait dengan privasi informasi sangatlah besar dan jauh lebih besar dibandingkan dengan permasalahan hukum kekayaan intelektual yang memotivasi Hakim Easterbrook untuk menulis esainya yang berjudul “Law of the Horse”. Sekalipun terdapat perbedaan dalam hak kekayaan intelektual di seluruh sistem hukum dalam negeri, hal ini hampir selalu merupakan perbedaan dalam ruang lingkup dan bukan jenisnya. Kapan sebuah karya seni atau sastra harus memasuki ranah publik adalah persoalan yang bisa dan akan berbeda-beda di kalangan orang yang berakal sehat. Namun, gagasan bahwa seorang penulis harus memiliki kepentingan properti yang dilindungi dalam karyanya bukanlah sesuatu yang akan ditolak sepenuhnya oleh hampir semua negara demokrasi industri.

Namun, kendali atas informasi pribadi secara kualitatif berbeda. Di AS, sistem hukum menolak, hampir secara kategoris, gagasan bahwa pers harus dilarang menyebarkan informasi yang jujur namun memalukan mengenai pejabat publik, tokoh masyarakat, dan orang-orang yang terlibat dalam permasalahan yang menjadi perhatian publik. Komitmen terhadap arus informasi yang tidak diatur sangatlah kuat dan mendalam. Terlebih lagi, pers biasanya dapat memutuskan sendiri apakah suatu informasi tertentu merupakan “masalah yang menjadi perhatian publik.” Berbeda dengan di Eropa, baik badan legislatif maupun pengadilan tidak mempunyai banyak kewenangan. keleluasaan untuk memutuskan bahwa informasi yang benar tentang pejabat publik atau tokoh masyarakat tidak relevan dengan wacana publik.

Oleh karena itu, hal seperti hak untuk dilupakan (RTBF), yang pertama kali diakui oleh CJEU di Google Spanyol dan kini dikodifikasi oleh GDPR, tidak dikenal di AS. Dan, sebagaimana telah dijelaskan sebelumnya, Amandemen Pertama akan menghadirkan hambatan yang tidak dapat diatasi terhadap pemerintah yang melarang pengungkapan informasi pribadi yang jujur, namun memalukan, jika subjeknya adalah pejabat publik, tokoh masyarakat, atau jika informasi yang dipermasalahkan berkaitan dengan suatu masalah. menjadi perhatian publik.

Meskipun AS menolak untuk ikut serta dalam kebijakan privasi data global, tampaknya cukup jelas bahwa konsensus global yang mendukung pembatasan yang lebih ketat pada pengumpulan dan distribusi data pribadi mulai muncul. GDPR tidak hanya menetapkan RTBF, tetapi juga menetapkan batasan konkret mengenai pengumpulan dan penggunaan data pribadi secara lebih umum. Selain itu, CJEU berpendapat bahwa, dalam bentuknya yang sekarang, GDPR tidak memiliki dampak ekstrateritorial. Beberapa perlindungan serupa dapat diberlakukan di Amerika Serikat tetapi harus dilakukan dengan sangat hati-hati untuk menghindari kesulitan dalam Amandemen Pertama.

Misalnya, bentuk RTBF yang lebih terbatas sudah ada dalam konteks data pribadi pelaporan kredit berdasarkan FCRA. Meski begitu, kewajiban hukum umum dari pihak penyedia mesin pencari untuk menghapus indeks informasi pribadi yang memalukan namun jujur akan kemungkinan besar akan dibatalkan atas dasar kebebasan berpendapat di AS. Informasi yang dipermasalahkan di Google Spanyol, misalnya, jelas merupakan masalah yang menjadi perhatian publik dan pemerintah tidak dapat melarang publikasi informasi tersebut secara konstitusional. Proses hukum resmi apa pun, termasuk penjualan properti pribadi secara paksa untuk memenuhi kewajiban pajak utang, akan dianggap sebagai masalah yang menjadi perhatian publik di AS.

Kita mungkin akan melihat peningkatan tekanan dari UE dan yurisdiksi perlindungan privasi lainnya terhadap AS agar lebih menjamin hak privasi informasi. RTBF memberikan contoh bagus mengapa tren seperti ini hampir pasti akan terjadi. Jika informasi tersedia di mana saja, maka informasi tersebut dapat dikatakan tersedia di mana saja. Perintah penghapusan indeks terbatas pada situs yang menggunakan nama domain geografis tertentu, seperti .fr, .de, atau .es, berarti bahwa informasi tersebut akan tersedia jika ada-seseorang yang mencarinya cukup menggunakan Google atau Bing versi asing (misalnya, google.com). Tentu saja benar bahwa dalam kasus Google yang melibatkan badan pengatur privasi Perancis (CNIL), CJEU menyatakan bahwa GDPR tidak mengizinkan dikeluarkannya perintah global yang mengharuskan deindeksasi hasil mesin pencari di seluruh dunia. Namun , keputusan CJEU merupakan keputusan yang sempit dan bersifat teknis.

Oleh karena itu, seperti yang tertulis saat ini, GDPR tidak memiliki dampak ekstrateritorial di luar batas negara-negara anggota UE. Namun, pada saat yang sama, CJEU dengan jelas menyatakan bahwa jika UE ingin mengesahkan perintah global untuk menegakkan RTBF, maka UE harus kompetensi untuk mengadopsi peraturan tersebut. Jika UE akan mengubah GDPR di masa depan untuk secara tegas mengesahkan perintah penghapusan indeks global, CJEU hampir pasti akan menjunjung tinggi peraturan yang

direvisi tersebut sebagai cara yang proporsional dan diperlukan untuk mengamankan data pribadi (serta privasi dan martabat manusia secara umum). Pada titik ini, konflik antara undang-undang privasi data Eropa, di satu sisi, dan undang-undang kebebasan berpendapat di AS, di sisi lain, akan menjadi sangat problematis. Setiap bisnis yang ingin melakukan bisnis di UE dan AS akan menghadapi pilihan Hobson: Hapus indeks materi yang pengguna di AS memiliki hak konstitusional untuk membaca dengan teliti (dan berisiko kehilangan pengguna tersebut karena mesin pencari AS yang tidak memiliki hak konstitusional untuk membaca). kehadiran di Eropa) atau membatasi penghapusan pengindeksan hasil penelusuran ke situs-situs yang menargetkan pengguna di UE (dan berisiko dikenakan denda dan hukuman besar karena gagal menerapkan perintah sah dari regulator privasi Eropa untuk menghapus hasil secara global, atau di seluruh dunia).

Bagaimana kita bisa menyelesaikan konflik ini? Yang pasti, keputusan Google CJEU, yang tidak mengizinkan upaya regulator privasi Prancis (CNIL) yang mewajibkan Google menerapkan perintah de-indexing RTBF Prancis secara global, telah menunda hari perhitungan hingga tiba saatnya ketika UE mengadopsi peraturan perlindungan data yang secara jelas memiliki dampak ekstrateritorial. Namun, karena hasil pencarian yang tersedia di mana saja sebenarnya tersedia di mana saja, masalah konflik hukum ini harus diatasi suatu saat nanti. AS mempunyai kepentingan yang kuat untuk bekerja secara konstruktif untuk menciptakan peraturan global yang melindungi kepentingan Amandemen Pertama penduduk AS sambil juga menghormati kepentingan privasi hukum penduduk UE.

Dalam hal ini, digitalitas global adalah mungkin dan diperlukan. Sekalipun kesepakatan mengenai peraturan substantif yang mengatur perlindungan data pribadi tidak mungkin tercapai karena adanya konflik prioritas dalam konstitusi privasi di Eropa dan kebebasan berpendapat di AS namun masih mungkin untuk menyepakati kapan sebuah negara berdaulat dapat mengatur pengumpulan data secara sah dan sah. penyimpanan, dan penggunaan data yang disimpan di luar negeri. AS tentunya mempunyai kepentingan penting dalam menentukan kapan perusahaan-perusahaan AS harus menyediakan data kepada pemerintah atau dunia usaha asing. Aturan yang mengatur penerapan peraturan privasi data pribadi ekstrateritorial dapat dinegosiasikan secara global. Melakukan hal ini juga akan membuat semua orang mendapat pemberitahuan yang adil mengenai peraturan mengenai perilaku dan aktivitas yang berpotensi memicu penerapan peraturan privasi di suatu negara. Pendekatan ini akan jauh lebih unggul daripada rezim swadaya semacam "Wild West" digital di mana pemerintah nasional memberlakukan aturan privasi data yang saling bersaing, tumpang tindih, dan bertentangan.

Faktanya, permasalahan ini mungkin tidak menemui jalan buntu berdasarkan peraturan privasi Eropa, melainkan berdasarkan peraturan konten yang diadopsi oleh negara seperti Tiongkok atau Turki. Kita dapat dengan mudah membayangkan Tiongkok berupaya menerapkan perintah de-indeks global untuk konten yang dianggap bertentangan dengan kepentingan politik dalam negeri oleh Partai Komunis Tiongkok. Akses ke pasar Tiongkok dapat digunakan sebagai pengaruh untuk memaksa perusahaan-perusahaan yang berbasis di AS menyensor hasil mesin pencari tidak hanya di Tiongkok, tetapi juga di AS. Perlu juga

dicatat bahwa CJEU dan ECtHR telah memperjelas bahwa informasi yang mengandung kepentingan publik yang sah tidak akan dideindeks. Cakupan masalah kepentingan umum, tentu saja, lebih dibatasi dalam yurisprudensi CJEU dan ECtHR dibandingkan yurisprudensi Mahkamah Agung Amerika Serikat, namun terdapat komitmen bersama mengenai hak asasi manusia untuk menghormati kebebasan berpendapat. untuk memfasilitasi proses musyawarah kolektif yang penting agar pemerintahan mandiri yang demokratis dapat berjalan. Perbedaannya berkaitan dengan sejauh mana pers dapat mendefinisikan sendiri, sesuai keinginannya, konsep publikasi untuk kepentingan publik.

Sebaliknya, pemerintah Tiongkok tidak memiliki komitmen serupa terhadap pasar gagasan politik yang terbuka dan dinamis. Tiongkok akan berupaya menyensor konten sebagai cara untuk menerapkan kontrol sosial menyeluruh terhadap penduduknya. Oleh karena itu, pemerintah Eropa harus berhati-hati terhadap keinginan mereka. Mungkin saja jika Brussel menerima perintah penghapusan indeks global secara sepihak maka pemerintah otokratis Beijing akan menjadi penerima manfaat utama. Alih-alih melindungi warga negara Eropa dari publikasi ulang informasi yang memalukan di situs-situs Amerika, mungkin saja warga negara Amerika dan Eropa akan lebih sulit mengakses informasi jujur yang jelas-jelas berhubungan dengan kepentingan publik.

BAGIAN III

HUKUM KONTRAK KONSUMEN

BAB 5
PERDAGANGAN ONLINE GLOBAL PADA HUKUM KONTRAK DAN KONSUMEN

5.1 PENDAHULUAN

Perdagangan online telah berkembang secara dramatis dalam dekade terakhir dan menjadi cara utama konsumen membeli barang. Pandemi Covid-19 pada tahun 2020–2021 semakin menegaskan dan mempercepat kenyataan baru ini. Pedagang dan konsumen dapat berinteraksi secara langsung atau melalui platform seperti eBay atau Amazon.

Amazon memainkan beberapa peran penting dalam perdagangan modern, yang semuanya semakin penting selama dekade terakhir dan memberikan ilustrasi berguna tentang berbagai aspek perdagangan modern yang dimediasi teknologi. Dalam perannya yang paling familiar, Amazon bertindak sebagai pengecer barang kepada konsumen yang membeli langsung dari Amazon; mereka juga memproduksi sendiri beberapa barang tersebut melalui Amazon Marketplace, yang sepenuhnya terintegrasi dengan fungsi penjualan langsungnya. Amazon berfungsi sebagai platform di mana barang-barang dijual oleh pihak lain, dengan Amazon menerima potongan penjualan yang signifikan sebuah bisnis yang mungkin secara mengejutkan menyumbang lebih dari setengah total penjualan keseluruhannya. Dengan demikian, sementara Amazon terus membangun dan persediaan lebih banyak di gudang untuk mencoba meningkatkan kecepatan dan kemudahan pengiriman produk, produsen dan banyak penjual barang sebenarnya berada jauh dari pembeli. Yang terakhir, melalui Amazon Web Services, Amazon bertindak sebagai tuan rumah bagi banyak bisnis online melalui layanan cloud-nya, yang pada dasarnya menyewakan hak untuk menggunakan server dan perangkat lunaknya untuk interaksi pelanggan, analisis data, manufaktur dan manajemen pasokan, dan sebagainya. Dengan kata lain, bahkan perdagangan online yang tidak dilakukan di platform Amazon sering kali mengandalkan teknologinya.

Mengingat peran sentralnya dalam banyak aspek e-niaga, tidak mengherankan jika kekayaan Jeff Bezos, pendiri dan CEO Amazon, membengkak hingga lebih dari Rp.200 miliar karena saham perusahaannya naik lebih dari 85% selama tiga kuartal pertama tahun 2020. Sementara sebagian dari peningkatan kontrak online selama pandemi ini pada akhirnya akan surut, dan sebagian besar peningkatan tersebut kemungkinan akan bertahan lama. Mencerminkan harapan ini, pengecer tradisional telah mengajukan permohonan keringanan kebangkrutan dalam jumlah besar, banyak di antara mereka yang melakukan likuidasi dibandingkan mencoba melakukan reorganisasi. Transaksi online berbeda dari transaksi tradisional dalam banyak hal, beberapa di antaranya menguntungkan konsumen dan ada

pula yang tidak. Di antara perubahan-perubahan lainnya, transaksi konsumen kini lebih sering melintasi batas negara dibandingkan sebelumnya, melibatkan tingkat kecepatan dan otomatisasi yang jauh lebih besar, dan bergantung pada bentuk-bentuk baru intermediasi pasar dan, seringkali, manipulasi. Praktik-praktik transaksi baru memerlukan bentuk-bentuk peraturan baru, namun undang-undang tersebut gagal untuk mengimbanginya. Teknologi telah memberdayakan pedagang dan platform untuk melampaui hukum konsumen dan perlindungan konsumen. Perlindungan hukum menjadi tidak memadai mengingat realitas praktik transaksi berbasis internet yang umum. Hal ini disebabkan oleh lemahnya undang-undang dan seperangkat regulator yang terhambat oleh keterbatasan politik, hukum, dan kelembagaan.

Kelemahan-kelemahan dalam regulasi kontrak konsumen di Amerika Serikat, termasuk lintas batas negara, dan menilai usulan solusi teknologi dan pasar, yang dianggap jauh lebih menjanjikan dibandingkan dengan kenyataan yang ada. Hal ini memerlukan solusi yang melibatkan perubahan undang-undang, kelembagaan, dan teknologi yang sepadan dengan cakupan permasalahan aktual yang ditimbulkan oleh dunia perdagangan konsumen yang sudah terglobalisasi dan digital.

5.2 UNDANG-UNDANG DAN LEMBAGA HUKUM KONSUMEN

Undang-undang dan lembaga hukum melindungi konsumen dengan berbagai cara dalam bertransaksi dengan pedagang. Transaksi konsumen dinilai memerlukan perlindungan khusus karena beberapa alasan. Pedagang adalah pelaku yang terspesialisasi dan berulang, yang dapat memanfaatkan keahlian mereka untuk mengubah skala proses transaksi demi keuntungan mereka. Mereka mempunyai setiap peluang dan insentif untuk mengembangkan pengetahuan yang mendalam dan terperinci mengenai produk, pasar, dan konsumen mereka.

Kendala reputasi dan pasar membatasi eksploitasi mereka terhadap posisi superior mereka sampai tingkat tertentu namun tidak sepenuhnya menutupi ketidakseimbangan tersebut. Sejumlah besar penelitian di bidang psikologi perilaku dan ekonomi telah memberikan pemahaman yang semakin menyeluruh tentang aspek-aspek khusus dari konsumen. menarik. Selain itu, tidak semua konsumen mempunyai situasi yang sama. Kelompok konsumen yang rentan memerlukan perlindungan yang lebih besar. Hal ini mungkin mencakup mereka yang memiliki kerentanan tradisional seperti usia lanjut atau kurangnya pendidikan, namun juga mereka yang tidak memiliki akses terhadap teknologi, termasuk teknologi pembayaran.

Memahami regulasi perdagangan konsumen online lintas batas di Amerika Serikat memerlukan pemahaman terhadap undang-undang dan otoritas yang berbeda-beda. Yang paling jelas, kontrak konsumen lintas batas harus tunduk pada prinsip-prinsip common law yang telah lama dikembangkan oleh pengadilan, serta, di wilayah tertentu, undang-undang seperti Uniform Commercial Code dan Magnuson-Moss Guarantee Act. Namun pengaturan berbagai aspek transaksi konsumen masih tunduk pada undang-undang kontrak dan perlindungan konsumen negara bagian yang tidak seragam. Baik undang-undang federal

maupun berbagai badan hukum negara bagian belum ditinjau ulang secara signifikan mengingat perubahan wajah transaksi konsumen, khususnya sebagaimana dimediasi oleh teknologi baru, meskipun banyak proposal telah dibuat selama bertahun-tahun.

Karena kurangnya pedoman legislatif yang berarti, pengadilan telah memperluas doktrin negara ini untuk mencakup transaksi online. Upaya pengadilan dalam hal ini mengalami hambatan dan kontroversial. Misalnya saja, pengadilan kesulitan menerapkan gagasan tradisional tentang persetujuan dalam konteks kontrak adhesi, yang sering kali berupaya mengalihkan perselisihan ke arbitrase atau memberlakukan pembatasan pada pilihan tempat, gugatan kelompok atau prosedur litigasi agregat lainnya, dan upaya hukum yang tersedia. Meskipun masalah-masalah ini sudah ada sebelum peralihan ke perdagangan online, masalah ini telah menjadikannya lebih mendesak, karena semakin banyak transaksi yang diatur oleh syarat dan ketentuan yang panjang dan dibuat khusus oleh para pedagang. Pertahanan tradisional seperti sikap tidak berbudi luhur dan penipuan konsumen telah terjadi. penerapan yang tidak jelas ketika diminta oleh konsumen yang menentang persyaratan yang terkandung dalam perekat, kontrak online, atau serangkaian *"kebijakan"* online yang mungkin merupakan bagian dari kontrak atau tidak yang paling penting adalah apa yang disebut *"kebijakan privasi."*

Pedagang menjadi lebih canggih dalam menghadirkan antarmuka penjualan yang disesuaikan berdasarkan karakteristik konsumen tertentu. Perusahaan menggunakan kecerdasan buatan dan analitik "Big Data" untuk mengidentifikasi pelanggan yang mungkin lebih rentan terhadap promosi penjualan tertentu atau yang mungkin bersedia membayar lebih dari harga yang dibebankan kepada pelanggan lain. Perusahaan bahkan berupaya untuk menghalangi pelanggan tertentu yang tidak diinginkan atau memaksakan perjanjian penyelesaian sengketa yang lebih ketat terhadap pelanggan yang profilnya menunjukkan bahwa mereka cenderung mengajukan tuntutan hukum, untuk mengurangi kemungkinan litigasi atau dengan kata lain, untuk mengurangi kemungkinan adanya akuntabilitas atas praktik penyalahgunaan.

Meluasnya perbedaan pendapat mengenai orientasi dan ketidakpastian bidang hukum ini ditunjukkan dengan adanya pertikaian yang luar biasa. Pada bulan Mei 2019, usulan Pernyataan Ulang Undang-Undang, Kontrak Konsumen yang sudah lama tertunda, yang dirancang, direvisi, dan dipertahankan oleh tiga reporter ulung, gagal mendapatkan persetujuan dari American Law Institute. Selanjutnya membahas perselisihan ini, yang dengan tepat menggambarkan tantangan transaksi konsumen pada momen konflik ini. Usulan Pernyataan Kembali menghadapi tentangan keras baik dari pendukung konsumen maupun pendukung komunitas bisnis. Kontroversi tersebut berpusat pada beberapa ketentuan yang dimaksudkan untuk memperjelas bagaimana hukum kontrak seharusnya diterapkan pada transaksi konsumen online. Upaya para wartawan untuk mengusulkan pendekatan yang seimbang gagal karena para pendukung dari kedua belah pihak merasa bahwa keseimbangan akhir mungkin lebih menguntungkan mereka; beberapa dekade setelah perdagangan mulai beralih ke online, undang-undang tersebut masih belum stabil sehingga harapan akan keuntungan besar muncul di kedua belah pihak.

Sejumlah ciri praktis perdagangan modern berinteraksi dengan berbagai badan hukum yang menghalangi konsumen memberikan solusi efektif terhadap berbagai jenis kerugian. Masalahnya lebih dari sekadar doktrin kontrak. Undang-undang tanggung jawab produk dikembangkan sebagai bagian dari undang-undang tort AS, bukan kontrak, meskipun tentu saja hal ini menjadi latar belakang setiap transaksi. Hal ini memberikan serangkaian perlindungan penting bagi konsumen yang dirugikan oleh cacat pada produk yang diproduksi secara massal. Namun hal ini dilemahkan oleh struktur perdagangan online yang semakin meningkat. Transaksi berbasis platform telah mengurangi tanggung jawab atas cacat produk yang tidak langsung terlihat oleh pembeli atau pengguna barang. Platform seperti Amazon telah berusaha untuk menghindari tanggung jawab atas produk yang mereka jual "hanya" sebagai pasar. Namun penjual yang "asli" mungkin sulit diidentifikasi, sulit untuk dituntut lintas negara, atau "bukti penilaian" (yaitu, kurangnya sumber daya yang memadai untuk membayar keputusan atau dengan mudah dapat melunasi hutang keputusan dalam keadaan bangkrut), sehingga pelanggan yang dirugikan tidak mendapatkan ganti rugi. Baik faktor hukum maupun reputasi yang melindungi konsumen dalam interaksi ritel yang lebih tradisional sering kali hilang dalam transaksi online. Hukum perusahaan juga berperan dalam hal ini; hal ini mempermudah menjalankan bisnis melalui entitas cangkang dengan sedikit akuntabilitas bagi pemilik atau operator akhir. Dalam transaksi online, konsumen sering kali kurang mengenal penjual tertentu dan kecil kemungkinannya untuk melakukan kontak lebih dari satu kali. Produsen dan penjual produk berkualitas rendah pada akhirnya mungkin harus menghadapi tanggung jawab, baik karena dikeluarkan dari platform atau kehilangan bisnis karena ulasan negatif, namun proses ini membutuhkan waktu, dan dalam periode jeda, konsumen menjadi sangat terekspos. Dan tentu saja, entitas "etalase" baru dapat dengan mudah dibentuk, sehingga berpotensi memulai seluruh proses dari awal lagi. Semakin banyaknya produsen dan penjual yang berada di luar batas negara dari konsumen membawa tambahan batasan praktis dan hukum yang mempersulit proses produksi. konsumen untuk mendapatkan ganti rugi. Faktor-faktor praktis ini melemahkan perlindungan hukum – peraturan perundang-undangan tidak sesuai dengan kenyataan yang ada.

Aturan prosedural juga berperan sebagai aspek penting dalam perlindungan konsumen, dan aturan tersebut semakin merugikan konsumen. Selain aspek prosedural dari undang-undang yang telah disebutkan, terdapat batasan-batasan lain yang juga penting. Sengketa sering kali dialihkan ke arbitrase, sehingga potensi penyelesaian apa pun jarang ada gunanya untuk dilakukan. Upaya hukum kolektif seperti gugatan kelompok (class action) menjadi lebih sulit karena adanya perubahan doktrin dan maraknya klausul anti-gugatan kelompok dalam kontrak adhesi.

Privasi juga menjadi semakin penting. Seperti yang diketahui sekarang, informasi konsumen merupakan komponen utama dari pertimbangan yang diterima oleh pedagang, dan hak untuk mengumpulkan dan mengeksploitasi informasi konsumen secara komersial adalah cara non-moneter utama di mana platform menerima kompensasi atas peran mereka sebagai perantara. Dunia usaha mengeksploitasi informasi pribadi konsumen tanpa henti. Meskipun perhatian meningkat dalam beberapa tahun terakhir, undang-undang privasi

masih belum berkembang di Amerika Serikat. Tidak adanya undang-undang privasi yang melindungi konsumen memungkinkan pedagang secara agresif dan diam-diam mengambil dan menggunakan data konsumen yang berharga, sehingga membebankan biaya yang sebagian besar tidak diketahui kepada konsumen yang terlibat dalam aktivitas komersial online. Bukan saja perlindungan substantifnya kurang, namun selain itu, pengadilan juga menerapkan batasan dalam membela konsumen yang informasi pribadinya telah disusupi. Batasan ini meningkatkan biaya dan risiko litigasi serta menghalangi konsumen untuk memperoleh ganti rugi.

Hal ini dan peraturan lainnya berdampak pada keseimbangan kekuasaan antara pedagang dan konsumen. Bahkan gambaran ini masih jauh dari sempurna. Terdapat undang-undang dan peraturan perlindungan konsumen di tingkat negara bagian dan federal, yang sering dikenal sebagai undang-undang UDAP, yang secara luas melarang tindakan atau praktik yang tidak adil atau menipu terhadap konsumen. Beberapa undang-undang jenis UDAP mengizinkan tindakan yang bersifat pribadi, namun undang-undang lainnya membebankan biaya kepada regulator untuk melakukan tindakan yang bersifat pribadi. kekuasaan eksklusif untuk menyelidiki potensi pelanggaran dan menegakkan peraturan ini. Hak konsumen untuk bertindak tunduk pada beberapa batasan praktis dan prosedural yang telah dibahas sebelumnya; Meskipun beberapa undang-undang UDAP mengatur ketentuan ganti rugi dan pengalihan biaya yang memfasilitasi klaim konsumen, sebagian besar tidak menyediakannya.

Para pembuat kebijakan di negara bagian pada umumnya kekurangan dana dan kekurangan staf. Selain itu, mereka masih rentan terhadap tekanan politik dan aktivitas mereka sangat berbeda-beda di setiap negara bagian. Pentingnya politik bagi para pembuat peraturan mungkin membuat mereka terikat pada dunia usaha di wilayah mereka dan kurang responsif terhadap kebijakan pemerintah. aktor atau regulator lintas batas. Selain itu, meskipun pembuat kebijakan sering berkolaborasi lintas negara, dalam beberapa kasus mereka mungkin tidak memiliki kapasitas atau kewenangan hukum untuk melakukan hal tersebut secara efektif.

Bagian ini telah memberikan gambaran lanskap hukum untuk kontrak konsumen online. Gambarannya suram, dan jelas bahwa masalahnya jauh melampaui hukum kontrak dan komersial. Namun, ada juga alasan untuk berharap: Setiap bidang yang disurvei sebelumnya tidak hanya mewakili bidang kelemahan saat ini namun juga potensi pengungkit kebijakan bagi pendukung konsumen, peluang potensial untuk mempengaruhi dan melakukan perubahan. Kemajuan dapat dicapai dalam berbagai bentuk dan dari banyak aktor—di tingkat global, nasional, negara bagian, atau lokal, dan dari lembaga yudikatif, eksekutif, dan legislatif.

5.3 BATASAN PTEKNOLOGI PADA PERLINDUNGAN KONSUMEN

Jika perkembangan teknologi berperan penting dalam merugikan kepentingan konsumen, apakah perkembangan teknologi juga berperan dalam membantu mereka? Tentu saja, teknologi telah memberikan banyak bantuan kepada konsumen: Meskipun bahaya dari

kontrak online masih diremehkan, kontrak konsumen online memang memberikan banyak keuntungan kepada konsumen dibandingkan konteks pembelian tradisional.

Berbelanja dari rumah lebih nyaman, pribadi, dan santai daripada pergi ke lokasi fisik dan berinteraksi dengan penjual langsung. Selain itu, e-niaga memungkinkan perbandingan belanja yang lebih mudah untuk berbagai macam barang, dengan informasi termasuk ulasan pengguna yang mudah diakses. Penghematan biaya dapat terjadi karena pedagang tidak perlu lagi mengelola lokasi fisik atau mempekerjakan staf bagian penjualan, serta meningkatnya persaingan di antara penyedia barang di luar wilayah geografis tertentu. Pada akhirnya, hal ini juga dapat memperluas akses terhadap perdagangan bagi mereka yang menghadapi keterbatasan terkait lokasi, transportasi, atau kesehatan. Dunia online adalah sebuah anugerah, misalnya, bagi mendiang ibu saya, yang senang berkontribusi pada kesejahteraan keluarga melalui belanja, namun, sebagai akibat dari penyakit Multiple Sclerosis progresif primer, ia menghabiskan lebih dari dua puluh tahun dengan mobilitas yang sangat terbatas, sehingga menjadikannya sebuah anugerah. sulit dan tidak nyaman untuk mengunjungi toko fisik.

Selain itu, teknologi telah diadaptasi untuk mengatasi beberapa kelemahan hukum konsumen. Beberapa pelaku terbesar dalam perdagangan online telah membangun perlindungan mereka sendiri bagi pelanggan, seiring mereka berupaya membangun kepercayaan konsumen terhadap pasar baru, sistem pembayaran, dan bentuk transaksi. Misalnya, platform online berupaya mencegah penipuan dan sering kali memberikan kompensasi kepada konsumen yang ditipu. Dengan biaya yang besar, mereka telah membangun infrastruktur untuk menyediakan mekanisme pembayaran yang dapat diandalkan bagi konsumen, hal ini sangat penting mengingat kelemahan sistem pembayaran global yang sudah ketinggalan zaman. Beberapa dari perlindungan ini mungkin akan tertanam sebagai norma pro-konsumen yang diharapkan terjadi di pasar online di masa depan.

Layanan penyelesaian sengketa online adalah salah satu "produk" paling menarik dan menjanjikan yang muncul di persimpangan antara perdagangan online dan perlindungan konsumen. Platform dan pasar telah berinvestasi secara signifikan dalam menyediakan cara yang murah dan relatif dapat diandalkan untuk menyelesaikan perselisihan mendasar antara penjual dan pembeli. Upaya penyelesaian sengketa online (ODR) yang dilakukan oleh platform seperti eBay menjanjikan penyelesaian berbagai perselisihan, khususnya dalam transaksi konsumen skala kecil, dengan harga dan kenyamanan yang membuat partisipasi konsumen menjadi realistis. Alat-alat ini merupakan program sederhana yang berupaya memfasilitasi penyelesaian dengan mewajibkan penyerahan bukti dan penjelasan secara online secara cepat oleh masing-masing pihak dan memberikan analisis yang sebagian besar bersifat otomatis terhadap banyak perselisihan yang biasa terjadi, seperti perselisihan mengenai kondisi produk pada saat kedatangan. Program-program tersebut juga dapat memfasilitasi mediasi atau arbitrase atas perselisihan, walaupun sering kali keputusan tersebut tidak mengikat: Pihak-pihak yang memilih untuk mengajukan tindakan hukum formal masih dapat melakukan hal tersebut, meskipun jumlah yang diperdebatkan jarang

mendukung langkah tersebut. Layanan penyelesaian sengketa dapat menjadi bagian yang diharapkan dari paket layanan yang disediakan oleh platform.

Semua manfaat dan perkembangan yang menjanjikan ini harus diakui, namun juga benar bahwa peralihan ke perdagangan online telah menambah biaya bagi konsumen dan pasar. Banyak di antaranya berkaitan dengan efek agregasi dan jaringan. Sebagian besar perdagangan online difasilitasi oleh sejumlah kecil platform yang telah memberikan keandalan dan kepercayaan seperti yang baru saja saya gambarkan. Meskipun platform dan pasar online memfasilitasi persaingan antar penyedia barang, mereka mengeksploitasi posisi oligopolistik mereka dan meraup keuntungan yang luar biasa. Banyak penyedia platform membebankan biaya yang sangat tinggi kepada pedagang yang menggunakan platform mereka, namun kekuatan pasar mereka memungkinkan mereka untuk mempertahankan struktur biaya ini. Pedagang, terutama pedagang kecil, merasa tidak punya pilihan. Selain itu, layanan penyedia platform memiliki biaya tersembunyi. Misalnya, Amazon dituduh gagal melakukan pengawasan terhadap barang palsu atau curian; mereka dituduh menggunakan posisi istimewanya untuk membuat dan menjual produk tiruannya sendiri dan melemahkan penjual asli barang-barang unik tersebut. Namun banyak penjual percaya bahwa mereka tidak bisa berhenti menjual produk di Amazon. Bahkan produsen sebesar Nike tidak mampu meyakinkan Amazon untuk memberikan perlindungan yang memadai dari produk “tiruan”; akhirnya Nike menarik diri dari melakukan penjualan langsung melalui Amazon: “Nike dilaporkan kesulitan mengendalikan pasar Amazon. Penjual pihak ketiga yang listingannya dihapus muncul begitu saja dengan nama yang berbeda. Ditambah lagi, produk resmi Nike mempunyai ulasan yang lebih sedikit, sehingga mendapat posisi yang lebih buruk di situs.

Bagi konsumen juga, penyaluran begitu banyak perdagangan melalui beberapa penyedia penting menimbulkan biaya yang signifikan, ada yang terlihat jelas dan ada yang tersembunyi. Misalnya, pasar menggunakan data konsumen yang disesuaikan untuk mendorong produk mereka dan melakukan diskriminasi harga. Mereka juga memonetisasi informasi pribadi konsumen dan data tentang perilaku konsumen dengan berbagai cara yang, setidaknya, tidak diketahui dengan baik oleh konsumen dan mungkin akan ditolak oleh banyak konsumen jika mereka memahami apa yang sedang terjadi dan mempunyai cukup kesempatan untuk menolak. Penyedia perdagangan internet menekankan harga dan kenyamanan, namun meskipun hal ini mungkin merupakan poin yang paling menonjol bagi sebagian besar konsumen, biaya e-niaga yang mudah diabaikan dan tersembunyi dapat berarti bahwa kesepakatan yang diperoleh konsumen tidak begitu baik.

Sedangkan untuk penyelesaian sengketa online (ODR), hal ini memberikan lapisan perlindungan yang penting namun, dalam bentuknya yang sekarang, memiliki keterbatasan yang signifikan. Portal ODR yang ada sebagian besar terbatas pada pengiriman, pembayaran, dan kondisi awal produk. Mereka berhasil menyelesaikan perselisihan sesuai dengan kewenangannya, namun memiliki keterbatasan yang tajam. Platform menolak keras ketika dihadapkan dengan klaim atas cedera pribadi atau cedera properti skala besar, seperti tempat tinggal yang hancur akibat kebakaran listrik yang disebabkan oleh cacat produk. Fokus yang terlalu sempit pada kontrak dan pembayaran tidak boleh mengalihkan perhatian

dari kurangnya perlindungan yang lebih luas, misalnya, tanggung jawab produk, praktik komersial yang melanggar hukum, dan skema pembiayaan yang melanggar hukum. Terlebih lagi, alat ODR memungkinkan penyedia layanan terpusat yang memiliki hak istimewa untuk mengumpulkan lebih banyak kekuatan pasar. Hal ini menimbulkan kekhawatiran mengenai harga, kurangnya akses konsumen terhadap teknologi, dan semakin meningkatnya konsentrasi informasi mengenai perilaku konsumen di tangan segelintir orang.

Namun yang lebih memprihatinkan, penggunaan alat ODR yang bertujuan mencari keuntungan berisiko menciptakan kelompok konsumen dan perselisihan yang memiliki hak istimewa karena teknologi penyelesaiannya sudah tersedia, sementara mereka yang tidak memiliki akses, atau mereka yang perselisihannya tidak dapat diselesaikan di platform, tidak diikutsertakan. Akses terhadap teknologi semakin mendominasi akses terhadap pasar, dan beberapa kelompok masih memiliki keterbatasan dalam kemampuan mereka untuk mengakses teknologi. ODR berfungsi paling baik, dari sudut pandang pedagang dan platform, sehubungan dengan perselisihan standar yang dapat diselesaikan dengan cepat, baik secara otomatis atau dengan sedikit keterlibatan manusia atau pertimbangan manajemen. Penyedia layanan nirlaba memiliki sedikit insentif untuk berinvestasi dalam prosedur ODR untuk menyelesaikan perselisihan yang memerlukan pertimbangan atau pengambilan keputusan yang lebih disesuaikan. Perselisihan yang tidak memenuhi kriteria yang ditetapkan oleh penyedia ODR akan diserahkan ke pengadilan atau arbitrase, dan pada kenyataannya, banyak tuntutan seperti itu tidak akan pernah diajukan, tidak peduli betapa pentingnya tuntutan tersebut dalam kebijakan publik. Dunia usaha akan berinvestasi dalam prosedur yang memadai untuk membangun kepercayaan terhadap platform mereka di kalangan konsumen utama, namun prioritas mereka tidak akan mencakup masalah distributif dan keadilan yang mungkin penting bagi masyarakat secara keseluruhan.

Pesan dari bab ini tentu saja bukanlah utopianisme teknologi, namun juga bukan pesimisme teknologi. Sebut saja realisme teknologi. Pendekatan pasar dan teknologi terhadap masalah perlindungan konsumen baru dalam perdagangan online memang cukup menjanjikan, namun hal tersebut tidak boleh dilebih-lebihkan.

Teknologi harus dimanfaatkan oleh pembuat undang-undang, regulator, dan pendukung konsumen untuk membantu konsumen mengatasi masalah perlindungan konsumen yang mewabah di era digital. Sehubungan dengan hal ini, terdapat upaya yang menjanjikan dalam mencari cara yang lebih baik bagi konsumen untuk mengorganisir diri mereka guna menekan pedagang dan mengerahkan kekuatan reputasi dalam hal perlindungan konsumen. Upaya-upaya ini masih terbatas cakupannya namun merupakan area yang menjanjikan untuk penelitian dan penelitian lebih lanjut. percobaan.

Bagian selanjutnya mengilustrasikan beberapa pertarungan hukum dan politik yang penting dalam perlindungan konsumen modern dengan berfokus pada perselisihan baru-baru ini mengenai Pernyataan Kembali Undang-Undang dan Kontrak Konsumen. Pekerjaan ini mencoba untuk membentuk kembali hukum kontrak agar sesuai dengan realitas praktik modern, untuk memberikan kejelasan bagi pedagang dan konsumen. Namun, hal ini

mendapat pertentangan sengit dari kedua belah pihak dan menunjukkan betapa terpecah dan tidak menentunya hubungan antara konsumen dan pedagang di era e-niaga.

5.4 KONSUMEN YANG MENOLAK MENGONTRAK "TAWAR-MENAWAR"

Pada tahun 2019, dalam kontroversi hukum konsumen yang paling sengit sepanjang sejarah, American Law Institute menolak menyetujui usulan Pernyataan Kembali Hukum dan Kontrak Konsumen. Para reporter Restatement adalah akademisi yang dihormati, semuanya telah melakukan pekerjaan penting dan inovatif yang berfokus pada praktik komersial modern dan perlindungan konsumen. Proyek ini mengalami beberapa revisi sebagai tanggapan atas kritik. Meskipun demikian, setelah melalui perjuangan yang sengit, proyek tersebut diajukan oleh anggota penuh ALI. Kegagalannya bahkan fakta bahwa proyek ini mendapat tentangan yang begitu sengit mengejutkan banyak orang, dan mungkin para wartawan sendiri.

Pernyataan Kembali ini merupakan sebuah upaya jalan tengah, sebuah upaya untuk memperjelas dan mengkonsolidasikan undang-undang kontrak di era perdagangan konsumen yang disederhanakan dan khususnya online. Sebuah tawaran besar terletak pada intinya: Pernyataan Kembali ini menyatakan bahwa persetujuan konsumen terhadap ketentuan-ketentuan kontrak yang ditulis oleh bisnis, baik sebelum atau di tengah-tengah hubungan kontrak, sebagian besar dapat diasumsikan, asalkan persyaratannya memenuhi standar dasar pemberitahuan, dan bahwa kebijakan privasi secara umum akan dimasukkan sebagai persyaratan dalam kontrak konsumen, yang semuanya dipertimbangkan agar menguntungkan kepentingan dunia usaha. Namun Pernyataan Kembali ini juga menekankan, dan bisa dibilang meningkatkan, akses konsumen terhadap berbagai pembelaan dan tantangan terhadap penegakan ketentuan kontrak. Hal ini bertujuan untuk merevisi doktrin ketidakwajaran dan penipuan, mempersulit perusahaan untuk menolak pernyataan prakontrak, menerapkan persyaratan kontrak yang tidak biasa atau mengejutkan, atau menggunakan "aturan pembuktian bersyarat" untuk menolak manfaat dari pernyataan yang dibuat sebelum kontrak bagi konsumen. saat terjadinya kontrak oleh wakil pedagang.36

Pernyataan Kembali ini dimaksudkan untuk didasarkan pada analisis yang cermat dan kuantitatif terhadap sejumlah besar kasus hukum yang relevan. Ternyata, analisis empiris yang menjadi dasar temuan-temuan utama proyek ini justru menjadi isu yang menyulitkan pihak-pihak yang menentangnya. Tantangan paling tajam terhadap Pernyataan Kembali diposisikan sebagai hal yang bersifat metodologis dan berpusat pada analisis Pernyataan Kembali terhadap kasus-kasus kontrak yang ada. Penekanan metodologis ini diperlukan karena para wartawan telah mengumandangkan pendekatan empiris kuantitatif dan inovatif mereka sebagai memberikan dasar yang kuat untuk kesimpulan mereka. Para penentang mempertanyakan bukti-bukti yang mendasarinya, dengan alasan antara lain bahwa hanya sedikit pengadilan yang benar-benar mendasarkan keputusan mereka pada prinsip-prinsip yang disajikan dalam Pernyataan Kembali dan bahwa terdapat banyak preseden yang mendukung kesimpulan yang berbeda atau bahkan berlawanan. Mereka berpendapat bahwa jumlah kasus hukum yang ada terlalu sedikit untuk mencapai konsensus dan bahwa

kasus hukum yang jarang itu sendiri bersifat samar-samar dalam mendukung prinsip-prinsip yang diumumkan dalam Pernyataan Kembali.

Pernyataan Kembali ini ditentang oleh koalisi yang paling luar biasa: Perwakilan kepentingan bisnis dan pendukung konsumen sama-sama menentangnya dengan sengit. Namun, aliansi dalam oposisi tidak menunjukkan aliansi dalam penalaran. Kepentingan bisnis paling mendapat perhatian dengan diperkenalkannya konsep dan istilah dari literatur akademis dalam Pernyataan Ulang tetapi tidak dikenal dalam kasus hukum, seperti konsep arti-penting; mereka takut bahwa pengadilan akan mengarahkan para pendukung konsumen kreatif ke jalur hukum yang tidak menguntungkan, sehingga mengganggu apa yang mereka anggap sebagai status quo yang secara umum menguntungkan.

Sebaliknya, sebagian besar pendukung konsumen mengungkapkan rasa frustrasinya terhadap gambaran konsensus hukum yang tegas mengenai masalah pembentukan dan persetujuan kontrak. Bagi sebagian dari mereka, tidak adanya hukum yang mengatur perkara itu sendiri mempunyai arti, hal ini menunjukkan bahwa bidang hukumnya masih belum jelas, atau bahkan mungkin para pedagang sengaja memastikan bahwa kasus-kasus yang "buruk" tidak akan dibawa ke pengadilan. Tidak diragukan lagi, banyak kasus yang diajukan ke arbitrase, diselesaikan melalui putusan, tidak menghasilkan opini tertulis, atau ditangani oleh regulator dan bukan melalui proses peradilan. Atau kerugian tersebut hanya "disamakan" oleh konsumen.

Dengan adanya kritik terhadap klaim metodologis proyek yang ambisius ini, para penentang menganggap proyek ini bukan sekedar "pernyataan kembali" undang-undang seperti yang telah diterapkan oleh pengadilan, namun sebagai upaya untuk membentuk dan memperjelas hal-hal yang masih belum matang dan belum terselesaikan. Hebatnya, dengan memanfaatkan banyak kesalahan empiris dalam Pernyataan Kembali dan menyerang karya empiris yang disajikan sebagai dasar utama proyek, para penentang sangat melemahkan proyek tersebut. Para penentang mampu mengalihkan perdebatan, memaksa para anggota Institut Hukum Amerika, yang mempertimbangkan pilihan mereka mengenai masalah ini, untuk tidak meratifikasi suatu tindakan yang telah disetujui oleh mayoritas pengadilan, namun untuk mengambil sikap berdasarkan keinginan normatif atas keseimbangan yang dicapai oleh Pernyataan Kembali.

Secara praktis, perdebatan empiris, meskipun penting, akan menjadi kepentingan akademis dan tidak akan menghancurkan proyek jika para penentang—atau mungkin salah satu dari dua kubu utama menganggap hasil substantif dari proyek tersebut cukup baik. Meskipun Pernyataan Kembali mempunyai pendukung,42 keberatan tersebut dipublikasikan secara luas dan penolakan pada pertemuan ALI telah diorganisir sebelumnya; upaya melawan rintangan untuk menggagalkan Pernyataan Kembali berhasil. Upaya ini tidak hanya mencerminkan upaya untuk melindungi integritas ilmu hukum empiris, meskipun tujuan tersebut mungkin penting bagi banyak orang yang menolaknya; upaya strategis yang rumit ini mencerminkan pertentangan yang kuat terhadap substansi "Tawaran Besar". Jadi, ada baiknya mempertimbangkan alasan substantif mengapa para pendukung menentang

Pernyataan Kembali dan bagaimana perdebatan tersebut mencerminkan pandangan yang lebih luas terhadap hukum kontrak konsumen di lingkungan saat ini.

Seperti telah disebutkan, Pernyataan Kembali ditentang keras oleh para pendukung terkemuka baik dari sisi pedagang maupun konsumen—sebuah koalisi yang membingungkan. Kepentingan bisnis menentang "Tawaran Besar" karena berisiko memperluas ketersediaan pertahanan konsumen. Mereka nampaknya percaya bahwa baik dalam arbitrase maupun pengadilan, mereka dapat unggul dalam pembentukan kontrak dan menyetujui serta mengalahkan standar pembelaan hukum yang ada. Dengan kata lain, mereka percaya bahwa perselisihan saat ini diatur oleh versi undang-undang kontrak yang relatif pasti dan ramah bisnis, lebih baik bagi mereka daripada Pernyataan Kembali, khususnya dengan upaya perluasan pembelaan yang tidak masuk akal dan penipuan yang berpotensi berisiko.

Dunia usaha mempunyai alasan untuk optimis. Pengadilan pada umumnya tampaknya percaya bahwa hakim harus menyesuaikan hukum adat tradisional dengan pentingnya merangsang perdagangan massal yang mudah, namun kebijakan publik atau permasalahan distribusi harus diserahkan kepada lembaga legislatif. Pengadilan sering kali mendasarkan keputusannya pada asumsi-asumsi yang naif mengenai perekonomian dan menggunakan alasan ekonomi yang sederhana dan tidak didukung secara empiris untuk mendukung "adaptasi" hukum umum terhadap praktik bisnis modern. Keputusan Mahkamah Agung Amerika Serikat yang terkenal kejam dalam Carnival Cruise Lines v. Shute memberikan contoh yang mudah. Dalam keputusan tersebut, mayoritas Pengadilan menerapkan klausul pemilihan forum yang mendukung perusahaan pelayaran, terhadap konsumen yang dirugikan serius dalam perjalanan mereka. sebuah kapal pesiar tetapi tidak mampu untuk mengajukan tindakan di forum pilihan perusahaan pelayaran tersebut. Klausul yang dipermasalahkan tercantum di antara banyak persyaratan cetak kecil lainnya pada tiket kapal pesiar yang diterima hanya setelah transaksi selesai. Pelanggan rupanya "menyetujui" istilah tersebut dengan tidak membatalkan pelayaran setelah menerima tiket.

Dalam membenarkan keputusannya, Pengadilan Karnaval menyatakan bahwa masuk akal bahwa penumpang yang membeli tiket yang memuat klausul forum seperti yang dipermasalahkan dalam hal ini mendapatkan keuntungan dalam bentuk pengurangan tarif yang mencerminkan penghematan yang dinikmati perusahaan pelayaran dengan membatasi forum yang dapat digugat.

Tentu saja, sama sekali tidak jelas apakah penghematan biaya Karnaval melebihi peningkatan biaya (dalam bentuk risiko) yang dikenakan pada semua pelanggan; atau bahwa kelebihan apa pun yang dihasilkan akan disalurkan ke konsumen dalam bentuk biaya yang lebih rendah daripada ke pemegang saham sebagai keuntungan tambahan, mengingat karakteristik pasar kapal pesiar yang sebenarnya, dan bukan dunia ideal yang terdiri dari pasar yang sangat kompetitif dan kaya informasi. Tampaknya Pengadilan mendasarkan keputusannya pada hal tersebut. Pengadilan juga gagal untuk mengakui kekhawatiran distributif yang diajukan: Haruskah konsumen secara keseluruhan mendapatkan

penghematan biaya dibandingkan dengan mereka yang tidak memiliki sumber daya untuk mengajukan perkara di tempat yang jauh?

Keputusan Carnival Cruise Line bukanlah satu-satunya keputusan yang menuruti asumsi pro-bisnis dan keekonomian untuk menegakkan ketentuan kontrak. Dunia usaha pada umumnya, meskipun tidak secara universal, mengandalkan pendekatan seperti ini dari pengadilan AS. Oleh karena itu, memberikan tantangan kepada konsumen terhadap penegakan persyaratan kontrak secara spontan merupakan risiko yang terlalu besar, bahkan jika hal tersebut memungkinkan pedagang untuk mengkonsolidasikan kemajuan yang mereka rasakan di bidang lain. Tampaknya, para pedagang takut akan adanya argumen-argumen praktik yang tidak masuk akal atau menipu yang muncul dari konsumen yang mungkin terikat oleh persyaratan standar yang tidak menguntungkan dalam kontrak adhesi pedagang. Para pedagang lebih memilih undang-undang yang berlaku saat ini karena undang-undang tersebut secara umum berasumsi bahwa persyaratan standar yang mereka sukai sudah ada dan hanya memberikan peluang sempit kepada konsumen untuk meminta pembelaan. Seperti telah disebutkan, karena pedagang dapat menggunakan arbitrase atau penyelesaian rahasia untuk "mengubur" kasus-kasus yang mana pembelaan tersebut mungkin akan berhasil, maka ketersediaan preseden pro-konsumen menjadi lebih kurang dari yang seharusnya. Dalam pandangan para pedagang, Pernyataan Kembali ini berisiko memberi konsumen terlalu banyak cara untuk berbuat jahat memberikan kejelasan mengenai pertahanan yang sebagian besar masih berada dalam bayang-bayang.

Sebaliknya, para pendukung konsumen berargumentasi bahwa prinsip-prinsip yang diusulkan kurang memberikan penekanan pada upaya memastikan bahwa konsumen benar-benar memahami dan menyetujui ketentuan-ketentuan tersebut. Para pendukung konsumen menolak anggapan bahwa konsumen harus menanggung beban untuk mendesak pembelaan terhadap persyaratan kontrak. Daripada mengizinkan hakim untuk menyangkal bahwa ketentuan-ketentuan yang pernah disepakati yang diakui semua orang, merupakan kenyataan yang mungkin terjadi dalam banyak kontrak konsumen pernyataan Kembali akan memaksa para hakim untuk membatalkan ketentuan-ketentuan yang dianggap sah. Para pendukung konsumen merasa skeptis bahwa pengadilan akan menerima pembelaan seperti itu secara teratur, bahkan ketika hal tersebut memang pantas dilakukan. Meskipun pandangan mereka berbeda-beda, para pendukung konsumen pada umumnya berpandangan bahwa beban untuk menetapkan keberlakuan persyaratan kontrak harus dialihkan ke pedagang. Mereka berpendapat bahwa untuk menegakkan persyaratan tertentu, pedagang harus diminta untuk menunjukkan bahwa persyaratan tersebut tidak bersifat kasar atau tidak adil dan bahwa proses kontrak tidak menipu konsumen yang bersangkutan. Sebagian besar juga percaya bahwa sejumlah persyaratan yang tidak adil harus dilarang secara eksplisit dan menyeluruh, tidak hanya berdasarkan undang-undang perlindungan konsumen namun berdasarkan hukum kontrak itu sendiri. Ketentuan-ketentuan arbitrase, dan khususnya ketentuan-ketentuan yang melarang gugatan kelompok (class action), adalah contoh yang baik dari hal tersebut.

Para pendukung konsumen memprioritaskan pelestarian akses terhadap pengadilan, dan terhadap doktrin-doktrin perlindungan konsumen berdasarkan undang-undang yang berlaku umum dan modern. Mereka mempunyai banyak argumentasi yang kuat. Pertama, doktrin tradisional menyajikan gagasan persetujuan yang lebih kuat dibandingkan yang menjadi norma dalam kontrak online. Sekali lagi, meskipun perdebatan mengenai kontrak adhesi tidak hanya terjadi dalam konteks e-commerce, perdebatan mengenai kontrak adhesi menjadi lebih penting ketika kontrak tersebut berupaya mengendalikan sebagian besar pembelian barang dan jasa. Para pendukung konsumen berpendapat bahwa pengadilan harus lebih skeptis terhadap upaya pedagang untuk memukul semua konsumen dengan "ketentuan layanan" yang tidak masuk akal, terlepas dari pemahaman atau persetujuan konsumen yang sebenarnya.

Pendukung konsumen juga mempunyai argumen yang kuat berdasarkan praktik pedagang yang sebenarnya (walaupun argumen ini tampaknya tidak muncul dalam perdebatan Pernyataan Kembali). Seperti yang ditunjukkan oleh banyak penelitian luar biasa, dunia usaha semakin banyak menggunakan kecerdasan buatan dan sejumlah besar data untuk menargetkan konsumen individu dan menentukan harga serta aspek lain dari penawaran mereka kepada konsumen sering kali justru untuk memaksimalkan kemungkinan pembelian sekaligus meminimalkan pemahaman sebenarnya tentang istilah-istilah yang tidak diinginkan. para pendukung konsumen berpendapat bahwa hal ini adalah hal yang sangat sinis dan munafik jika bisnis menyesuaikan pengalaman pelanggan demi keuntungan mereka untuk kemudian memprotes bahwa mereka tidak boleh dipaksa untuk mempertimbangkan kembali ekspektasi wajar konsumen atau persetujuan mereka terhadap kontrak. ketentuan. Karena pedagang dapat dan memang menyesuaikan interaksi mereka dengan pelanggan dalam berbagai cara, sering kali memanfaatkan keuntungan informasi mengenai konsumen individu, mereka tidak dapat diizinkan untuk menyangkal pengetahuan individu atau kemampuan untuk menyesuaikan interaksi untuk memastikan bahwa praktik kontrak benar-benar mencapai sesuatu seperti cita-cita kontraktual berupa perjanjian yang dibuat oleh pihak-pihak yang memiliki informasi demi keuntungan bersama.

Pada akhirnya, para pendukung konsumen menilai bahwa apa pun yang diperoleh konsumen dari Pernyataan Kembali tidak layak untuk mengkonsolidasikan kerugian mereka dalam hal persetujuan/formasi. Para pendukung konsumen mungkin merasa bahwa pada masa pemerintahan Partai Republik tidak menunjukkan banyak perhatian terhadap isu-isu konsumen. , mereka tidak punya tempat tujuan selain naik. Pendukung konsumen mungkin juga berpikir bahwa keadaan sedang berubah; dan memang benar, sikap masyarakat terhadap teknologi telah berubah. Misalnya, akhir-akhir ini perhatian publik tertuju pada masalah privasi konsumen dan bahaya sentralisasi kekuasaan dan uang di tangan segelintir perusahaan besar. Ketika pandangan berubah, penolakan politik terhadap undang-undang kontrak yang menguntungkan partai-partai ini mungkin akan meningkat. Pengadilan dan pembuat undang-undang mungkin lebih menerima perlindungan konsumen melalui undang-undang kontrak serta melalui badan hukum dan peraturan lain yang khusus berorientasi konsumen, meskipun hal ini masih harus dilihat.

5.5 REGULASI DAN TEKNOLOGI KONSUMEN DI ERA DIGITAL

Sebuah revolusi dalam perdagangan konsumen memerlukan revolusi dalam perlindungan konsumen. Revolusi pertama telah tiba; yang lainnya belum. Apakah kekuatan politik akan bersatu untuk memungkinkan perubahan hukum masih belum jelas, namun kebutuhannya jelas. Bagian ini membahas prospek perubahan dan bentuk-bentuk perubahan yang mungkin terjadi.

Perubahan terhadap undang-undang yang berlaku dapat membawa perbedaan yang jelas dan signifikan. Hal ini mencakup aturan-aturan substantif mengenai bagaimana dan syarat-syarat apa yang membentuk kontrak lihat perdebatan Pernyataan Kembali yang dibahas sebelumnya dan juga cara-cara prosedural untuk memperbaiki kerugian. Mungkin aspek hukum konsumen yang paling terkenal adalah bahwa kerugian akibat praktik bisnis yang salah mungkin, pada tingkat per konsumen, terlalu kecil untuk membuat tuntutan hukum menjadi layak untuk diajukan. Meskipun fakta ini diakui secara luas secara universal?, dampaknya terhadap undang-undang yang sebenarnya masih terbatas. Faktanya, akses terhadap penyelesaian kolektif telah menyempit dalam beberapa tahun terakhir; pada saat yang sama, karena undang-undang federal yang sangat pro-arbitrase, konsumen di Amerika Serikat sering kali terpaksa keluar dari pengadilan dan masuk ke forum arbitrase di mana sebagian besar klaim mereka dengan cepat dan diam-diam berakhir.

Sejauh ini, pengadilan membatasi kesempatan konsumen untuk mendapatkan ganti rugi secara hukum. Memastikan bahwa konsumen dapat bersatu dan mencari ganti rugi melalui gugatan kelompok (class action) dan bentuk gugatan kolektif lainnya akan menjadi salah satu cara yang menjanjikan untuk melakukan reformasi, seperti halnya memberikan ganti rugi menurut undang-undang dan biaya pengacara jika tindakan yang dilakukan tidak ekonomis. Selain perubahan legislatif dan peraturan, perubahan sikap sosial dapat menyebabkan hakim menjadi lebih mudah menerima adaptasi upaya hukum yang ada. Perubahan hukum mungkin sangat penting dalam bidang privasi konsumen. Seiring berjalannya waktu, beberapa kesimpulan mengenai data pribadi konsumen menjadi semakin jelas, tidak hanya bagi para ahli yang mungkin sudah mengetahuinya sejak awal, namun juga bagi banyak orang di masyarakat luas. Pertama, risiko dari masalah ini sangat besar bagi konsumen, karena penyalahgunaan informasi pribadi mereka dapat mengganggu setiap aspek kehidupan mereka dalam masyarakat yang jenuh dengan internet, mengganggu keamanan pribadi, kehidupan sosial, dan akses terhadap pekerjaan, perumahan, kredit, dan akses terhadap informasi pribadi. perdagangan. Kedua, perusahaan tidak akan cukup menjaga diri mereka sendiri dan dinamika pasar tidak dapat dipercaya untuk melindungi data. Pada akhirnya, perlindungan data konsumen memerlukan intervensi legislatif, setidaknya beberapa di antaranya memerlukan koordinasi nasional dan bahkan internasional agar dapat berhasil. Beberapa wilayah hukum telah mengesahkan undang-undang yang mewakili langkah awal yang bermanfaat dalam hal ini, namun sebagian besar masih lamban, bahkan belum memulai perjalanan panjang menuju regulasi substantif dan prosedural yang tepat mengenai dimensi kehidupan dan kehidupan modern yang penting dan menantang perdagangan.

Membina lembaga regulasi juga penting untuk perlindungan konsumen di era digital. Lembaga pengatur memainkan peran penting dan memiliki banyak aspek dalam perlindungan konsumen. Pertama, lembaga pengatur merupakan penghubung penting antara hukum yang tertulis dan hukum yang berlaku. Konsumen dan pendukungnya jarang dapat melakukan tindakan hukum dengan biaya yang efektif, terutama dalam kondisi saat ini, yang tidak mendukung bentuk-bentuk penyelesaian kolektif. Para pembuat kebijakan dapat menyelidiki dan mengambil tindakan yang mungkin tidak dapat dilakukan oleh pihak lain, misalnya karena tingkat kerumitan yang tinggi atau karena kerugian yang ditimbulkan pada masing-masing konsumen relatif kecil. Kedua, pembuat peraturan sering kali dapat mengeluarkan peraturan baru dan mengeluarkan panduan, sehingga dapat merespons tantangan-tantangan yang muncul dengan lebih gesit dibandingkan dengan pembuat undang-undang. Ketiga, regulator berperan dalam penelitian, melalui pengumpulan dan agregasi informasi, serta memberikan analisis terhadap praktik dan tren industri. Dengan memberikan panduan mengenai isu-isu yang muncul, dengan mengumpulkan dan menyebarkan informasi dan analisis, dan dengan menyediakan titik fokus untuk advokasi, regulator dapat membantu memfasilitasi organisasi dan aktivisme konsumen.

Namun seperti yang disurvei, regulator mempunyai keterbatasan dalam berbagai hal. Banyak di antara mereka yang tidak memiliki kewenangan hukum untuk mengajukan klaim tertentu, mengumumkan peraturan tertentu, atau mengambil tindakan lain yang akan melayani kepentingan publik. Yang lainnya kekurangan dana. Sifat perdagangan digital yang bersifat lintas batas menambah lebih banyak kesulitan. Karena tidak ada regulator konsumen transnasional yang efektif atau sarana untuk melakukan kerja sama regulasi reguler, regulator mungkin tidak memiliki kewenangan untuk menangani permasalahan tersebut, atau bahkan motivasi konsumen yang dirugikan di luar yurisdiksi tertentu mungkin tidak dapat memberikan tekanan yang cukup kepada otoritas yang ditunjuk untuk mengatur dengan baik. bisnis yang terhubung dalam yurisdiksi tersebut.

Sangat mudah untuk melihat bahwa regulator dapat terbantu dengan peningkatan pendanaan; melalui otorisasi undang-undang untuk mengatur dan menegakkan, termasuk lintas batas negara dan melalui kerja sama yang lebih besar dengan otoritas lain; dan dengan upaya untuk mendorong penelitian dan pengembangan alat dan pendekatan baru. Sekali lagi, meskipun langkah-langkah tersebut mungkin terlihat mudah, perubahan dalam sikap politik dapat membawa perubahan yang cepat. Penting juga untuk diingat bahwa di Amerika Serikat, masing-masing negara bagian mempunyai kekuatan untuk melakukan banyak dari langkah-langkah tersebut. melangkah sendiri; California, New York, dan negara-negara lain telah mengesahkan undang-undang dan memperkuat lembaga perlindungan konsumen dalam beberapa tahun terakhir.

Regulasi itu sendiri dapat mengambil bentuk-bentuk baru, misalnya, sebagai kombinasi perangkat teknologi dan hukum. Profesor Lauren Willis telah mengusulkan kombinasi perlindungan hukum dan teknis dalam bentuk apa yang disebutnya “regulasi berbasis kinerja.” Ketika diterapkan pada kontrak konsumen, modelnya akan mengharuskan perusahaan untuk menunjukkan bahwa pelanggan mereka mengetahui apa yang telah

mereka sepakati untuk ketentuan kontrak konsumen yang mengikat. Usulannya terdengar aneh dari sudut pandang peraturan tradisional, namun hal ini muncul dari pengamatan mendalam tentang bagaimana pedagang sebenarnya terlibat dalam perdagangan online. Peraturan ini memperhitungkan strategi pemasaran dan penjualan yang baru dan mungkin bukan hanya merupakan bentuk regulasi efektif yang paling efektif namun juga paling murah.

Penyelesaian sengketa secara online juga dapat memberikan keringanan nyata bagi konsumen. Meskipun upaya ODR yang paling maju masih merupakan upaya yang dikembangkan oleh pihak swasta, ODR mempunyai potensi yang cukup besar. Dengan pengawasan publik untuk memastikan bahwa kekhawatiran terhadap keadilan dan akses menjadi lebih dikedepankan, ODR dapat secara signifikan menurunkan biaya penyelesaian sengketa dan dengan demikian meningkatkan kemampuan untuk memperbaiki berbagai bentuk kerugian konsumen yang saat ini "ditanggung bersama oleh konsumen." Sekali lagi, teknologi adalah hal yang sangat penting. tidak ada obat mujarab; ini bukan sekedar penerapan sistem ODR yang siap pakai untuk menyelesaikan semua perselisihan konsumen. Namun mengingat banyaknya kegagalan dalam sistem penyelesaian sengketa konsumen yang ada, ODR merupakan jalan penting bagi potensi perubahan dan perbaikan status quo.

Kesimpulan

Perlindungan konsumen sangat penting, karena dampak konsumen terhadap perekonomian sangat besar, sehingga melindungi dan memfasilitasi berfungsinya pasar konsumen secara sehat adalah hal yang berharga, namun juga karena terdapat nilai independen dalam perlindungan konsumen, khususnya terhadap individu yang rentan. Mengizinkan produsen dan penjual mengambil keuntungan dari konsumen berarti mengabaikan komitmen dasar masyarakat terhadap kesetaraan dan peluang.

Bab ini berargumentasi bahwa kontrak konsumen di era digital menghadirkan tantangan nyata dan saat ini dimana struktur hukum, peraturan, teknologi, dan sosial kita saat ini tidak memadai. Praktik bisnis telah berubah dengan cepat, mengubah pasar konsumen. Namun kewaspadaan terhadap peraturan masih kurang. Perangkat hukum masih tertinggal, dan dukungan publik terhadap lembaga pengatur tidak memadai.

Pekerjaan perlindungan konsumen tidak pernah selesai. Undang-undang dan peraturan yang diperlukan untuk menjamin akses konsumen terhadap kebutuhan hidup harus berkembang seiring dengan berkembangnya cara konsumen berinteraksi dengan pasar dan produk. Mengatasi tantangan perlindungan konsumen saat ini secara memadai memerlukan keterlibatan teknologi, namun kita tidak dapat mengharapkannya. kemajuan nyata dengan hanya mengandalkan teknologi secara pasif. Sebaliknya, mengembangkan teknologi baru dan bentuk hukum perlindungan konsumen yang kita perlukan memerlukan komitmen baru terhadap penelitian, organisasi politik, pengacara kepentingan publik, dan bentuk keterlibatan sosial lainnya.

BAB 6
PANDANGAN HUKUM KONSUMEN DI ERA DIGITAL

6.1 PENDAHULUAN

Kontrak konsumen dan peraturan hukumnya merupakan salah satu bidang inti hukum UE dan konsep pasar tunggal Eropa di Uni Eropa. Pasal 114(1)(2) Traktat tentang Fungsi Uni Eropa (TFEU) memungkinkan adanya harmonisasi ketentuan-ketentuan yang "tujuannya adalah pembentukan dan berfungsinya pasar internal", yang mencakup isu-isu konflik - Hukum Sumeria. Selain itu, Art. 38 Piagam Hak-Hak Dasar Uni Eropa (CFR) menjamin perlindungan konsumen tingkat tinggi sebagai hak dasar. Pada saat yang sama, digitalisasi terus berkembang pesat, terus menerus menantang hukum dan menuntut adanya reaksi dari pihak hukum. Dengan latar belakang ini, tampaknya ada harapan untuk menjelaskan bagaimana pesatnya proses digitalisasi mempengaruhi bidang kontrak konsumen dari perspektif Eropa. Untuk melakukan hal ini, pertimbangan berikut akan fokus pada contoh kontrak bisnis-ke-konsumen (B2C) untuk penjualan barang konvensional di lingkungan yang semakin digital, khususnya dalam bentuk penjualan online. Kita mungkin bertanya-tanya apakah, dalam menelusuri hubungan antara kontrak konsumen dan kemungkinan munculnya hukum digitalitas global, menganalisis konten kontrak yang sudah "didigitalkan" akan lebih bermanfaat. Pendekatan tersebut dapat berfokus, misalnya, pada kontrak penyediaan konten digital yang baru-baru ini menjalani proses harmonisasi di UE.

Namun, untuk mengamati kemungkinan munculnya pola "kode digital" dalam undang-undang konsumen, mungkin akan lebih meyakinkan jika kita berfokus pada jenis kontrak tradisional, seperti penjualan barang, yang berasal dari dunia offline dan menanyakan apakah dan sejauh mana hal tersebut dipengaruhi oleh pola digitalitas baru.

Argumen utama bab ini adalah, meskipun tidak ada undang-undang yang komprehensif dan terpisah untuk penjualan online lintas negara dalam konteks Eropa, undang-undang penjualan secara umum sangat dipengaruhi oleh paradigma baru penjualan digital. Dalam paradigma ini, tujuan utama hukum kontrak tidak lagi melindungi otonomi individu para pihak dan menyeimbangkan kepentingan mereka, namun semakin melindungi dan memfasilitasi pasar. Dalam skenario tersebut, perspektif hukum kontrak yang berpusat pada partai digantikan oleh perspektif yang berpusat pada pasar. Peralihan ke paradigma pasar ini tidak hanya terbatas pada hukum kontrak substantif saja, namun juga mencakup teknik pengaturan dalam hukum perdata internasional, penegakan hukum, dan perkembangan praktik kontrak swasta.

Analisis berikut akan dilanjutkan dalam beberapa langkah: Setelah melihat lebih dekat konsep pendekatan hukum kontrak yang berpusat pada pasar, peran utamanya dalam penjualan konsumen akan ditelusuri di berbagai sub-bidang. Hal ini termasuk yurisdiksi internasional dan konflik hukum, isu terkait penerapan hukum konsumen UE ekstra-teritorial, tren penting dalam undang-undang penjualan substantif UE, cara-cara alternatif penyelesaian sengketa dan penegakan hukum.

6.2 PENDEKATAN HUKUM KONTRAK YANG BERPUSAT PADA PASAR

Dengan semakin pentingnya penjualan online di pasar digital, kita dapat menyaksikan paradigma baru hukum konsumen, yaitu pergeseran dari perspektif hukum kontrak konsumen yang berpusat pada partai menjadi perspektif yang berpusat pada pasar.

Untuk memahami pergeseran ini, ada baiknya kita menjelaskan paradigma klasik hukum kontrak yang tertanam dalam tradisi Eropa Kontinental, khususnya dalam Kitab Undang-undang Hukum Perdata Jerman (Bürgerliches Gesetzbuch). KUH Perdata Jerman menganut konsep normatif yang bisa disebut sebagai perhitungan "pribadi" dalam hukum kontrak. Konsep ini mengklasifikasikan sebuah kontrak, pertama dan terutama, sebagai tindakan otonom para pihak dan bertujuan untuk memastikan keseimbangan kepentingan yang memadai antara para pihak. mereka. Tolok ukur keadilan kontrak ditentukan oleh gagasan otonomi swasta. Para pihak memanfaatkan kontrak sebagai sarana untuk secara independen mengatur kondisi kehidupan mereka dan untuk mencapai tujuan yang tidak dipertanyakan atau disalurkan oleh hukum kontrak. Hal ini pada umumnya menghasilkan kerangka hukum formal yang tidak dimaksudkan untuk melayani kepentingan mereka sendiri. kebijakan ekonomi bertujuan tetapi untuk mengatur hubungan hukum pribadi. Konsisten secara logika, kerangka hukum ini merupakan hukum perdata umum yang berlaku terlepas dari apakah para pihak dalam suatu kontrak adalah anggota kelompok pasar tertentu seperti pedagang atau konsumen. Fokusnya adalah pada subjek hukumnya dan bukan pada keberadaannya di pasar.

Sebaliknya, undang-undang konsumen UE dalam versi digitalnya kurang fokus pada perlindungan otonomi individu dan menyamakan kepentingan semua pihak, namun lebih fokus pada perlindungan dan fasilitasi pasar. Dalam konteks ini, kita dapat menemukan kaitan yang kuat dengan tujuan kebijakan untuk mendorong pasar tunggal Eropa, khususnya dengan memperkuat konsumsi lintas batas negara. Tujuan menyeluruh ini menyebabkan perspektif mikro dari hubungan kontrak pribadi digantikan oleh perspektif makro. perspektif pasar. Akibatnya, fokus normatif bergeser dari pihak-pihak yang terikat kontrak sebagai subjek hukum individual ke pemikiran yang lebih luas dalam kelompok pasar seperti pedagang dan konsumen. Oleh karena itu, hukum kontrak UE tidak hadir sebagai hukum perdata umum melainkan sebagai hukum komersial jenis baru dengan fokus pada kontrak B2C.

Setelah menguraikan dikotomi antara perspektif hukum kontrak yang berpusat pada partai dan perspektif yang berpusat pada pasar, ada dua peringatan yang tampaknya penting. Pertama, ada yang berpendapat bahwa fokus pada fasilitasi pasar yang terdapat dalam undang-undang kontrak UE bukanlah sesuatu yang baru di era digitalisasi, namun selalu menjadi inti dari gagasan pasar tunggal Eropa. Secara khusus, konsep UE mengenai fasilitasi pasar tunggal perlindungan konsumen tidak pernah terbatas pada tujuan menciptakan lingkungan hukum di mana konsumen memiliki sarana untuk membuat keputusan otonom yang substansial dalam perspektif klasik hukum kontrak yang berpusat pada partai. Sebaliknya, pendekatan UE, bahkan sebelum munculnya digitalisasi, telah memberikan penekanan yang kuat pada peningkatan kepercayaan konsumen dalam konteks

hubungan lintas batas dan peningkatan konsumsi. Namun, konsumsi lintas batas oleh konsumen sangat terbatas. pada tingkat praktis sebelum munculnya penjualan online digital. Tentu saja, para pedagang dapat secara fisik mengirimkan barang mereka melintasi perbatasan untuk langsung menawarkannya kepada konsumen di seluruh Eropa, dan UE telah lama melakukan yang terbaik untuk mendukung proses ini. Namun hanya dengan adanya kesempatan bagi konsumen untuk "menjangkau" melalui pesanan digital maka pendekatan kontrak konsumen yang berpusat pada pasar dapat mencapai momentum penuh. Oleh karena itu, tidak mengherankan jika UE sendiri mencanangkan paradigma baru dengan agendanya untuk mengubah pasar tunggal Eropa menjadi "pasar tunggal digital".

Kedua, adalah suatu kesalahan untuk mengasumsikan adanya kontradiksi murni antara pendekatan hukum kontrak yang berpusat pada pasar dan yang berpusat pada partai. Pasar adalah sarana yang memungkinkan badan hukum dapat memasuki hubungan kontraktual yang otonom sebagai subjek yang bebas dan setara. Dengan latar belakang tersebut, hukum pasar tunggal Eropa dapat dianggap sebagai kerangka institusional yang memungkinkan kebebasan individu (Freiheitsermöglichungsrecht). Begitu pula sebaliknya, hukum kontrak tradisional tidak hanya sebatas menjadi latar belakang hubungan hukum individual belaka, namun juga bersifat tatanan kelembagaan yang mengatur transaksi ekonomi seperti itu. Namun demikian, meskipun terdapat banyak transisi dan interkoneksi antara keduanya, paradigma, kita masih dapat membedakan apa yang dimaksud dengan Leitmotiv hukum kontrak.

Gagasan tradisional yang terkandung dalam catatan klasik KUH Perdata Jerman berfokus pada kebebasan berkontrak. Prinsip ini dilengkapi dengan aturan baku yang memenuhi fungsi layanan bagi para pihak dengan menghilangkan tekanan dari proses negosiasi kontrak dan dengan membuat kesenjangan dalam kontrak dapat dikendalikan. Yang terakhir, undang-undang yang bersifat wajib di samping kemungkinan berfungsinya perlindungan bagi pihak ketiga dan kepentingan publik pada dasarnya dimaksudkan untuk melindungi pihak-pihak yang "lemah" dalam situasi di mana prasyarat untuk pengambilan keputusan yang otonom dan substantif tidak terpenuhi (misalnya undang-undang perlindungan konsumen dalam arti sempit).

Sebaliknya, pendekatan baru yang berpusat pada pasar semakin menggantikan gagasan kebebasan berkontrak dengan standarisasi kemungkinan isi kontrak. Secara khusus, kami menemukan hukum wajib untuk transaksi B2C dalam hukum UE tidak hanya sebagai sarana untuk melindungi pihak-pihak yang "lemah" namun bahkan ketika kebutuhan khusus untuk melindungi otonomi konsumen sulit untuk dipahami. Dalam konteks tersebut, kita menghadapi fenomena apa yang disebut "aturan bonus" bagi konsumen. Hal ini mengacu pada peraturan yang sangat ramah konsumen dan biasanya bersifat wajib yang tidak dimaksudkan untuk melindungi ekspektasi yang sah tetapi untuk meningkatkan insentif konsumsi. Yang terakhir, paradigma pasar dalam hukum kontrak terfokus pada kesetaraan persaingan bagi para pedagang dalam transaksi lintas batas negara. Semua sifat ini cukup koheren untuk sebuah perangkat hukum yang tidak terlalu dimaksudkan untuk menjamin

pemerataan kepentingan para pihak. dalam hubungan hukum yang dipersonalisasi tetapi untuk memastikan kelancaran perdagangan dan konsumsi lintas batas.

6.3 YURISDIKSI INTERNASIONAL DAN KONFLIK HUKUM

Pendekatan yang berpusat pada pasar, pertama-tama, dapat dikenali dari faktor penghubung yang dipilih oleh hukum perdata internasional Eropa untuk yurisdiksi internasional dan konflik hukum. Aturan yang relevan dapat ditemukan di Art. 17(1)(c) Peraturan Ibis Brussels (yurisdiksi internasional) dan Art. 6 Peraturan Roma I (konflik hukum). Jika penjual "mengarahkan" usahanya ke negara di mana konsumen bertempat tinggal dan jika kontrak "termasuk dalam lingkup" kegiatan yang diarahkan, maka

1. tempat tinggal konsumen akan menjadi tempat yurisdiksi dan hukum substantif tempat ini akan berlaku pada kontrak, selanjutnya
2. para pihak dalam kontrak tidak boleh menyimpang dari aturan-aturan ini sehingga merugikan konsumen melalui perjanjian pilihan pengadilan atau pilihan hukum.

Menurut kasus hukum Pengadilan Uni Eropa (CJEU), pertanyaan apakah penjual telah mengarahkan bisnisnya ke pasar di mana konsumen bertempat tinggal harus ditentukan dengan mempertimbangkan semua keadaan. fakta bahwa situs web penjual dapat diakses di negara konsumen dan menggunakan bahasa negara tersebut tidaklah cukup. Namun konten situs web (bahasa yang dapat disesuaikan, kemungkinan pilihan tujuan pengiriman), tampilannya (domain tingkat atas khusus negara) serta penyediaan layanan pelanggan internasional (kode panggilan internasional, dll.) harus dipertimbangkan. akun. Dengan menundukkan pedagang pada standar hukum pasar sasaran, undang-undang UE tidak hanya memberikan hak istimewa kepada konsumen namun juga memfasilitasi standardisasi kompetitif tanpa memandang tempat usaha pedagang yang bertindak. Hal ini karena pemberlakuan standar target pasar memperlakukan semua pemasok secara setara yang mengarahkan bisnisnya ke wilayah geografis tertentu.

Perlu juga dicatat bahwa CJEU telah memberikan Art. 17(1)(c) Peraturan Ibis Brussels dan Pasal. 6 Regulasi Roma I memberikan pemahaman yang sangat luas, jauh melampaui area inti penjualan online lintas batas. Dalam kasus Mühlleitner, dinyatakan bahwa Art. 17(1)(c) Peraturan Ibis Brussels tidak hanya berlaku untuk penjualan jarak jauh tetapi juga untuk kasus di mana konsumen hanya memperoleh informasi pra-kontrak di situs web yang ditujukan ke negara asalnya dan kemudian memilih untuk menandatangani kontrak di luar negeri di tempat usaha penjual. Keputusan ini tidak dapat dihindari sejak deklarasi bersama Dewan Eropa dan Komisi UE tentang ex-Art. 15 Peraturan Brussel I (Pasal 17 Peraturan Ibis Brussel), yang juga disebut dengan Peraturan Roma I, telah menyatakan bahwa aturan tersebut harus dibatasi pada kasus penjualan jarak jauh. Selanjutnya, CJEU memutuskan dalam kasus Emrek bahwa apabila penjual mengarahkan usahanya ke pasar luar negeri melalui internet, konsumen yang berdomisili di pasar tersebut yang kemudian melakukan transaksi lokal di tempat usaha penjual di luar negeri dapat memanfaatkan Art. 17(1)(c) Peraturan Ibis Brussel meskipun penargetan online penjual tidak mempunyai pengaruh sebab akibat terhadap kontrak. Misalnya, jika seorang turis dari Jerman membeli barang di

department store di Paris, ia nantinya dapat untuk menuntut penjual di Jerman (Pasal 17(1)(c) Peraturan Ibis Brussel) dan undang-undang perlindungan konsumen Jerman mungkin berlaku (Pasal 6 Peraturan Roma I) jika department store telah mempromosikan barang terkait di Jerman online, meskipun konsumen Jerman tidak mengetahui aktivitas penargetan ini sebelum menandatangani kontrak di Paris. Aturan keputusan Emrek ini telah dikritik karena terlalu melindungi konsumen. Namun, mengingat keputusan Mühlleitner sebelumnya, tampaknya ini merupakan langkah berikutnya yang masuk akal. Jika aturan dalam Art. 17(1)(c) Peraturan Ibis Brussels dan Pasal. 6 Peraturan Roma I tidak lagi terbatas pada penjualan jarak jauh tetapi juga diperluas ke transaksi lokal, hal ini akan membahayakan kepastian hukum jika ditanyakan lebih lanjut apakah aktivitas online sebelumnya memiliki pengaruh sebab akibat terhadap kontrak yang ada. Bagaimanapun, rangkaian keputusan dari Mühlleitner hingga Emrek adalah contoh nyata dari hipotesis bahwa paradigma penjualan online lintas batas juga semakin mempengaruhi penjualan konsumen tradisional.

6.4 PENERAPAN HUKUM KONSUMEN UE EKSTRA-TERITORIAL

Beralih ke isu penerapan undang-undang konsumen UE ekstra-teritorial dalam lingkungan digital, kita harus memperhatikan keterkaitan masalah ini dengan prinsip orientasi pasar berdasarkan Art. 17(1)(c) Peraturan Ibis Brussels dan Pasal. 6 Regulasi Roma I sudah dibahas. Semakin rendah persyaratan untuk mengarahkan bisnis ke target pasar konsumen UE oleh penjual non-UE, semakin besar penerapan undang-undang konsumen UE ekstra-teritorial yang akan terjadi hanya dengan penerapan aturan yang diuraikan sebelumnya. Memang benar, CJEU mengikuti semacam pendekatan jangka panjang dalam hal ini dengan melonggarkan persyaratan untuk mengarahkan bisnis ke pasar sasaran berdasarkan doktrin kasus hukum Pammer dan Hotel Alpenhof: misalnya penyediaan layanan pelanggan internasional dan layanan pelanggan yang dapat disesuaikan. pilihan bahasa dan penyampaian di situs web mungkin cukup untuk kriteria penargetan.

Dalam kasus-kasus yang tidak memenuhi persyaratan untuk mengarahkan bisnis ke pasar konsumen tertentu, kita mungkin masih bertanya apakah undang-undang konsumen UE atau undang-undang konsumen di Negara Anggota UE tertentu dapat diterapkan sebagai apa yang disebut ketentuan wajib utama (Eingriffsnormen) di bawah art. 9 Regulasi Roma I. Aturan-aturan tersebut didefinisikan sebagai ketentuan-ketentuan yang penghormatannya dianggap penting oleh suatu negara untuk melindungi kepentingan publiknya, seperti organisasi politik, sosial atau ekonominya, sedemikian rupa sehingga hal ini dapat diterapkan pada situasi apa pun yang berada dalam cakupannya, terlepas dari hukum yang berlaku pada kontrak. (Pasal 9(1) Regulasi Roma I)

Meskipun konsep ini secara tradisional berfokus pada peraturan perundang-undangan yang berdaulat, seperti misalnya undang-undang perdagangan luar negeri, CJEU juga menunjukkan simpati umum untuk mengklasifikasikan hukum perdata sebagai ketentuan yang mengesampingkan ketentuan wajib jika landasan pemikirannya tidak hanya untuk melindungi pihak-pihak yang “lemah” namun juga untuk menyusun pasar dan

melindungi perdamaian sosial. Posisi ini harus dilihat mengingat fakta bahwa alokasi kompetensi antara UE dan Negara-negara Anggota biasanya mengamanatkan UE untuk memberlakukan undang-undang hukum privat dibandingkan undang-undang peraturan publik yang klasik. Oleh karena itu, dimasukkannya hukum perdata ke dalam konsep mengesampingkan ketentuan-ketentuan wajib akan memperkuat kemampuan Uni Eropa untuk memberlakukan peraturan-peraturan yang bersifat wajib secara internasional.

Ide ini awalnya dikembangkan dalam keputusan Ingmar yang terkenal untuk bidang agen komersial wiraswasta. Di sini, Pengadilan memutuskan bahwa jaminan hukum wajib Uni Eropa untuk agen komersial juga dapat berlaku dalam kasus di mana kontrak untuk agen diselesaikan dengan prinsipal non-UE dan diatur oleh hukum non-UE tetapi aktivitas agen komersialnya dilakukan di dalam UE. Alasan penting atas keputusan ini adalah bahwa Petunjuk Agen Komersial UE tidak hanya dimaksudkan untuk melindungi agen individu tetapi juga untuk menciptakan lapangan bermain yang setara bagi semua kegiatan agen komersial di UE. Di sini, kami sekali lagi menemukan fokus yang jelas pada pendekatan yang berpusat pada pasar.

Pendekatan keputusan Ingmar telah diperluas oleh kasus Unamar menjadi jaminan perlindungan yang melampaui standar UE dan didasarkan pada hukum privat Negara-negara Anggota. Menurut CJEU, aturan-aturan tersebut dapat dikualifikasikan sebagai mengesampingkan ketentuan-ketentuan wajib dalam pengertian Art. 9 Regulasi Roma I jika hal tersebut tidak hanya dimaksudkan untuk melindungi individu tetapi juga struktur pasar. Pendekatan ini selanjutnya dapat membuka jalan bagi kemungkinan penerapan hukum konsumen ekstra-teritorial. Namun demikian, keputusan akhir mengenai hal ini tetap berada di pihak masing-masing Negara Anggota UE yang telah memberlakukan aturan-aturan yang mungkin memenuhi syarat sebagai aturan yang bersifat wajib. Kita dapat mengamati pendekatan-pendekatan yang agak kontradiktif dalam kasus hukum nasional dalam hal ini. Misalnya, pengadilan Perancis agak berpikiran terbuka terhadap penerapan undang-undang konsumen Perancis ekstra-teritorial, khususnya untuk pinjaman konsumen, sementara pengadilan Jerman sejauh ini mengikuti pendekatan yang lebih ketat. Bagaimanapun, pilihan untuk mengklasifikasikan konsumen UU yang lebih bersifat wajib memberikan contoh lain mengenai pergeseran pendekatan yang berpusat pada partai menjadi berpusat pada pasar.

6.5 TREN HUKUM PENJUALAN SUBSTANTIF UE

Perundang-undangan terbaru yang paling relevan mengenai undang-undang penjualan UE adalah Petunjuk Hak Konsumen (2011) dan Petunjuk Penjualan Barang yang baru (2019). Meskipun peraturan tersebut menekankan pada kewajiban untuk memberi informasi dan hak untuk menarik diri (inter alia, dalam jarak jauh). kontrak penjualan), yang terakhir ini memiliki fokus pada standar kesesuaian barang dan hak-hak konsumen jika terjadi ketidaksesuaian. Proposal awal Petunjuk Penjualan Barang yang baru dirancang hanya untuk penjualan jarak jauh konsumen sebagai bagian sejati dari agenda pasar tunggal digital.46 Namun, cakupan versi final diperluas ke semua penjualan konsumen sejak set yang

berbeda. penerapan undang-undang UE untuk kontrak online dan offline akan menyebabkan fragmentasi undang-undang yang tidak semestinya.

Meskipun demikian, kebutuhan pasar online lintas negara mendominasi isi Petunjuk Penjualan Barang yang baru, sehingga memperkuat pengamatan bahwa paradigma dunia digital cenderung "meluap" ke penjualan konsumen tradisional. Secara khusus, banyak peraturan dalam Petunjuk Penjualan Barang yang baru mencerminkan peraturan dan standar yang serupa dengan Petunjuk tentang Pasokan Konten Digital yang baru. Pendekatan ini harus mengatasi transisi yang semakin kabur antara kontrak untuk penjualan barang dan untuk penyediaan barang. konten digital, misalnya dalam hal produk fisik dengan komponen digital yang luas (mobil yang saling terhubung, telepon pintar, perangkat yang dapat dikenakan, dll.). Berfokus pada substansi paradigma pasar digital yang dapat ditemukan dalam undang-undang penjualan UE baru-baru ini, kita harus memperhatikan dua aspek utama.

Pertama, kami menemukan adanya pergeseran dari prinsip harmonisasi minimum yang mendominasi undang-undang konsumen UE sebelumnya (misalnya Petunjuk Penjualan Barang tahun 1999), ke prinsip harmonisasi penuh yang tertanam dalam Petunjuk Hak Konsumen (Pasal 4) dan peraturan baru. Petunjuk Penjualan Barang (Pasal 4). Prinsip harmonisasi minimum memerlukan standar perlindungan UE sebagai semacam "batas" yang dapat dilampaui oleh hukum nasional Negara-negara Anggota demi kepentingan konsumen. Sebaliknya, prinsip harmonisasi penuh tidak hanya mendefinisikan tingkat minimum tetapi juga tingkat maksimum perlindungan konsumen yang dapat disyaratkan oleh Negara-negara Anggota sebagai semacam "batas atas". Pergeseran peraturan ini telah banyak dibahas dan juga dikritik dalam beberapa tahun terakhir. Di antara aspek-aspek lainnya, kritik tersebut berfokus pada fakta bahwa harmonisasi penuh tidak mempertimbangkan kepentingan spesifik negara-negara anggota tertentu yang mungkin memerlukan standar perlindungan yang lebih tinggi dalam hal perlindungan terhadap negara. beberapa bidang dan tidak memungkinkan adanya persaingan peraturan antara solusi yang berbeda berdasarkan perlindungan konsumen minimum yang umum. Meskipun kritik ini memang ada manfaatnya, argumen utama legislator UE yang mendukung peralihan menuju harmonisasi penuh adalah persepsi perlunya kesetaraan persaingan antara semua bisnis di pasar online Eropa sebagai sarana untuk meningkatkan kinerja lintas batas negara. pasokan dan konsumsi. Kesetaraan persaingan tersebut hanya dapat dicapai melalui sistem harmonisasi penuh. Sekali lagi, latar belakang peraturan ini memberikan bukti fakta bahwa strategi legislatif saat ini sangat dipengaruhi oleh perspektif yang berpusat pada pasar, bahkan dengan mengorbankan keuntungan lain yang mungkin terkait dengan strategi alternatif seperti prinsip harmonisasi minimum.

Kedua, kita akan menemukan fenomena dalam instrumen baru UE yang mungkin disebut "aturan bonus" bagi konsumen. Aturan-aturan ini tidak dapat sepenuhnya dijelaskan berdasarkan kebutuhan perlindungan konsumen yang sah, namun lebih ditujukan untuk menghasilkan sikap umum yang positif terhadap konsumsi (online) dan, dengan demikian, meningkatkan pasar. Saya ingin fokus pada dua contoh aturan tersebut.

Contoh pertama adalah hak penarikan wajib selama 14 hari bagi konsumen dalam kontrak penjualan jarak jauh, khususnya penjualan online, berdasarkan Art. 9 Petunjuk Hak Konsumen. Meskipun hak penarikan paralel dalam kontrak di luar lokasi sebagian besar tidak terbantahkan karena beban psikologis yang berlebihan yang biasanya dihadapi oleh konsumen dalam situasi seperti itu, kebutuhan perlindungan yang serupa seringkali dipertanyakan untuk kontrak penjualan jarak jauh. Mungkin saja ada argumen bahwa alternatif hak untuk memilih antara kontrak dengan atau tanpa hak penarikan (pada tingkat harga yang berbeda) sudah mencakup kepentingan sah konsumen dalam penjualan jarak jauh. Dengan menerapkan hak penarikan umum yang diwajibkan, legislator Eropa telah memilih untuk "bonus" khusus bagi konsumen yang melakukan konsumsi online.

Contoh kedua adalah pengalihan beban pembuktian wajib selama satu tahun mengenai cacat kualitas demi kepentingan konsumen menurut Art. 11 dari Petunjuk Penjualan Barang yang baru. Berdasarkan aturan ini, setiap ketidaksesuaian yang tampak dalam waktu satu tahun sejak barang diserahkan, dianggap sudah ada pada saat barang diserahkan, kecuali dibuktikan sebaliknya atau kecuali anggapan ini tidak sesuai dengan ketentuan yang berlaku. sifat barangnya atau dengan sifat ketidaksesuaiannya.

Hal ini berarti perluasan perlindungan konsumen yang cukup besar dibandingkan dengan Art. 5(3) Petunjuk Penjualan Barang tahun 1999, yang mengatur bahwa peralihan beban pembuktian dibatasi hingga enam bulan, meskipun berdasarkan prinsip harmonisasi minimum. Pada tingkat praktis, peraturan baru ini dalam banyak kasus mungkin sama dengan jaminan wajib satu tahun untuk kualitas dan daya tahan. Meskipun solusi ini mungkin sesuai dengan tujuan keberlanjutan yang lebih luas, hal ini menyimpang dari keseimbangan kepentingan kontraktual yang memungkinkan untuk pilihan yang lebih berbeda mengenai tanggung jawab penjual terhadap daya tahan, terutama sehubungan dengan barang pada tingkat harga yang berbeda.

Ringkasnya, terdapat bukti bahwa undang-undang penjualan konsumen UE memang sedang beralih dari gagasan undang-undang konsumen sebagai sarana untuk melindungi pihak-pihak yang "lemah" dan semakin fokus pada memfasilitasi dan meningkatkan pasar (online) dengan menciptakan semacam lingkungan konsumsi yang bebas beban.

6.6 ALTERNATIF PENYELESAIAN SENGKETA DAN PENEGAKAN HAK KONSUMEN

Meskipun undang-undang konsumen UE telah lama berfokus pada peningkatan hak-hak substantif konsumen, baru-baru ini UE juga mengambil langkah-langkah signifikan untuk memperkuat penegakan praktis hak-hak tersebut. Hal ini terkait dengan keengganan konsumen untuk menegakkan hak-hak mereka melalui prosedur pengadilan tradisional yang seringkali rumit, mahal dan memakan waktu. Masalah-masalah ini khususnya berkaitan dengan transaksi lintas batas negara dan berdampak pada, khususnya, kontrak online internasional. Oleh karena itu, pengembangan cara-cara penegakan hak-hak konsumen yang efisien, mudah dan cepat mendapat peringkat tinggi dalam agenda undang-undang konsumen UE baru-baru ini dan proyek terbaru "Kesepakatan Baru untuk Konsumen".

Sebagai semacam karya pionir, Petunjuk Mediasi tahun 2008 mengharuskan Negara-negara Anggota UE untuk memfasilitasi mediasi dalam kasus perdata. Hal ini dimulai dari premis bahwa mediasi adalah prosedur yang menghemat waktu dan biaya yang memperkuat penerimaan resolusi konflik oleh warga negara. dan dengan demikian meningkatkan akses terhadap keadilan bagi mereka. Meskipun sejauh ini dampak praktis dari instrumen mediasi masih terbatas, UE kemudian memulai inisiatif komprehensif untuk mempromosikan cara-cara penyelesaian sengketa alternatif (ADR) dalam sengketa konsumen. Hasil terpenting dari inisiatif ini dimulai pada tahun 2013 dan merupakan Petunjuk tentang ADR Konsumen (ADR Directive) dan Peraturan Penyelesaian Sengketa Konsumen Secara Online (Peraturan ODR)60 yang harus dilihat sebagai langkah-langkah yang terkoordinasi. Petunjuk ADR mengharuskan Negara-negara Anggota UE untuk membentuk lembaga-lembaga yang memadai untuk penyelesaian alternatif sengketa konsumen. Dalam melakukan hal ini, Negara-negara Anggota dapat menggunakan lembaga ADR swasta namun harus memastikan bahwa lembaga-lembaga tersebut memenuhi standar efisiensi dan kualitas tertentu. Peraturan ODR tidak memperkenalkan mekanisme terpisah untuk ADR online namun hanya menciptakan sebuah platform yang memungkinkan konsumen untuk mengidentifikasi lembaga ADR nasional yang sesuai dan kompeten dalam menangani perselisihan yang timbul dari penjualan online atau kontrak layanan (Pasal 2(1) Peraturan ODR). Untuk tujuan ini, platform ODR Eropa yang mencantumkan semua entitas ADR nasional telah dibentuk oleh Komisi UE berdasarkan Art. 5 Peraturan ODR.

Selain itu, undang-undang UE juga menangani masalah ganti rugi yang efektif dalam kasus kerugian yang tersebar. Dalam rekomendasinya pada bulan Juni 2013, Komisi UE masih mengusulkan agar semua Negara Anggota UE harus menerapkan opt-in class action untuk bantuan moneter dalam situasi kerugian massal. Namun, perkembangan terakhir telah beralih dari class action ke arah solusi dengan tindakan representatif, yang lebih selaras dengan tradisi penegakan hukum Eropa Kontinental. Oleh karena itu, UE baru-baru ini memperkenalkan Petunjuk mengenai tindakan representatif untuk melindungi kepentingan kolektif konsumen. Terakhir, Petunjuk baru mengenai penegakan yang lebih baik dan modernisasi peraturan perlindungan konsumen memberikan penekanan pada hukuman moneter bagi perusahaan yang tidak melakukan tindakan yang representatif. mematuhi aturan terkait.

Semua cara penyelesaian sengketa dan penegakan hak-hak konsumen yang baru ini telah menjadi bahan perdebatan intensif dan pada saat ini hanya dapat disinggung secara singkat. Misalnya, keberatan utama terhadap inisiatif ADR konsumen adalah bahwa Negara-negara Anggota UE akan diminta untuk mengembangkan dan memantau sistem ADR yang kompleks yang tidak sesuai untuk menegakkan hak-hak konsumen yang bersifat wajib dan yang, sebagai privatisasi parsial dari sistem peradilan, dapat mengganggu perlindungan hukum oleh pengadilan umum di bidang ini. Oleh karena itu, beberapa alternatif untuk penegakan hak-hak konsumen yang efisien telah disarankan. Usulan-usulan tersebut berkisar dari penerapan proses peradilan dengan risiko kecil yang disederhanakan di pengadilan setempat hingga penerapan gugatan kelompok (class action) konsumen.

Dalam kasus apa pun, tampak jelas bahwa mekanisme yang baru diperkenalkan ini, setidaknya tidak terutama, bertujuan untuk menegakkan hak-hak konsumen di masyarakat. merupakan cara yang "legal" namun fokus mereka lebih pada solusi cepat, murah dan terstandarisasi yang mengutamakan keandalan dan pengoperasian pasar konsumen. Dalam kasus ADR yang dikelola oleh badan-badan swasta dan mungkin juga melalui perangkat online, hal ini dapat mengarah pada semacam "keadilan yang kasar" yang mungkin akan diterima dibandingkan dengan bahaya kegagalan total penegakan hak-hak konsumen dalam sistem pengadilan negara. Sebaliknya, pendekatan "Kesepakatan Baru untuk Konsumen" yang terbaru dengan fokus pada tindakan perwakilan dan hukuman moneter dapat dianalisis sebagai jenis pengawasan pasar semi-publik yang agak bergeser dari pemikiran dalam hubungan hukum perdata individu.

Terlepas dari kelebihan dan bahaya yang dimiliki instrumen-instrumen baru tersebut, perkembangan di bidang penyelesaian sengketa dan penegakan hukum menegaskan kecenderungan untuk berfokus pada perlindungan dan fasilitasi pasar dibandingkan pada pemikiran dalam hubungan hukum perdata individual yang stricto sensu.

6.7 TATA KELOLA SWASTA BERDASARKAN KONTRAK DAN TEKNOLOGI

Sehubungan dengan fenomena tata kelola swasta berdasarkan kontrak dan teknologi untuk kontrak konsumen, semakin pentingnya platform perantara online tampaknya merupakan perkembangan yang paling menonjol. Meskipun banyak dari platform ini, pada saat yang sama, juga beroperasi sebagai pemasok barang dan jasa kepada konsumen, fungsi terpenting mereka adalah bertindak sebagai "penjaga pasar" atau "pembuat pasar". Permasalahan ini berdampak pada berbagai tingkat konsumen. relevansi hukum.

Pertama, platform online berfungsi sebagai penjaga gerbang dalam mengambil keputusan mengenai pemasok dan konsumen mana yang akan diterima di pasar platform masing-masing. Secara khusus, model algoritmik yang digunakan oleh operator platform sering kali mengarah pada pembentukan preferensi yang tidak kentara atau bahkan penolakan penuh atau sebagian terhadap akses konsumen terhadap platform dan penawarannya. Dari sudut pandang kontrak, standar yang dapat diterima dari model tersebut penjagaan gerbang hanya diatur secara terpisah di tingkat UE. Jika pembatasan akses tertentu oleh konsumen didasarkan pada kriteria yang mencurigakan, Petunjuk terhadap perilaku diskriminatif dalam hubungan kontrak mungkin berlaku. Pada tingkat lintas batas, Peraturan Geo-Blocking melarang gangguan akses terhadap antarmuka online, seperti situs web profesional, berdasarkan kewarganegaraan atau tempat tinggal (Pasal 3) dan juga melarang pembuatan ketentuan umum akses terhadap barang atau jasa yang bergantung pada kriteria ini (Pasal 4). Namun, aturan-aturan ini tidak berarti kewajiban untuk berurusan dengan pelanggan tertentu atau mengirimkan barang ke negara bagian tertentu, dan kepatuhan terhadap Peraturan Geo-Blocking itu sendiri tidak berarti menargetkan pasar tertentu. Art. 17(1)(c) Peraturan Ibis Brussels dan Pasal. 6 Peraturan Roma I. Hal ini menyebabkan kontribusi Peraturan Geo-Blocking terhadap hak konsumen untuk mengakses platform pada tingkat praktis menjadi terbatas. Namun, mungkin ada

beberapa pendekatan tambahan dalam undang-undang nasional untuk mengatasi masalah ini akses platform oleh konsumen. Misalnya, Mahkamah Konstitusi Federal Jerman telah memutuskan bahwa pelaku swasta tidak boleh mengecualikan individu tanpa alasan yang baik dan proses yang wajar dari kegiatan yang (umumnya) terbuka untuk umum dan akses terhadap kegiatan yang penting untuk berpartisipasi dalam kehidupan sosial. Meskipun kasus yang dihadapi berasal dari dunia offline dan berkaitan dengan akses ke stadion sepak bola, dapat dikatakan bahwa beberapa platform online saat ini setidaknya sama pentingnya bagi kehidupan sosial dengan acara olahraga. Sejalan dengan itu, keputusan Mahkamah Konstitusi Federal dapat menjadi titik awal dari pengawasan hukum yang lebih ketat terhadap keputusan operator platform online dalam hal penerimaan ke platform tersebut.

Kedua, fenomena platform online menumbuhkan pemikiran dalam hubungan pelanggan secara keseluruhan dengan mengorbankan pemikiran hukum tradisional tentang hak dan kewajiban spesifik dalam kontrak individu (penjualan). Hal ini karena banyak operator platform mengambil nilai ekonomi yang cukup besar dari perolehan data konsumen dalam jangka panjang selama aktivitas platform. Bahkan ada yang mungkin berpendapat bahwa, dalam beberapa kasus, mengadakan kontrak yang melibatkan barang atau jasa tertentu dengan konsumen bukan lagi tujuan bisnis, melainkan sekadar sarana untuk menciptakan surplus yang lebih penting dalam struktur pasar berbasis data. Hal ini sejalan dengan asumsi bahwa banyak platform terkemuka sering kali lebih bermurah hati dalam hal penanganan kontrak tertentu dibandingkan dengan standar yang disyaratkan oleh hukum konsumen UE (misalnya terkait dengan persyaratan hak penarikan).

Semua ini memberikan tekanan pada menurunnya relevansi hak dan kewajiban hukum dalam kontrak tertentu terhadap manfaat pengelolaan pasar secara keseluruhan. Ketiga, pembuatan peraturan swasta oleh platform perantara online untuk transaksi yang dilakukan melalui platform menimbulkan permasalahan penting tentang bagaimana mengklasifikasikan aturan-aturan ini (ketentuan penggunaan, sistem pembayaran, sistem umpan balik, klausul penyelesaian sengketa, dll.) dari lembaga hukum. sudut pandang. Akun tradisional, yang antara lain masih diikuti oleh pengadilan Jerman, mengklasifikasikan ketentuan yang ditetapkan oleh operator platform sebagai ketentuan standar meskipun operator tersebut bukan merupakan pihak dalam kontrak penjualan yang dibuat oleh pemasok dan konsumen melalui platform. Oleh karena itu, ketentuan-ketentuan tersebut, pada prinsipnya, tunduk pada peninjauan kembali berdasarkan Petunjuk Ketentuan Kontrak yang Tidak Adil UE. Namun, muncul pandangan berlawanan yang menganalisis ketentuan-ketentuan ini bukan dari perspektif kontrak tetapi menganggapnya sebagai sarana pengorganisasian pasar oleh pihak ketiga. aktor pihak. Menurut pandangan ini, ketentuan penggunaan yang disediakan oleh operator platform tidak boleh tunduk pada tinjauan hukum pada tingkat kontrak tetapi hanya berdasarkan aturan hukum persaingan jika masing-masing operator platform memperoleh posisi dominan di pasar. Jika pandangan ini berlaku, pemikiran kontraktual sekali lagi akan tertinggal dari perspektif struktur pasar secara keseluruhan.

Yang terakhir, perdebatan intensif muncul mengenai cara mengatasi fenomena bahwa, melalui platform perantara online, konsumen sering kali tidak lagi mengadakan kontrak dengan pemasok profesional besar, melainkan dengan perusahaan kecil dan menengah atau bahkan dengan konsumen secara langsung. sisi pemasok juga. Perkembangan ini dapat membahayakan efektivitas undang-undang konsumen UE, karena peraturan ini memerlukan transaksi B2C dan tidak berlaku untuk kontrak C2C. Dengan latar belakang tersebut, amandemen terbaru terhadap Petunjuk Hak Konsumen mengharuskan operator platform untuk memastikan transparansi yang ketat mengenai siapa mitra konsumen dalam kontrak yang dibuat melalui platform.

Lebih jauh lagi, masalah hubungan hukum yang saling terkait dalam platform Bisnis ini telah menghasilkan usulan kebijakan yang menyatakan bahwa operator platform harus bertanggung jawab atas setiap pelanggaran kontrak yang dilakukan melalui platform. Tanggung jawab ini akan berlaku meskipun operator platform telah menjelaskan bahwa mereka hanya akan berfungsi sebagai perantara dan bukan sebagai mitra kontrak dalam transaksi platform. Yang paling menonjol adalah Model Rules on Online Intermediary Platforms, yang diadopsi oleh European Law Institute (ELI) pada tahun 2020, menyarankan tanggung jawab seperti itu di pihak operator platform jika operator memiliki "pengaruh dominan" terhadap pemasok yang menawarkan barang. atau layanan di platform (Pasal 20 Aturan Model ELI). Namun, terdapat kritik bahwa pendekatan seperti itu akan terlalu mengkompromikan prinsip-prinsip kontrak yang sudah ada, khususnya gagasan privasi kontrak (Relativität der Schuldverhältnisse), mempertanyakan apakah operator platform, selain perannya sebagai perantara, bertanggung jawab jika terjadi pelanggaran kontrak yang dilakukan melalui platform, pada prinsipnya harus diserahkan pada solusi kontrak yang bebas (misalnya melalui jaminan yang diberikan kepada konsumen oleh operator platform). Sebaliknya, jika pandangan Aturan Model ELI menang, maka hal ini akan sekali lagi menandai kemenangan tatanan pasar atas pemikiran kontraktual klasik dalam bidang kontrak konsumen yang terdigitalisasi.

6.8 KESIMPULAN

Analisis sebelumnya menunjukkan bahwa proses digitalisasi mendorong perubahan paradigma dalam hukum kontrak konsumen UE. Pandangan klasik yang berpusat pada partai dengan fokusnya pada pemerataan kepentingan partai dan melindungi partai-partai yang "lemah" untuk mengamankan pengambilan keputusan yang otonom telah semakin digantikan oleh pendekatan yang berpusat pada pasar dengan fokus pada perlindungan dan fasilitasi (online) pasar melalui hukum kontrak. Pada tingkat yurisdiksi internasional dan konflik hukum, pergeseran ini ditandai dengan orientasi faktor-faktor penghubung yang relevan pada aktivitas pasar dan kecenderungan penerapan pada cakupan geografis yang lebih luas. Sehubungan dengan undang-undang penjualan substantif, kita dapat menyaksikan pergeseran ke arah standarisasi hubungan kontraktual melalui harmonisasi penuh dalam undang-undang UE dan melalui fenomena "aturan bonus" bagi konsumen yang meninggalkan gagasan perlindungan konsumen semata dan lebih memilih untuk

memfasilitasi dan meningkatkan konsumsi di pasar online. Pada tingkat prosedural, proses ini diapit oleh peningkatan prosedur ADR dan tindakan perwakilan kolektif yang lebih mengutamakan solusi cepat dan terstandar daripada penegakan hak-hak individu yang ketat. Di bidang online platform perantara, pemikiran mengenai kontrak terpisah semakin digantikan oleh manajemen hubungan konsumen yang terdigitalisasi oleh operator platform.

Hal ini, pada gilirannya, mendorong usulan kebijakan untuk mengkompromikan prinsip-prinsip kontrak yang sudah ada seperti gagasan privasi kontrak demi mengintensifkan tanggung jawab operator platform terhadap konsumen. Terakhir, perspektif kontrak penjualan digital yang berfokus pada pasar juga memiliki pengaruh yang kuat tentang perkembangan hukum UE yang berlaku untuk kontrak penjualan offline tradisional. Hal ini mengakibatkan semakin mendominasinya paradigma digital terhadap hukum penjualan konsumen secara umum.

BAGIAN IV
HUKUM MEDIA

BAB 7
HUKUM MEDIA DIGITAL

7.1 PLATFORM DIGITAL UNTUK IKLAN POLITIK DAN KOMERSIAL

Saat ini, ada banyak platform digital yang dapat digunakan untuk iklan politik dan komersial. Pilihan platform akan tergantung pada target audiens, tujuan kampanye, dan anggaran yang tersedia. Beberapa platform yang umumnya digunakan termasuk:

Untuk Iklan Politik:

1. **Facebook:**
    - Memiliki alat target yang kuat berdasarkan demografi, lokasi, minat, dan perilaku.
    - Mampu menjangkau beragam kelompok audiens.
2. **Twitter:**
    - Cocok untuk kampanye politik karena sering digunakan untuk diskusi politik.
    - Adanya fitur iklan yang dapat ditargetkan.
3. **Instagram:**
    - Terutama efektif untuk menargetkan pemilih muda.
    - Menggunakan gambar dan video untuk menyampaikan pesan dengan daya tarik visual.
4. **YouTube:**
    - Video iklan dapat digunakan untuk menyampaikan pesan dengan lebih mendalam.
    - Targeting berdasarkan tampilan video sebelumnya, minat, dan demografi.
5. **LinkedIn:**
    - Cocok untuk kampanye politik yang lebih berorientasi pada bisnis dan profesional.

Untuk Iklan Komersial:

1. **Google Ads:**
    - Menampilkan iklan berbasis pencarian dan iklan display di berbagai situs web.
    - Mampu menjangkau pengguna yang aktif mencari informasi terkait produk atau layanan.
2. **Amazon Advertising:**
    - Penting untuk iklan produk komersial, terutama jika Anda menjual barang secara online.
    - Menawarkan berbagai opsi iklan, termasuk iklan di hasil pencarian dan iklan di halaman produk.
3. **Snapchat:**
    - Cocok untuk mencapai audiens muda dengan konten visual yang menarik.
4. **TikTok:**

- Menghadirkan peluang kreatif untuk iklan berbasis video, khususnya untuk menargetkan generasi Z.

5. **Pinterest:**
    - Efektif untuk produk visual dan inspirasional.
    - Dapat menjangkau pengguna yang sedang mencari ide dan inspirasi.

Pastikan untuk memahami karakteristik target audiens Anda dan mengukur efektivitas kampanye Anda secara teratur. Setiap platform memiliki keunggulan dan kelemahan tertentu, dan strategi yang baik seringkali melibatkan kombinasi dari beberapa platform untuk mencapai hasil terbaik.

Jika kita mengacu pada hukum media digital di negara lain, Amerika Serikat misalnya. Salah satu upaya pertama AS untuk menerjemahkan sistem transparansi analog ke dunia digital adalah Undang-undang Iklan Jujur (Honest Ads Act), yang diperkenalkan untuk kedua kalinya pada bulan Maret 2019. Dalam upaya untuk menjunjung tinggi prinsip bahwa pemilih mempunyai hak untuk mendapatkan informasi yang lengkap, undang-undang tersebut akan menutup celah digital untuk iklan kampanye online. Platform harus mengungkapkan identitas pembeli iklan politik. Meskipun Undang-Undang Iklan Jujur terhenti di Kongres, beberapa negara bagian telah bergerak maju untuk mengadopsi undang-undang serupa, termasuk California, Maryland, Washington, dan New York.

Undang-Undang Pengungkapan Media Sosial California tahun 2018 mewajibkan pengungkapan sponsor iklan politik. Undang-Undang Perlindungan Demokrasi New York tahun 2018 mewajibkan iklan politik berbayar untuk menampilkan penafian yang menyatakan apakah iklan tersebut disahkan oleh seorang kandidat serta siapa yang benar-benar membayar iklan tersebut. Negara bagian Washington telah mengubah undang-undang pendanaan kampanyenya untuk mewajibkan pengungkapan nama dan alamat sponsor iklan politik serta biaya iklan. Kanada telah mengesahkan undang-undang yang mewajibkan platform mempublikasikan nama asli pembeli iklan yang terverifikasi.

Pengungkapan yang ditujukan untuk perantara juga dapat ditemukan di semua undang-undang transparansi iklan kampanye yang diusulkan dan diadopsi. Undang-Undang Iklan Jujur akan mewajibkan platform untuk memelihara penyimpanan iklan publik dari semua pengiklan politik yang telah menghabiskan lebih dari Rp. 5.000.000 untuk iklan atau postingan bersponsor. Undang-undang periklanan politik Kanada juga mengamanatkan penyimpanan iklan. DISCLOSE Act di Kalifornia mewajibkan pengiklan kampanye politik untuk mencantumkan tiga kontributor dan platform teratas mereka untuk memelihara database iklan politik yang dijalankan di negara bagian tersebut. Undang-Undang Perlindungan Demokrasi New York mengamanatkan bahwa iklan politik dikumpulkan dalam arsip online yang dikelola oleh Dewan Negara Pemilu. Negara bagian Washington mewajibkan pengungkapan "lokasi geografis dan audiens yang ditargetkan, serta jumlah total tayangan yang dihasilkan oleh iklan atau komunikasi tersebut."

Undang-undang Maryland, yang saat ini diperintahkan oleh hakim federal yang menemukan adanya pelanggaran Amandemen Pertama, melangkah lebih jauh dibandingkan undang-undang di New York atau California dengan mewajibkan pengungkapan jangkauan iklan yang lebih luas di luar total tayangan iklan di bawah kewenangan persyaratan inspeksi

negara bagian yang diberikan kepada Dewan Pemilihan. Beberapa negara bagian lainnya, termasuk Wyoming dan Vermont, telah memperluas undang-undang pendanaan kampanye yang sudah ada sebelumnya ke pengiklan digital. Tanpa legislasi federal yang komprehensif, regulasi periklanan politik akan tetap terpecah-belah.

Secara keseluruhan, pendorong munculnya undang-undang keterbukaan informasi terkait iklan digital pasca tahun 2016 adalah terungkapnya campur tangan asing dalam pemilu yang dilakukan oleh Rusia. Oleh karena itu, undang-undang baru ini jelas diarahkan untuk memitigasi upaya manipulasi serupa di masa depan dan sejauh ini berdampak pada pengiklan platform jaringan non-AS. Namun, seperti telah disebutkan, undang-undang publik yang baru tidak memiliki pengaruh yuridis terhadap periklanan digital di luar AS. Pada saat yang sama, platform-platform tersebut ingin membuat pendekatan mereka seragam secara global. Facebook pertama kali menguji praktik pengungkapan yang dilakukan sendiri di Kanada sebelum menerapkannya di AS. Sebagai respons terhadap persyaratan pengungkapan iklan di Negara Bagian Washington, Facebook memutuskan untuk melarang iklan politik sama sekali di negara bagian tersebut, dan hal ini menjadi pendekatan yang dilakukan Twitter secara nasional. ada kemungkinan bahwa platform-platform tersebut akan bergerak ke arah ini secara global.

7.2 HUKUM PLATFORM DIGITAL UNTUK DEEP FAKES DAN BOT

Bot telah memungkinkan kampanye pesan besar-besaran yang menyamarkan kepenulisan, dan dengan cara ini meningkatkan persepsi nilai atau kekuatan sebuah opini. Sejumlah besar tautan yang di-tweet adalah bot dan akun palsu yang dirancang untuk membanjiri ruang informasi dengan opini yang sering diungkapkan, orang-orang mempercayainya. Kepalsuan yang mendalam menciptakan kesan yang menipu tentang kepenulisan melalui ventrilokui, menggunakan AI untuk memalsukan apa yang telah dikatakan atau dilakukan. Undang-undang yang diusulkan dan diadopsi untuk mengatasi kepalsuan yang mendalam dan ucapan yang dihasilkan oleh bot berupaya untuk memastikan bahwa masyarakat mendapat informasi tentang siapa sedang berbicara kepada mereka (dalam kasus bot) dan apakah yang mereka rasakan itu nyata (dalam kasus kepalsuan).

California SB 1001 melarang bot berkomunikasi dengan seseorang dengan “niat untuk menyesatkan dan tanpa secara jelas dan mencolok mengungkapkan bahwa bot tersebut bukanlah orang perseorangan,” dan mengharuskan penghapusan akun yang melanggar. Hal ini mengharuskan “ akun ['bot'] online otomatis” mengidentifikasi dirinya seperti itu jika digunakan untuk melibatkan seseorang di California guna memengaruhi mereka agar melakukan pembelian atau memberikan suara. Khususnya, undang-undang tersebut memperjelas bahwa undang-undang tersebut tidak membebankan kewajiban kepada penyedia layanan platform online.

Di tingkat federal, Senator Feinstein telah memperkenalkan Undang-Undang Pengungkapan dan Akuntabilitas Bot untuk membatasi penggunaan bot media sosial oleh kandidat politik. RUU ini akan mencegah para kandidat, tim kampanye mereka, dan kelompok politik lainnya, menggunakan bot sebagai salah satu jenis iklan politik. FTC akan

diberikan kekuasaan untuk mengarahkan platform jaringan untuk mengembangkan kebijakan yang mewajibkan pengungkapan bot oleh pembuat dan penggunanya. Mengikuti contoh di California, Senator Mark Warner telah mengusulkan untuk mewajibkan platform untuk mengidentifikasi akun tidak autentik dan menentukan asal usulnya. postingan dan atau akun.

RUU ini, jika diberlakukan, akan terbatas pada komunikasi dalam yurisdiksi Amerika Serikat. Seperti semua intervensi tata kelola internet, terdapat potensi bahwa platform tersebut akan menyesuaikan perilaku mereka secara global dengan standar yang paling menuntut demi kesederhanaan dan keseragaman. Memang benar, ketika Mark Zuckerberg berbicara secara terbuka tentang peraturan baru untuk internet, dia telah mereferensikan proposal seperti standar tinjauan konten Prancis seolah-olah dapat diterapkan di mana pun. Dalam opininya baru-baru ini, ia menyerukan negara-negara untuk mengadopsi peraturan serupa GDPR untuk memperkenalkan kerangka kerja bersama lintas batas.

7.3 AKSES PEMERINTAH BERDASARKAN DOKTRIN FORUM PUBLIK

Dalam Knight First Amandemen Inst. di Universitas Columbia. v. Trump, 302 F. Supp. 3d 541 (S.D.N.Y. 23 Mei 2018), sekelompok tujuh warga menggugat Presiden Trump karena memblokir mereka di Twitter. Klaimnya adalah bahwa Presiden, bersama pemerintah, terlibat dalam diskriminasi sudut pandang di “forum publik” yang melanggar Amandemen Pertama. Pengadilan memutuskan bahwa feed Twitter Presiden Trump, yang digunakan secara konsisten untuk urusan pemerintahan, merupakan “forum publik yang ditunjuk” seperti taman umum tempat orang berkumpul untuk mengekspresikan pandangan mereka. Pengadilan membedakan “ruang interaktif” dari feed tersebut, di mana pengguna dapat berinteraksi dengan tweet Presiden dengan merespons, me-retweet, dll., dari tweet asli Trump, yang merupakan pidato pemerintah dan tidak tunduk pada klaim Amandemen Pertama.

Pada tingkat banding di Sirkuit Kedua, panel yang terdiri dari tiga hakim dengan suara bulat menguatkan pengadilan distrik, dengan menetapkan bahwa Amandemen Pertama tidak mengizinkan pejabat publik yang menggunakan akun media sosial untuk segala keperluan resmi untuk mengecualikan orang dari lingkungan terbuka. dialog online karena mereka menyampaikan pandangan yang tidak disetujui oleh pejabat tersebut. Pengadilan menyatakan bahwa setelah Presiden memilih sebuah platform dan membuka ruang interaktifnya bagi jutaan pengguna dan peserta, ia tidak boleh secara selektif mengecualikan mereka yang pandangannya tidak ia setujui. Pengadilan dengan cepat menambahkan bahwa tidak semua akun media sosial yang dioperasikan oleh pejabat publik adalah akun pemerintah, dan bahwa dalam banyak kasus, [kasus serupa] akan menjadi penyelidikan berdasarkan fakta, tergantung pada bagaimana pejabat tersebut menjelaskan dan menggunakan akun tersebut, fitur apa saja yang disediakan, dan bagaimana orang lain memandang dan memperlakukan akun tersebut. Putusan Sirkuit Kedua, sebagai kasus Amandemen Pertama, tidak memiliki dampak ekstrateritorial yang dapat diperkirakan.

7.4 TANGGUNG JAWAB PLATFORM DIGITAL SEBAGAI PENERBIT DAN DISTRIBUTOR

Pasal 230 Undang-Undang Kepatutan Komunikasi tahun 1996 (CDA)26 melindungi perantara online seperti platform media sosial dari tanggung jawab atas transmisi konten pihak ketiga. Tujuan legislatif yang jelas di balik Pasal 230 adalah untuk mendorong moderasi konten sekaligus memberikan kelonggaran bagi perantara untuk bereksperimen dengan strategi moderasi. Pada saat teknologi internet masih muda dan marjinal dalam sirkulasi pembicaraan, Pasal 230 dibuat untuk memberikan pionir dalam hal ini. teknologi internet awal ruang untuk berinovasi.

Senator Ron Wyden salah satu penulis Pasal 230 mengibaratkan kekebalan sebagai perisai dan pedang. Hal ini melindungi platform internet dari tanggung jawab atas konten pihak ketiga yang dihostingnya, sekaligus memberdayakan platform untuk memoderasi dan mengkurasi konten secara bebas. Dalam kedua kasus tersebut, apakah memoderasi atau gagal memoderasi, platform ini tidak diperlakukan sebagai penerbit dan oleh karena itu tidak tunduk pada tanggung jawab penerbit pada umumnya. Pasal 230 adalah ketentuan pelabuhan aman yang paling kuat dalam hal ini. jenisnya dalam hal kegiatan yang dicakupnya dan cakupan kekebalan yang ditawarkannya.

Ada pengecualian terhadap kekebalan Pasal 230. Tidak ada kekebalan dari tanggung jawab yang terkait dengan hukum pidana federal, kekayaan intelektual (yang diatur oleh undang-undang seperti Digital Millennium Copyright Act), dan undang-undang komunikasi digital tertentu. Pengadilan juga telah memperjelas bahwa perlindungan Pasal 230 tidak berlaku pada platform yang berpartisipasi dalam pengembangan, pembuatan, atau fasilitasi proaktif konten yang melanggar hukum.

Ketika platform internet menjadi begitu dominan dalam mengendalikan arus pembicaraan, maka Pasal 230 pasti akan mendapat tekanan. Kontraksi besar pertama dari Pasal 230 datang dengan undang-undang tahun 2018 yang mengizinkan negara dan korban untuk melawan perdagangan seks online (FOSTA). FOSTA, bersama dengan Undang-Undang Hentikan Perdagangan Seks (SESTA), memperluas tanggung jawab pidana federal untuk perdagangan seks. FOSTA/SESTA memungkinkan tindakan perdata dan penuntutan pidana negara bagian terhadap layanan internet karena melanggar undang-undang perdagangan seks federal.34 Singkatnya, undang-undang tersebut membuat perantara bertanggung jawab karena “dengan sengaja membantu, mendukung, atau memfasilitasi pelanggaran perdagangan seks.” FOSTA/SESTA berlaku bagi warga negara AS yang terlibat dalam perdagangan manusia di mana pun mereka berada.

Interpretasi Yudisial terhadap Pasal 230

Pasal 230 terus ditafsirkan secara luas.35 Dua kasus pada tahun 2019 dapat memberikan gambaran.

Herrick v.Grindr LLC

Herrick v. Grindr, melibatkan serangan “e-personation” apa yang disebut “malicious catfishing” terhadap Mr. Herrick melalui postingan Grindr palsu dari mantan pacarnya. Aplikasi jejaring sosial dan kencan tersebut gagal merespons serangan Herrick banyak permintaan keringanan dari ribuan pertanyaan online yang tidak diminta. Dia menggugat

Grindr berdasarkan teori pertanggungjawaban produk dalam upaya menghindari pembelaan berbasis Pasal 230. Dia mengklaim bahwa dia tidak menggugat Grindr atas perannya sebagai penerbit konten pihak ketiga, melainkan karena "manajemen penggunanya" yang buruk. Dia membidik desain dan pengoperasian aplikasi Grindr (yaitu tindakan keamanan yang tidak memadai). Pengadilan distrik dua kali memenangkan Grindr berdasarkan Pasal 230 dan Pengadilan Banding Sirkuit Kedua menegaskannya.

Second Circuit menegaskan bahwa "layanan komputer interaktif" yang tercakup dalam Pasal 230 mencakup "situs jejaring sosial dan layanan pencocokan online yang, seperti Grindr, memberi pelanggan akses ke server umum." Menolak upaya Herrick untuk menghindari masalah Pasal 230, pengadilan mengatakan bahwa "ucapan online pelaku justru menjadi dasar klaimnya bahwa Grindr cacat dan berbahaya. Klaim tersebut didasarkan pada informasi yang diberikan oleh penyedia konten informasi lain dan oleh karena itu memenuhi elemen kedua dari kekebalan § 230." Pengadilan juga menolak untuk menerima teori inovatif penggugat bahwa publikasi informasi geolokasi oleh Grindr merupakan pembuatan konten. Pengadilan mencatat bahwa informasi tersebut dihasilkan melalui proses otomatis yang dibuat oleh pengguna secara real-time. Akhirnya, argumen penggugat yang didasarkan pada dugaan cacat desain dan pengoperasian Grindr gagal. Pengadilan memutuskan bahwa "klaim cacat produksi dan desain berupaya meminta pertanggungjawaban Grindr atas kegagalannya memerangi atau menghapus konten pihak ketiga yang menyinggung, dan dilarang oleh § 230."

Force v. Facebook, Inc.

Yang lebih kuat lagi dalam penegasannya terhadap ruang lingkup Pasal 230 adalah kasus Force v. Facebook, yang juga muncul dalam Second Circuit. Kasus ini merupakan salah satu dari beberapa tuntutan hukum yang menuduh platform jaringan memberikan dukungan material terhadap terorisme. Second Circuit menjadi pengadilan banding federal pertama yang memutuskan bahwa Pasal 230 melarang klaim terorisme sipil terhadap perusahaan media sosial. Mungkin yang lebih penting, Force menegaskan bahwa kekebalan Pasal 230 berlaku untuk platform bahkan ketika proses moderasinya salah.

Di sini, keluarga korban serangan teror Hamas di Israel berusaha meminta pertanggungjawaban Facebook berdasarkan Undang-Undang Anti-Terorisme federal (ATA) karena menyediakan forum komunikasi bagi Hamas. Penggugat menegaskan berbagai klaim anti-terorisme federal terhadap Facebook, antara lain menuduh bahwa penyediaan forum bagi Hamas untuk berkomunikasi di Facebook konon memungkinkan serangan tersebut. Pada tahun 2017, pengadilan rendah menolak gugatan tersebut, dengan memutuskan bahwa "pilihan Facebook mengenai siapa yang boleh menggunakan platformnya secara inheren terikat dalam keputusannya mengenai apa yang boleh dikatakan di platformnya," yang berarti bahwa dugaan pelanggaran (yaitu kegagalan untuk menghapus hal-hal yang tidak pantas) pelaku penting dan jahat) tentu melibatkan aktivitas "penerbitan" yang dilindungi berdasarkan Bagian 230.

Pengadilan banding memutuskan bahwa terdakwa tidak akan dianggap telah mengembangkan konten pihak ketiga kecuali tergugat secara langsung dan secara material

berkontribusi terhadap apa yang membuat konten itu sendiri melanggar hukum. Karena Facebook tidak mengedit atau menyarankan pengeditan untuk konten Hamas. konten, itu bukan pengembang. Selain itu, algoritmenya tidak merusak kekebalan. Menyediakan konten adalah inti dari fungsi penerbit dan tidak berarti mengembangkan konten. Pengadilan menolak anggapan penggugat bahwa penggunaan proses algoritmik menjadikan Facebook bukan penerbit dan karenanya berada di luar cakupan Pasal 230. Singkatnya, pengadilan Force menetapkan bahwa tindakan Facebook sesuai dengan definisi "penerbit" Pasal 230. Facebook adalah bukan pengembang konten Hamas, penggunaan proses algoritmiknya tidak membahayakan status penerbitnya, dan yang terakhir, kecukupan dalam moderasi konten bukan merupakan prasyarat untuk kekebalan Pasal 230.

Perbedaan pendapat/pendapat yang disepakati oleh Ketua Hakim Katzmann dalam Force v. Facebook juga mendapat perhatian yang signifikan. Katzmann berpendapat bahwa dengan menghubungkan teroris melalui saran teman algoritmik, Facebook telah melampaui apa yang dimaksudkan untuk dicakup dalam Pasal 230. Ia berpendapat, antara lain, bahwa menghubungkan bukanlah penerbitan, dan lebih jauh lagi, bahwa penerbit dan platform adalah hal yang berbeda, yang terakhir adalah penyedia koneksi dan bukan konten. Untuk mendukung argumennya, pihak yang berbeda pendapat menganalogikannya dengan percakapan telepon, dengan menyatakan bahwa tidak masuk akal untuk mengkarakterisasi pembicara yang terlibat sebagai "penerbit" dan bukan sebagai fungsi yang lebih aktif dan terlibat.

Misalkan Anda adalah seorang penulis terbitan. Suatu hari, seorang kenalan menelepon. "Saya telah membaca semua yang pernah Anda terbitkan," dia memberi tahu Anda. "Saya juga telah melihat semua yang Anda katakan di Internet. Saya telah melakukan hal yang sama untuk penulis lain ini. Kalian berdua memiliki minat yang sangat mirip; Menurutku kalian akan akur." Kenalan tersebut kemudian memberi Anda informasi kontak dan foto penulis lain, beserta tautan ke semua karyanya yang diterbitkan. Dia menelepon kembali tiga kali lagi selama minggu depan dengan lebih banyak nama penulis yang harus Anda kenal. Meskipun gagal dalam kasus ini, perbedaan pendapat dapat memperoleh daya tarik dalam revisi Pasal 230 yang sedang dipertimbangkan di Kongres.

Pertanyaan Teritorial

Ketika Distrik Timur New York pertama kali menolak kasus Force, penggugat Force berusaha untuk berargumentasi bahwa Facebook secara tidak benar berupaya menerapkan Pasal 230(c)(1) secara ekstrateritorial. Undang-undang tersebut tidak memiliki indikasi eksplisit mengenai penerapan ekstrateritorial, sehingga pengadilan melihat ke fokus undang-undang tersebut. Teks biasa dari 230(c)(1) tidak menyewa ketentuan kekebalan berdasarkan lokasi penyedia konten atau pengguna atau penyedia layanan komputer interaktif. Pengadilan beralasan bahwa lokasi, pada kenyataannya, tidak relevan dengan penerapan Pasal 230 dan bahwa, mengingat fokus undang-undang pada pembatasan tanggung jawab, lokasi 'peristiwa teritorial' atau 'hubungan' yang relevan tidak dapat dijadikan acuan. tempat di mana klaim muncul, namun harus menjadi tempat di mana ganti rugi dicari dan kekebalan diperlukan." Dalam kasus ini, lokasi yang relevan bukanlah tempat terjadinya tindakan

merugikan (Israel) namun lokasi litigasi. Oleh karena itu, tidak diperlukan penerapan ekstrateritorial.

7.5 PROPOSAL REFORMASI TANGGUNG JAWAB PERANTARA

Hakim yang berbeda pendapat dalam kasus Force v. Facebook dengan tegas menyarankan agar Kongres mengubah Pasal 230 dan sepertinya Kongres akan melakukan hal tersebut. Ada sejumlah usulan reformasi yang sedang dipertimbangkan mengingat risiko pengurangan cakupan kekebalan perantara akan (1) mendorong platform menjadi terlalu menyensor dan dengan demikian melemahkan kebebasan berekspresi; (2) membuat pemerintah terlalu hadir dalam keputusan moderasi konten yang melanggar Amandemen Pertama; dan (3) merugikan perantara kecil yang tidak mampu mengelola risiko litigasi. Berikut adalah beberapa usulan reformasi besar.

Ex Pasca Tugas Perawatan

Salah satu pendekatan untuk memodifikasi tanggung jawab perantara adalah dengan menerapkan standar tugas kehati-hatian kepada perantara. Penerapan standar ini pada platform jaringan akan berfokus pada standar dan operasi pengelolaan konten secara keseluruhan, bukan pada kurasi dan/atau penghapusan secara individual. Berdasarkan model kewajiban kehati-hatian, suatu platform akan terkena tanggung jawab, namun tidak akan dianggap bertanggung jawab jika platform tersebut telah menjalankan kewajiban kehati-hatian sehubungan dengan moderasi konten. Pendekatan ini antara lain telah disarankan oleh Danielle Citron dan Benjamin Wittes. Bisa dibilang, pendekatan tugas kehati-hatian mendorong transparansi pada praktik moderasi konten (melawan apa yang disebut "logika keburaman") dan menghadirkan "pencegahan" pendekatan tatif" atau "kepatuhan" (dibandingkan dengan pendekatan hukuman). Perubahan seperti ini akan mengambil pendekatan yang lebih berpusat pada kelalaian terhadap tanggung jawab perantara. Hal ini akan memberdayakan pengadilan untuk menentukan apakah tindakan platform terkait konten tertentu masuk akal dengan mempertimbangkan konteks konten dan upaya platform untuk memerangi konten tersebut.

Citron dan Wittes mengutip Dirty.com, sebuah situs web "yang dikhususkan untuk menyebarkan gosip, seringkali tentang mahasiswa," sebagai contoh perusahaan internet yang diberikan perlindungan yang tidak semestinya dari Bagian 230. Dirty.com dirancang khusus untuk memperdagangkan barang-barang yang tidak pantas dan sering kali mencemarkan nama baik. gosip, namun melalui kombinasi imunitas menyeluruh dan tindakan anonim di dunia maya, penggugat secara efektif telah kehilangan hak untuk mendapatkan bantuan dalam menghadapi pencemaran nama baik atau pelanggaran privasi. Menciptakan standar perawatan yang wajar dapat memberi penggugat cara untuk mengejar pelaku kejahatan yang tidak mengambil tindakan yang cukup terhadap konten yang melanggar hukum.

Meskipun proposal Citron-Wittes akan memperluas pilihan hukum yang tersedia bagi mereka yang telah menderita kerugian yang sangat besar, hal ini juga akan membuka pintu bagi litigasi yang luas dan berpotensi tidak serius. Salah satu manfaat dari perlindungan Pasal

230 adalah memberikan kepastian hukum kepada perusahaan, termasuk perusahaan rintisan (startup) yang baru lahir dan forum skala kecil. Menurut Engine, sebuah organisasi yang melakukan advokasi atas nama perusahaan-perusahaan kecil, biaya untuk mempertahankan kasus Pasal 230 melalui seluruh proses penemuan dapat berkisar antara Rp.100.000.000 hingga lebih dari Rp.500..000.000. Menghapus kekebalan menyeluruh dari platform dengan imbalan standar kelalaian akan memungkinkan penggugat untuk terlibat dalam litigasi ekstensif yang bertujuan untuk menentukan apakah tindakan platform tersebut memang wajar.

Menciptakan Batasan Hukum Berbasis Genre

Beberapa komentator menyarankan agar Pasal 230 diperkecil untuk menghilangkan perlindungan pelabuhan aman untuk kategori komunikasi tertentu. Proposal terbaru menggunakan pendekatan ini, misalnya, sehubungan dengan pemalsuan mendalam (teknologi pembelajaran mesin canggih yang dapat membuat penggambaran audio dan video yang realistis) dan iklan yang dihosting oleh platform.

Dalam buku putih tahun 2018 mengenai peraturan platform informasi, Senator Mark Warner mengklaim bahwa perkembangan konten palsu akan "mengantar gelombang konten palsu dan memfitnah yang belum pernah terjadi sebelumnya." Buku putih tersebut menyatakan bahwa platform "mewakili 'penghindar biaya paling rendah'. ' dari dampak buruk ini" dan bahwa mereka "berada dalam posisi terbaik untuk mengidentifikasi dan mencegah konten semacam ini disebarkan di platform mereka." Senator Warner mengusulkan untuk merevisi Bagian 230 agar platform tersebut bertanggung jawab "atas gugatan hukum negara bagian karena kegagalan dalam menghapus konten audio atau video palsu atau konten audio/video lain yang dimanipulasi." Usulannya akan menciptakan sistem pemberitahuan dan penghapusan, yang mana korban dari pemalsuan mendalam dapat meminta platform untuk menghapus konten yang melanggar hukum (biasanya memfitnah). Jika mengeluarkan pemberitahuan penghapusan, platform akan bertanggung jawab jika mereka tidak mencegah konten tersebut diunggah ulang di masa mendatang.

Meskipun sistem pemberitahuan dan penghapusan, seperti yang tercantum dalam Digital Millennium Copyright Act, sering disalahgunakan, usulan Senator Warner, menurutnya, akan mengurangi risiko permintaan penghapusan yang tidak serius dengan mengharuskan korban untuk berhasil membuktikan di pengadilan bahwa konten sintetis itu berbahaya. di alam sebelum mengeluarkan permintaan penghapusan. John Bergmayer dari Public Knowledge, organisasi nirlaba kebijakan teknologi, telah menyarankan untuk mengecualikan seluruh kelas komunikasi dari perlindungan Pasal 230, dengan alasan bahwa akan bermanfaat untuk mengenakan tanggung jawab yang lebih besar pada platform untuk iklan yang mereka jalankan, bahkan ketika iklan tersebut disediakan oleh a pihak ketiga.

Pasar periklanan sangat membingungkan dan rumit sehingga perusahaan internet sering kali tidak mengetahui jenis iklan apa yang dilihat penggunanya. Selain itu, banyak iklan online yang diberikan kepada pengguna adalah penipuan, menyesatkan, atau bahkan vektor malware. Struktur pasar periklanan yang ada gagal menyelaraskan insentif dengan cara yang mempromosikan iklan berkualitas. Bagi Bergmayer, menempatkan platform pada tanggung

jawab yang lebih besar atas iklan yang mereka tayangkan berpotensi mengubah orientasi pasar sehingga meningkatkan kualitas iklan. Perusahaan-perusahaan internet dapat "memaksa industri teknologi periklanan dan penerbitan online untuk mengadopsi teknologi yang memberi mereka kontrol dan pengawasan lebih besar terhadap iklan yang mereka jalankan."

Kesamaan dari proposal Warner dan Bergmayer adalah bahwa mereka mengidentifikasi kelas konten yang berpotensi berisiko untuk dikecualikan dari perlindungan Pasal 230 guna menyelaraskan kembali insentif platform untuk mengurangi amplifikasi konten berbahaya.

Membuat Ukiran Berbasis Konten yang Sempit

Upaya terkait lebih mirip dengan pendekatan FOSTA dan terdiri dari penargetan pesan-pesan spesifik. Dalam sidang Komite Intelijen Senat mengenai pengaruh asing pada platform teknologi, Senator Joe Manchin mengajukan proposal untuk memasukkan konten perdagangan narkoba dari perlindungan Pasal 230. Langkah lainnya mungkin melibatkan pencabutan kekebalan terhadap pelecehan online, konspirasi untuk menghasut kekerasan, penguntitan dunia maya, atau penipuan konsumen.

Upaya-upaya seperti FOSTA memiliki manfaat dalam menargetkan kelas konten yang sempit, namun berisiko menciptakan kembali dilema moderator dan pidato platform yang mengerikan. FOSTA menyatakan tindakan membantu, memfasilitasi, atau mendukung perdagangan seks adalah melanggar hukum. Seperti yang dikatakan oleh seorang komentator, jika tanggung jawab dibuat berdasarkan apa yang "diketahui" oleh platform tentang konten buatan pengguna, mereka mungkin "secara rasional memilih untuk melakukan lebih sedikit pekerjaan kepolisian sebagai cara untuk mengurangi pengetahuan yang menimbulkan tanggung jawab."

Memperluas Definisi "Pengembangan" Konten

Meskipun Pasal 230 melindungi platform dari tanggung jawab yang terkait dengan konten buatan pengguna, namun hal ini tidak melindungi platform dari tanggung jawab yang terkait dengan "pembuatan atau pengembangan" konten yang melanggar hukum.

Pengadilan pada umumnya menafsirkan "pembangunan" dengan sangat sempit. Meskipun platform mengambil tindakan untuk mempromosikan atau mengkurasi konten, pengadilan menyatakan bahwa praktik ini bukan merupakan "pengembangan" konten. Dalam banyak kasus, platform membayar pengguna untuk membuat konten. Ini adalah perjanjian umum seperti YouTube, di mana platform tersebut mengadakan perjanjian pembagian pendapatan dengan pembuat konten. Pengadilan telah menolak untuk membatalkan perlindungan Pasal 230 untuk tingkat keterlibatan ini. Dalam kasus Blumenthal v. Drudge tahun 1998, pengadilan federal menyatakan bahwa AOL, yang membayar uang untuk mempromosikan artikel pencemaran nama baik yang diterbitkan oleh Drudge Report, dibebaskan dari tanggung jawab berdasarkan Bagian 230 meskipun perusahaan tersebut berkontribusi secara finansial terhadap promosi konten yang memfitnah. Hal ini terjadi karena AOL tidak berperan langsung dalam pembuatan pernyataan yang bersifat memfitnah tersebut. Platform dapat dikenakan tanggung jawab distributor jika platform tersebut

memberikan insentif finansial untuk pembuatan dan distribusi konten. Dengan kata lain, jika perusahaan seperti YouTube mengadakan perjanjian pembagian pendapatan dengan pembuat konten yang memproduksi konten yang melanggar hukum, maka perusahaan tersebut dapat dikenakan tanggung jawab untuk membantu pembuatan konten. Gagasan di balik reformasi Pasal 230 yang bertujuan untuk menciptakan tanggung jawab yang lebih luas dalam mengembangkan dan menyebarkan konten yang melanggar hukum adalah untuk mendorong platform untuk "mencari tahu dengan siapa mereka berbisnis."

Meskipun perubahan ini mungkin mendorong platform untuk lebih memperhatikan hubungan finansial mereka dengan pembuat konten, perubahan ini tidak akan mencakup banyak konten yang paling berbahaya hanya karena tidak ada tanggung jawab mendasar jika tidak ada Pasal 230. Hal ini berlaku, misalnya, pada konten mengganggu yang ditujukan untuk anak-anak. Karena konten tersebut belum tentu melanggar hukum, membuat platform bertanggung jawab atas konten yang dimonetisasi mungkin tidak menimbulkan tanggung jawab tambahan dan oleh karena itu tidak ada insentif hukum tambahan untuk memberantas konten tersebut.

Mandat "Netralitas Politik".

Pada tahun 2019, Senator Josh Hawley (R-MO) memperkenalkan Ending Support for Internet Censorship Act, yang akan memperlakukan perlindungan Pasal 230 sebagai hak istimewa dan bukan hak. Undang-undang ini mengharuskan perusahaan internet dengan ukuran tertentu untuk mengajukan permohonan " sertifikasi kekebalan" dari Federal Trade Commission (FTC). Untuk menerima sertifikasi tersebut, sebuah perusahaan harus menunjukkan, dengan kepuasan setidaknya empat komisaris, bahwa "perusahaan tidak memoderasi informasi yang diberikan oleh penyedia konten informasi lain dengan cara yang bias terhadap partai politik, kandidat politik , atau sudut pandang politik." Para komentator sangat kritis terhadap usulan Hawley, dengan menyatakan bahwa rancangan undang-undang tersebut dirancang dengan buruk, tidak tepat, dan sangat kabur. Pakar hukum Blake Reid mengkritik kurangnya kejelasan dalam mendefinisikan apa sebenarnya yang dimaksud dengan "moderasi yang bias secara politik." Pakar hukum Daphne Keller menganggap RUU ini mempunyai kelemahan pada tingkat mendasar karena "diasumsikan ada yang namanya netralitas politik dan bahwa FTC dapat mendefinisikan dan menegakkan hal tersebut. Persyaratan netralitas politik, meskipun persyaratan tersebut dapat bertahan dari tantangan yang tidak jelas, akan secara dramatis membatasi hak berpendapat para perantara online.

Proposal Senator Hawley saat ini tidak memiliki sponsor bersama di Senat dan kemungkinan besar tidak akan dilanjutkan. Namun, hal ini mungkin menjadi pertanda adanya upaya untuk membatasi kemampuan perusahaan internet dalam mengawasi platform mereka terhadap segala jenis konten yang berpotensi membahayakan.

Pasal 230 sebagai Regulatory Leverage

Menurut pakar hukum Rebecca Tushnet, perlindungan Pasal 230 pada akhirnya berarti pemberian kekuasaan tanpa tanggung jawab. Meskipun beberapa orang berdalih dengan gagasan bahwa Pasal 230 bertindak sebagai subsidi atau "hadiah," yang lain berpendapat bahwa undang-undang tersebut hanya meminta sedikit imbalan dari

perusahaan-perusahaan internet yang memperoleh manfaat darinya di masa depan, pembuat undang-undang dapat menggunakan Pasal 230 sebagai pengaruh untuk mendorong platform mengadopsi serangkaian tanggung jawab yang lebih luas. Proposal untuk menjadikan perlindungannya bergantung pada pemenuhan a serangkaian prasyarat dapat diklasifikasikan sebagai amandemen *"quid pro quo".*

Salah satu daya tarik dari reformasi Pasal 230 melalui amandemen quid pro quo adalah bahwa hal ini secara efektif membuat peraturan menjadi opsional. Hal ini memberikan anggota parlemen kemampuan untuk "mengatur" perusahaan teknologi sesuai dengan Amandemen Pertama. Struktur quid pro quo untuk perlindungan Pasal 230 akan memberikan platform pilihan: Apakah mereka ingin mengadopsi serangkaian tugas dan tanggung jawab tambahan dan transparan terkait moderasi konten atau apakah mereka bersedia melepaskan beberapa perlindungan yang diberikan oleh Pasal 230? Amandemen quid pro quo dapat dilakukan dalam berbagai bentuk. Misalnya, agar memenuhi syarat untuk mendapatkan kekebalan, platform mungkin diharuskan untuk mempublikasikan data tentang praktik kurasi dan prosedur moderasi mereka. Kemungkinan lainnya adalah bahwa platform dengan ukuran tertentu mungkin diharuskan untuk membayar sebagian dari pendapatan kotor mereka ke dalam dana yang didedikasikan untuk mendukung jurnalisme akuntabilitas yang diperlukan untuk ekosistem informasi yang sehat. Karen Kornbluh dan saya telah mengusulkan agar pelabuhan aman di Bagian 230 tunduk pada penerapan tanggung jawab platform yang lebih besar. Idenya adalah untuk mewajibkan platform besar untuk mengembangkan "praktik yang terperinci, transparan, dan menarik, khususnya untuk mengganggu kampanye terkoordinasi" yang terlibat dalam aktivitas yang "mengancam atau dengan sengaja memicu kekerasan fisik, yang jelas-jelas merupakan pelecehan online, atau merupakan penipuan komersial." Meskipun memperlakukan perlindungan Pasal 230 sebagai hak istimewa akan menjadi perubahan besar, usulan tersebut tidak melakukan diskriminasi berdasarkan sudut pandang dan memerlukan keputusan berdasarkan ex post. Hal ini mendorong platform untuk menjadi lebih bertanggung jawab dan dapat dipertanggungjawabkan serta memungkinkan mereka untuk beroperasi dengan tingkat kepastian dan penentuan nasib sendiri.

Memerlukan Prosedur Identifikasi Pengguna

Pakar hukum Gus Hurwitz telah mengajukan reformasi yang berorientasi pada proses ke dalam Pasal 230. Ia menyarankan untuk menjadikan kekebalan terhadap platform sebanding dengan kemampuan mereka untuk mengidentifikasi secara wajar pembicara yang menggunakan platform tersebut untuk terlibat dalam perkataan atau tindakan yang merugikan. Proposal ini kemudian diajukan. setelah keputusan baru-baru ini oleh Pengadilan Banding Third Circuit dalam kasus Oberdorf v. Amazon. com, di mana pengadilan memutuskan bahwa Amazon dapat dimintai pertanggungjawaban atas tindakan pengguna pihak ketiga di Pasar Amazon berdasarkan teori pertanggungjawaban produk. Third Circuit menyimpulkan hal itu, karena mereka memiliki keterlibatan yang cukup dalam memfasilitasi penjualan jika ada produk cacat yang penjualnya tidak diketahui, Amazon dapat

diperlakukan sebagai penjual produk tersebut, dan oleh karena itu tidak akan dilindungi berdasarkan Pasal 230.

Pendekatan Hurwitz menangani masalah umum anonimitas di ruang online. Platform yang melindungi anonimitas pembicara dapat secara fungsional memberikan perlindungan Pasal 230 kepada pembicara bertopeng yang membuat konten yang melanggar hukum. Jika identitas pembuat konten tidak diketahui dan platform tersebut mendapat ganti rugi, korban tindakan yang merugikan atau kriminal sering kali dibiarkan tanpa bantuan hukum yang berarti. Meskipun Hurwitz menyadari bahwa ucapan anonim seringkali merupakan alat yang penting, proposalnya mengharuskan platform untuk berhati-hati dalam memastikan bahwa pengguna yang terlibat dalam ucapan yang berpotensi melanggar hukum dapat diidentifikasi. Dengan kata lain, pendekatan ini akan diterapkan pada "platform yang menggunakan Pasal 230 sebagai perisai untuk melindungi mereka yang terlibat dalam ucapan atau perilaku yang melanggar hukum dari tuntutan hukum."

Standar Berbasis Pengetahuan

Kerangka kerja yang ditetapkan oleh Pedoman E-Commerce Uni Eropa memasukkan elemen pengetahuan ke dalam tanggung jawab perantara, sehingga membuat platform bertanggung jawab untuk menampung atau mentransmisikan konten ilegal setelah mereka memiliki pengetahuan aktual atau konstruktif tentang konten tersebut. Meskipun pendekatan ini belum populer di AS, standar serupa juga diterapkan dalam hukum hak cipta dan pidana. Kekhawatiran dari pendekatan semacam ini adalah peningkatan kontrol editorial akan digunakan sebagai bukti "pengetahuan", sehingga menghalangi platform untuk melakukan hal yang sama. jenis moderasi yang dituntut.

7.6 INISIATIF AMERIKA SERIKAT UNTUK MELAWAN DISINFORMASI

Serangkaian undang-undang dan usulan terakhir yang patut disebutkan adalah upaya melawan disinformasi dengan menggunakan pendekatan hukum lunak berupa anti-propaganda dan pendidikan media. Undang-Undang Penanggulangan Disinformasi dan Propaganda, yang dimasukkan dalam Undang-Undang Otorisasi Pertahanan Nasional (NDAA) tahun fiskal 2017, mendirikan Pusat Keterlibatan Global di dalam Departemen Luar Negeri. Pusat ini merupakan badan antarlembaga yang mengkoordinasikan upaya kontra-propaganda pemerintah dan memberikan hibah kepada kelompok-kelompok sipil yang fokus pada isu-isu serupa. RUU alokasi tahun fiskal 2018 juga mencakup Dana Melawan Pengaruh dan Agresi Rusia yang baru. Jumlah dana meningkat pada tahun 2019 dari Rp.250 juta menjadi Rp.275 juta.

Inisiatif tingkat negara bagian untuk melawan disinformasi umumnya berfokus pada literasi media. Setidaknya 24 negara bagian telah memperkenalkan rancangan undang-undang mengenai hal tersebut, yang sebagian besar diarahkan pada perubahan kurikulum tingkat sekolah dasar. Pada tahun 2018, California mengarahkan Departemen Pendidikan (DOE) untuk menyediakan sumber daya online bagi sekolah untuk evaluasi baru. Connecticut telah membentuk dewan kewarganegaraan digital, keamanan internet, dan literasi media di dalam DOE mereka. Anggota parlemen Massachusetts mengesahkan undang-undang pada

awal tahun 2018 yang mengamanatkan pendidikan kewarganegaraan dengan penekanan pada literasi media. Secara federal, Senator Amy Klobuchar (D-MN) baru-baru ini memperkenalkan Undang-Undang Kewarganegaraan Digital dan Literasi Media. Ada juga upaya baru untuk memperbarui Undang-Undang Pendaftaran Agen Asing (FARA) tahun 1938 untuk meningkatkan transparansi seputar media yang didanai asing.

BAB 8
HUKUM MEDIA EROPA DI ERA DIGITALITAS

8.1 PENDAHULUAN

Hukum media sangat dipengaruhi oleh digitalitas, terutama mengingat interaksi yang rumit antara media cetak tradisional (surat kabar) dan media yang lebih luas dalam segala bentuk komunikatifnya. Kedua dimensi ini berbeda, namun terhubung. Dalam istilah Jürgen Habermas, evolusi penting di zaman kita adalah komposisi media hukum (Rechtsmedium) dan, mengikuti Thomas Vesting, media hukum (Medien des Rechts). Praktik komputasi yang tersebar luas digitalitas dalam konteks penelitian ini terkait erat dengan media hukum Vesting dan figur hukum media. Saat ini kami sedang mengamati adanya konfigurasi ulang proses dan aktor komunikasi yang relevan dengan demokrasi. Institusi-institusi yang diciptakan pada era televisi publik pra-digital dan media lain yang kurang mapan kini diciptakan kembali untuk dinamika komunikasi digital. Media baru, konten yang lebih banyak, dan khalayak yang berbeda semuanya menimbulkan tantangan bagi hukum. Meskipun jika dilihat lebih dekat, banyak fenomena komunikasi online yang sebenarnya bukan merupakan perubahan struktural dan hanya mempercepat perkembangan yang sudah dimulai, namun proses komunikasi di platform media sosial pada dasarnya baru dan masih belum sepenuhnya dipahami. Hal ini tidak hanya berlaku pada munculnya tipe publik baru, namun juga pada rancangan peraturan yang optimal dalam ekosistem normatif sosioteknik yang kompleks.

Aturan yang ditetapkan oleh platform privat untuk komunikasi penggunanya mewakili suatu bentuk tatanan privat (dan merupakan hasil dari pembentukan tatanan privat). Meskipun sudah lama diketahui bahwa undang-undang tersebut berlaku di internet, kami menemukan bahwa sebagian besar komunikasi dan transaksi online yang relevan secara hukum terjadi di ruang pribadi tersebut. Dan ruang privat ini pada dasarnya tunduk pada aturan privat, syarat dan ketentuan umum, serta standar komunitas masing-masing perusahaan internet. Mereka menentukan apa yang bisa kita katakan secara online, apa yang bisa kita beli, perlindungan hukum pribadi apa yang bisa kita klaim. Dalam skala yang lebih besar, norma-norma privat ini menyusun tindakan-tindakan yang relevan secara publik dan memengaruhi proses-proses transaksi dan komunikasi yang penting bagi pembentukan ruang publik dan negosiasi masalah-masalah yang menjadi kepentingan publik dan dengan demikian masuk ke dalam keterkaitan yang menuntut dengan domain-domain publik. hukum publik. Hal ini juga merupakan bagian dari tatanan baru seputar hukum media.

Penegakan hukum yang ditetapkan negara secara efektif dalam ruang komunikasi digital memerlukan keterlibatan perusahaan swasta yang mengoperasikan ruang tersebut. Posisi kekuasaan mereka dan dampak sosial yang terkait dengannya sangatlah signifikan. Hal ini ditunjukkan pada bulan Januari 2021 ketika Facebook Inc dan Twitter Inc menanggapi pernyataan yang dibuat oleh Presiden AS Trump yang saat itu menjabat sebelum dan sehubungan dengan penyerbuan Capitol di Washington, DC dengan memblokir akunnya.

Perusahaan-perusahaan ini telah mengembangkan aturan-aturannya sendiri yang berbeda-beda dan, dalam pengertian fungsional, tatanan normatif. Hal ini dimasukkan ke dalam kontrak antara pengguna dan perusahaan berdasarkan hukum privat dan ditegakkan dengan desain teknis dan kelembagaan yang berbeda. Interaksi antara tatanan swasta dan publik ini rumit, dan dogma yang berbeda belum dikembangkan. Dalam penyeimbangannya, kekuasaan dan hukum dalam konstelasi hubungan yang semakin termediasi secara teknis saat ini, hukum dan keilmuannya baru saja mulai menyusun dogma normatif mengenai keterikatan dan interaksi antara hukum privat dan publik di internet mengingat perlunya hukum hibrida tata kelola pidato.

Bagaimana tatanan media Eropa menghadapi kompleksitas ini dan apakah tatanan tersebut telah berkembang secara memadai di bawah kondisi digitalitas sehingga dapat disebut sebagai "hukum media digitalitas"? Kontribusi ini akan menjawab pertanyaan-pertanyaan yang menjengkelkan ini dengan menyajikan elemen-elemen tatanan media UE saat ini sebelum membahas upaya reformasi. Pada akhirnya, kami menyimpulkan bahwa, ya, hukum digitalitas media Eropa sedang muncul.

8.2 TATANAN KOMUNIKASI EROPA DALAM DIGITALITAS

Tatanan komunikasi di era digital mengalami perubahan yang signifikan dibandingkan dengan era sebelumnya. Beberapa karakteristik utama dari tatanan komunikasi di era digital termasuk:

1. **Cepat dan Real-time:** Komunikasi dapat terjadi secara instan melalui berbagai platform digital seperti pesan teks, obrolan daring, atau media sosial. Informasi dapat tersebar dengan sangat cepat, memungkinkan respons yang lebih cepat terhadap peristiwa atau isu tertentu.
2. **Multichannel dan Multimodal:** Ada banyak saluran komunikasi yang tersedia, seperti email, pesan instan, panggilan video, dan media sosial. Selain itu, komunikasi tidak hanya terbatas pada teks, melainkan juga mencakup gambar, audio, dan video.
3. **Global dan Terhubung:** Komunikasi tidak lagi terbatas pada batasan geografis. Orang dapat terhubung dengan siapa pun di seluruh dunia dengan mudah. Hal ini memungkinkan pertukaran informasi lintas budaya dan kolaborasi internasional.
4. **Partisipatif dan Interaktif:** Era digital mendorong partisipasi aktif. Masyarakat dapat berkontribusi melalui komentar, suka, retweet, dan berbagai bentuk interaksi lainnya. Ini menciptakan lingkungan komunikasi yang dinamis dan terlibat.
5. **Personalisasi:** Teknologi memungkinkan personalisasi pesan dan konten berdasarkan preferensi dan perilaku individu. Layanan dan produk dapat disesuaikan dengan kebutuhan dan keinginan masing-masing pengguna.
6. **Big Data dan Analitika:** Data yang dihasilkan dari aktivitas digital dapat diolah dan dianalisis untuk mendapatkan wawasan yang lebih baik tentang perilaku konsumen, tren pasar, dan pola komunikasi. Ini membantu perusahaan dan organisasi untuk mengambil keputusan yang lebih informasional.
7. **Keamanan dan Privasi:** Kekhawatiran tentang privasi dan keamanan data menjadi lebih menonjol di era digital. Pengguna semakin sadar akan pentingnya melindungi

data pribadi mereka, dan perusahaan dituntut untuk mematuhi standar keamanan yang lebih tinggi.

8. **Berbasis Teknologi:** Komunikasi di era digital sangat tergantung pada teknologi. Penggunaan perangkat mobile, aplikasi, platform online, dan teknologi terkait lainnya menjadi sangat umum.
9. **Keterlibatan Multimedia:** Keterlibatan multimedia seperti gambar dan video memainkan peran besar dalam komunikasi digital. Platform seperti Instagram, YouTube, dan TikTok menjadi populer karena fokus pada konten visual.
10. **Algoritma dan Filter:** Algoritma dan filter memainkan peran penting dalam menentukan apa yang muncul di feed atau hasil pencarian pengguna. Ini dapat mempengaruhi persepsi dan paparan informasi.

Penting untuk diingat bahwa perubahan ini terus berlanjut seiring dengan kemajuan teknologi. Pemahaman dan adaptasi terhadap tren ini menjadi kunci untuk berhasil berkomunikasi di era digital.

Instrumen Hukum Khusus Media

Ruang lingkup dan isi instrumen hukum UE di sektor media dicirikan oleh kompetensi legislatif organ-organ Eropa, yang berasal dari hukum utama Eropa (yaitu Perjanjian Eropa). Jaminan pasar internal yang bebas untuk layanan termasuk layanan media audiovisual adalah titik awal dari semua langkah kebijakan media. Para legislator UE juga secara berkala merujuk pada perlindungan hak asasi manusia terkait informasi dan komunikasi dalam Art. 10(1) ECHR, dan terbatasnya kemungkinan pembatasan undang-undang dalam Art. 10(2) ECHR, sebagai dasar untuk harmonisasi instrumen hukum di bidang ini. Karena layanan media juga merupakan aset budaya yang mana UE hanya memiliki kompetensi pendukung yang terbatas fokus utama kebijakan media Eropa adalah menjamin pasar internal UE untuk media audiovisual dan penyedianya. Fokus ini bertujuan untuk menciptakan pasar untuk produksi dan distribusi layanan dan konten berdasarkan kerangka hukum yang homogen dan di mana persaingan yang sehat berlaku.

Landasan kerangka hukum media di tingkat UE adalah Audiovisual Media Services Directive (AVMSD), yang pada dasarnya menetapkan spesifikasi terkait dengan konten media audiovisual (yaitu video). Tujuan yang ingin dicapai di dalamnya berkaitan dengan harmonisasi spesifikasi undang-undang periklanan kualitatif dan kuantitatif, perlindungan martabat manusia dan anak di bawah umur, aksesibilitas, laporan berita singkat tentang acara publik, promosi karya Eropa dan independensi badan pengatur. Spesifikasi dalam Petunjuk ini biasanya tidak dapat diterapkan secara langsung, namun memerlukan transposisi ke dalam undang-undang nasional oleh masing-masing Negara Anggota. Untuk memperjelas hukum nasional mana yang harus dipatuhi oleh penyedia layanan, Petunjuk ini berisi ketentuan untuk menentukan yurisdiksi. Hal ini didasarkan pada prinsip negara asal, yang mengasumsikan bahwa hukum nasional masing-masing Negara Anggota di mana penyedia jasa didirikan secara umum berlaku. Petunjuk ini mengatur pembentukan Kelompok Regulator Eropa untuk Layanan Media Audiovisual (ERGA) untuk mendorong kesepakatan dan kerja sama yang lebih baik antara Negara-negara Anggota dalam menegakkan spesifikasi AVMSD yang diterapkan. AVMSD tidak berisi spesifikasi langsung

untuk memastikan keberagaman media, namun laporannya mencakup pernyataan dasar tentang nilai pluralisme media di pasar internal audiovisual.

Di samping kerangka penataan AVMSD terdapat undang-undang individual yang berisi ketentuan hukum mengenai konten media tertentu, misalnya dalam bidang penggambaran pelecehan seksual terhadap anak-anak. Peraturan Online Konten Teroris (TERREG)14 juga merupakan bagian dari peraturan terkait konten tersebut. aturan khusus yang memberikan persyaratan khusus untuk menangani konten yang melanggar hukum. Instrumen hukum khusus media selanjutnya adalah instrumen yang menetapkan program pendanaan untuk produksi media Eropa (khususnya Sub-Program MEDIA Eropa Kreatif) dan pengecualian khusus media, terutama di bidang aturan bantuan negara. Namun, hal ini tidak berlaku untuk semua media. merupakan aturan khusus konten media langsung untuk penyedia media.

Kerangka Hukum Khusus Sektor

UE telah mendampingi perkembangan teknologi, ekonomi dan sosial dalam bentuk informasi dan komunikasi elektronik paling lambat sejak awal tahun 1990an, termasuk melalui pengembangan lebih lanjut kerangka peraturan hukum terkait. Penawaran terkait terus muncul sebagai bentuk layanan, yang secara khusus didukung oleh Perjanjian Eropa. Berdasarkan latar belakang ini, telah muncul serangkaian peraturan yang subjeknya adalah penyediaan layanan yang disediakan atau disebarluaskan secara elektronik, dengan Pedoman e-Commerce sebagai intinya. Kerangka hukum khusus TIK dalam hukum kontrak, hukum kekayaan intelektual, dan hukum konsumen juga termasuk dalam kategori ini. Namun, konten komunikasi yang disebarluaskan secara elektronik bergantung pada infrastruktur teknis yang mengirimkan informasi dalam bentuk osilasi listrik atau bitstream. Oleh karena itu, kerangka hukum secara keseluruhan juga mencakup peraturan perundang-undangan di bidang telekomunikasi, yang pada dasarnya merupakan undang-undang persaingan usaha yang spesifik pada sektor tertentu. Selain itu, kerangka peraturan UE juga memuat spesifikasi konten yang berlaku di berbagai layanan, khususnya di bidang penggambaran dan ekspresi ilegal.

UU E-Commerce dan Jasa Elektronik

Salah satu arahan yang masih memiliki relevansi utama dalam sektor TIK adalah Pedoman e-Commerce, yang berisi aturan-aturan mendasar untuk penyediaan layanan elektronik. Ketika mengadopsi Petunjuk ini, para pembuat undang-undang Uni Eropa terutama berkepentingan untuk menciptakan suatu bidang hukum yang selaras sehingga standar minimum untuk penyediaan layanan elektronik komersial secara gratis di pasar internal digital dapat dipastikan. Resital tersebut juga mengacu pada perlindungan hak-hak dasar yang berkaitan dengan informasi dan komunikasi dari Art. ECHR, dan membatasi kebebasan tersebut. Hal-hal yang diselaraskan dengan Petunjuk e-Commerce adalah prinsip yang mengecualikan otorisasi sebelumnya dan kemungkinan untuk menyelesaikan kontrak yang sah secara hukum dalam penjualan jarak jauh kewajiban transparansi dan informasi terkait penyedia untuk komunikasi komersial dan kontrak; permasalahan yang berkaitan dengan penyelesaian perselisihan dan perlindungan hukum; dan hak tanggung jawab

sehubungan dengan konten yang disediakan pengguna dalam hal layanan perantara teknis. Petunjuk ini juga memberikan klarifikasi mengenai undang-undang nasional yang berlaku, sekali lagi dimulai dari prinsip negara asal.

Petunjuk tersebut, yang diadopsi pada tahun 2000, mendapat tekanan dalam beberapa tahun terakhir sehubungan dengan bentuk-bentuk layanan yang lebih baru dikembangkan, khususnya berkaitan dengan pertanyaan tentang kesesuaian dengan persyaratan hak tanggung jawab bagi perantara dan platform saat ini. Dengan latar belakang ini, Komisi Eropa telah mengembangkan pembaruan komprehensif Petunjuk e-Commerce sebagai bagian dari Digital Services Act (DSA). Undang-undang perpajakan juga menghadapi tantangan baru sehubungan dengan layanan digital lintas batas. Undang-undang perpajakan perusahaan klasik selalu mengasumsikan perusahaan mapan yang labanya dikenakan pajak di tempat di mana nilai tersebut diciptakan, dan akibatnya pendapatan perusahaan dapat dialihkan ke negara tertentu. Dengan adanya layanan non-fisik yang ditawarkan di seluruh UE dan dengan penyedia layanan dari luar UE, pendekatan tradisional terhadap perpajakan kini sudah melampaui batas. Usulan Petunjuk Pajak Layanan Digital (Petunjuk DST) merupakan upaya untuk menciptakan peristiwa yang dikenakan biaya atas pendapatan dari penyediaan layanan digital, dengan tarif sebesar 3%. Namun, setelah berkonsultasi dengan perwakilan AS, pendekatan tersebut ditinggalkan dan digantikan dengan pendekatan global dalam kerangka OECD.

UU Telekomunikasi

Undang-Undang (UU) Telekomunikasi di Indonesia adalah Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi. Namun, perubahan atau amendemen undang-undang dapat terjadi setelah tanggal pembaruan pengetahuan saya, dan perubahan tersebut mungkin belum termasuk dalam jawaban ini.

Undang-Undang Telekomunikasi ini mengatur sejumlah hal terkait dengan industri telekomunikasi di Indonesia, termasuk pengaturan mengenai:

1. **Lisensi dan Izin Operasional:** UU Telekomunikasi memberikan dasar hukum untuk memberikan lisensi dan izin operasional kepada penyelenggara jasa telekomunikasi. Hal ini termasuk ketentuan-ketentuan terkait dengan proses perizinan dan syarat-syarat yang harus dipenuhi oleh penyelenggara telekomunikasi.
2. **Pemanfaatan dan Pengelolaan Spektrum Frekuensi:** UU ini mengatur tentang pemanfaatan dan pengelolaan spektrum frekuensi radio yang digunakan dalam layanan telekomunikasi. Hal ini termasuk alokasi spektrum untuk berbagai layanan telekomunikasi.
3. **Hak dan Kewajiban Operator:** UU Telekomunikasi menetapkan hak dan kewajiban penyelenggara jasa telekomunikasi, termasuk tanggung jawab terhadap kualitas layanan, keamanan, dan privasi pengguna.
4. **Pengawasan dan Pengaturan:** Undang-Undang ini memberikan dasar hukum untuk kegiatan pengawasan dan pengaturan terhadap penyelenggara jasa telekomunikasi oleh Badan Regulasi Telekomunikasi Indonesia (BRTI) dan Kementerian Komunikasi dan Informatika.

5. **Pelepasan Saham dan Kepemilikan Asing:** UU Telekomunikasi juga mengatur tentang batasan kepemilikan saham dan partisipasi asing di perusahaan telekomunikasi yang beroperasi di Indonesia.

Penting untuk memeriksa sumber-sumber hukum terkini atau berkonsultasi dengan otoritas hukum setempat untuk memastikan bahwa informasi mengenai undang-undang telekomunikasi di Indonesia tetap akurat dan terkini.

Kode Komunikasi Elektronik Eropa (EECC) yang akan diterapkan pada tanggal 20 Desember 2020, menggantikan paket Petunjuk yang terakhir diubah pada tahun 2009 dalam undang-undang telekomunikasi UE dengan pengecualian Petunjuk e-Privasi. Tujuan dari Petunjuk lama dan Petunjuk kerangka hukum baru untuk telekomunikasi adalah harmonisasi kerangka hukum nasional untuk jaringan dan layanan komunikasi elektronik, fasilitas dan layanan terkait, serta bagian dari fasilitas akhir. Menyusul liberalisasi penuh jaringan telekomunikasi yang sebelumnya dikendalikan oleh negara, arahan dan peraturan tersebut bertujuan untuk meningkatkan regulasi pasar guna memastikan peningkatan persaingan, untuk mewujudkan pasar internal untuk komunikasi elektronik dan, semakin meningkatkan perlindungan konsumen dan hak-hak pengguna.

Kerangka hukum Eropa untuk telekomunikasi berkaitan dengan regulasi jaringan dan layanan komunikasi elektronik, termasuk spesifikasi alokasi frekuensi dan nomor serta koordinasi frekuensi lintas negara. Hal ini juga mencakup spesifikasi mengenai hak jalan untuk membangun dan memperluas jaringan telekomunikasi; ketentuan untuk akses jaringan dan penggunaan bersama atas komponen dan fasilitas jaringan; ketentuan mengenai keamanan dan integritas jaringan dan layanan; dan spesifikasi standarisasi dan interoperabilitas jaringan, layanan dan fasilitas terkait, termasuk layanan TV digital. Undang-undang telekomunikasi Eropa menetapkan serangkaian prosedur untuk menerapkan berbagai ketentuan (termasuk pemantauan terhadap perusahaan telekomunikasi dominan), menganalisis dan menentukan pasar relevan, dan menyelesaikan perselisihan antar perusahaan.

Relevansi kerangka undang-undang telekomunikasi untuk sektor audiovisual sangatlah tinggi. Meskipun undang-undang telekomunikasi Eropa mengecualikan penerapan terhadap konten yang dikirimkan, penyedia layanan harus bergantung pada layanan infrastruktur dan jaringan untuk menyediakan layanan media audiovisual, dan juga untuk menawarkan layanan masyarakat informasi umum. Mereka memerlukan lapisan transport untuk menyampaikan konten mereka sendiri kepada penggunanya dan, jika memungkinkan, untuk menerima permintaan kembali dari mereka. Lapisan tersebut terdiri atas layanan telekomunikasi berbasis perangkat lunak dan jaringan telekomunikasi berbasis perangkat keras. Layanan terkait konten dan penggunanya bergantung pada akses dan kegunaan lapisan dan jaringan transport yang mendasarinya sebagai saluran distribusi, dan saluran umpan balik (jika berlaku).

Oleh karena itu, permasalahan dan keputusan dalam undang-undang telekomunikasi menunjukkan hubungan langsung dan tidak langsung dengan kegiatan tertentu untuk menyediakan dan menyebarkan layanan masyarakat informasi dan dengan pilihan untuk menerima dan menggunakan layanan tersebut di pihak pengguna. Hal ini berkaitan dengan

manajemen frekuensi, ketentuan yang harus dibawa, netralitas jaringan, interoperabilitas, spesifikasi ketersediaan dan kualitas minimum jaringan dan layanan, pemisahan layanan yang terintegrasi secara vertikal dan, yang terakhir, cakupan perlindungan hak konsumen yang dimaksudkan.

Selain bentuk-bentuk interlacing dimana peraturan telekomunikasi mempengaruhi kemungkinan dan bentuk penyediaan layanan masyarakat informasi, terdapat pula layanan yang karena sifatnya berpotensi masuk langsung ke dalam ketentuan kerangka hukum telekomunikasi (lihat selanjutnya).

Spesifikasi Terkait Kontrak dan Perlindungan Konsumen di Sektor Media

Dalam beberapa tahun terakhir, UE telah mengadopsi instrumen hukum yang secara khusus berkaitan dengan layanan yang disediakan atau disebarluaskan secara elektronik, selain kerangka legislatif umum untuk perlindungan konsumen (lihat nanti).

Petunjuk Konten Digital (DCD), yang diadopsi pada Mei 2019 dan akan diterapkan pada 1 Juli 2021, bertujuan untuk menyelaraskan kerangka hukum kontrak untuk penyediaan konten digital atau layanan digital. Fokusnya adalah memastikan perlindungan konsumen tingkat tinggi agar penyelesaian kontrak lintas negara lebih terjamin secara hukum dan mengurangi biaya transaksi yang lebih tinggi yang ada hingga saat ini. Sebagai Petunjuk yang mengatur undang-undang kontrak, spesifikasi di sini terkait dengan kontrak yang menjadi dasar pengusaha menyediakan konten digital atau layanan digital kepada konsumen. Aspek yang menentukan bukanlah pembayaran, karena quid pro quo atau imbalan juga dapat diberikan melalui, antara lain, menyediakan data pribadi. Oleh karena itu, sebagian besar penawaran media dan platform digital termasuk dalam cakupan Petunjuk ini (lihat nanti). Persyaratan DCD kemudian menjadi ketentuan terkait kontrak yang juga harus dipatuhi oleh penyedia layanan, terlepas dari teknologi yang digunakan untuk penyediaan atau transmisi. Hal ini dapat berupa perangkat lunak, aplikasi, dan konten yang disediakan oleh penyedia media melalui sarana tersebut (seperti video, file audio, musik, permainan, atau publikasi elektronik). Selain itu, Petunjuk ini mencakup layanan seperti komputasi awan, hosting, media sosial, dan perangkat lunak sebagai layanan. Berdasarkan DCD, konten digital dianggap sesuai dengan kontrak jika sesuai dengan pernyataan kontrak mengenai deskripsi, kuantitas dan kualitas, fungsionalitas, kompatibilitas, interoperabilitas, dan fitur lainnya, dan “sesuai untuk tujuan tertentu yang mana konten digital tersebut dibuat. konsumen memerlukannya”. Beban pembuktian bahwa konten digital atau layanan digital sesuai kesepakatan terletak pada penyedia. Dalam hal ini, DCD menetapkan persyaratan yang tidak selalu mudah untuk ditafsirkan bagi layanan media dan berbeda dengan penyediaan layanan jurnalistik semata. Keadaan lain yang relevan mengenai DCD adalah fakta bahwa DCD merupakan Petunjuk yang mengikuti pendekatan yang disebut harmonisasi maksimum, yaitu, legislator UE telah mewajibkan Negara-negara Anggota untuk menerapkan spesifikasi secara tepat, tanpa kelonggaran atas peralihan dari Petunjuk normal, misalnya terkait dengan spesifikasi peraturan perundang-undangan nasional yang lebih ketat atau lebih lunak.

Peraturan Portabilitas diadopsi dengan tujuan untuk kebebasan bergerak di dalam UE, yang bertujuan untuk memastikan warga negara dapat menikmati akses tanpa hambatan terhadap layanan konten online di seluruh UE jika mereka untuk sementara tinggal di negara selain negara tempat mereka biasanya tinggal. Untuk itu, penyedia terkait wajib menyediakan akses yang sesuai kepada pelanggannya, termasuk dari negara UE lainnya, dengan cakupan fungsi yang sama dan tanpa biaya tambahan.

Peraturan Geo-Blocking juga didedikasikan untuk perlindungan konsumen. Dengan peraturan ini, UE berupaya mencegah diskriminasi secara tidak adil terhadap pengguna ketika melakukan pembelian online, misalnya berdasarkan kewarganegaraan, tempat tinggal, atau tempat pendirian mereka di UE. Berdasarkan ketentuannya, pemblokiran atau pembatasan akses pelanggan ke antarmuka pengguna seperti halaman atau aplikasi internet, dan syarat dan ketentuan yang diskriminatif atau tuntutan pembayaran tidak diperbolehkan, misalnya. Pengalihan halaman web ke portal atau toko khusus negara biasanya hanya diizinkan dengan persetujuan eksplisit, dan konten digital harus tersedia di seluruh UE (khususnya perangkat lunak, aplikasi, hosting web). Selain itu, penyedia harus menawarkan setidaknya satu alat pembayaran gratis. Peraturan ini hanya berlaku pada tingkat terbatas untuk layanan yang disediakan secara elektronik yang mencakup penyediaan karya yang dilindungi hak cipta. Misalnya, hal ini memungkinkan penyedia untuk mengoperasikan ketentuan layanan yang berbeda (harga, ketentuan pembayaran, ketentuan pengiriman) untuk konten yang ditawarkan melalui unduhan atau streaming. Terkait informasi mis. Jurnalistik layanan yang tidak berisi gambar atau karya yang dilindungi hak cipta tidak tercakup dalam pengecualian ini. Di sini, ketentuan Peraturan Geo-Blocking pada prinsipnya tetap berlaku. Penyedia siaran langsung dan perpustakaan media yang dioperasikan oleh perusahaan penyiaran publik juga dapat dengan bebas memutuskan sejauh mana mereka ingin mengikuti persyaratan peraturan tersebut.

Rencana dan usulan UE untuk menetapkan kerangka peraturan di bidang keputusan berbasis algoritma secara umum atau khusus kepada media, misalnya dalam bentuk Peraturan Algoritma Umum, belum terwujud dalam bentuk rancangan arahan atau peraturan. Usulan-usulan ini terkait dengan diskusi terkini mengenai kemungkinan dan batasan sistem kecerdasan buatan (AI) serta risiko terhadap hak-hak dasar yang terkait dengannya, tergantung pada domain yang bersangkutan. Mengingat sistem AI sudah digunakan oleh para produser media, penerbit dan perantara, perkembangan lebih lanjut di bidang ini dapat berdampak signifikan terhadap praktik media dan komunikasi publik. Baru-baru ini, Komisi menerbitkan proposal “Undang-Undang AI” sebagai bagian dari kerangka hukum Eropa bagi AI untuk mengatasi hak-hak dasar dan risiko keselamatan yang spesifik pada sistem AI. Sejauh platform media dan perusahaan media menggunakan AI (misalnya sebagai bagian dari rekomendasi sistem perbaikan), aturan yang terkandung dalam UU AI juga relevan bagi mereka.

Ketentuan Khusus Berdasarkan Hukum Persaingan Usaha

Peraturan tentang peningkatan keadilan dan transparansi bagi pengguna bisnis layanan intermediasi online (Peraturan P2B) merupakan instrumen yang UE

mempertimbangkan pentingnya platform dan perantara untuk visibilitas dan penyebaran layanan. Berkenaan dengan kompetensi, UE meminta kontribusi untuk memastikan kelancaran fungsi pasar internal UE. Peraturan P2B, yang mulai berlaku pada tanggal 21 Juli 2020, berlaku untuk layanan intermediasi online dan mesin pencari, yang dengannya para pengguna bisnis platform tersebut menawarkan produk dan layanan mereka kepada konsumen akhir. Konvensi ini menetapkan ketentuan-ketentuan dalam bidang ini yang bertujuan untuk memastikan transparansi, keadilan dan pilihan-pilihan pemulihan yang efektif bagi pengguna bisnis, terutama melalui persyaratan mengenai syarat dan ketentuan umum serta kewajiban informasi terhadap pengguna bisnis, dan pengungkapan kriteria seleksi dan peringkat saat menampilkan hasil pencarian. Dari sudut pandang penyedia layanan media, Peraturan P2B sangat relevan karena mewajibkan perantara untuk mengungkapkan dasar peringkat mereka, memperjelas kemungkinan perlakuan yang berbeda, dan menjelaskan modalitas akses ke platform dan data pengguna. Deskripsi terkait parameter untuk hal ini harus diungkapkan dalam bahasa yang jelas dan mudah dipahami. Untuk layanan perantara, peraturan ini memberikan aturan untuk penetapan prosedur pengaduan internal dan pilihan penyelesaian sengketa di luar pengadilan (aturan ini tidak berlaku untuk mesin pencari). Spesifikasi Peraturan P2B juga mencakup bidang kebijakan media yang telah lama menjadi bahan perdebatan: pertanyaan tentang transparansi seleksi dan logika pemeringkatan bagi perantara. Hal ini akan mengecualikan diskriminasi yang disengaja atau ditargetkan terhadap konten atau penyedia tertentu, yang dapat berdampak negatif terhadap keberagaman media. Dalam hal ini, Peraturan ini memperkenalkan ketentuan yang dapat menciptakan transparansi yang sesuai, meskipun dari perspektif hukum kontrak dan hukum persaingan usaha, dan tidak berkaitan dengan kebebasan individu atas informasi atau keragaman media. Fakta bahwa perspektif tersebut Keberagaman media tidak memainkan peran apa pun karena ini adalah bagian dari proses legislatif.

Ketentuan Khusus yang Berlaku pada Hak Kekayaan Intelektual

Kerangka kerja hak cipta memainkan peran penting dalam tatanan komunikasi UE melalui pemrosesan, pembuatan, publikasi, dan penyebaran konten yang tunduk pada hak cipta dan hak-hak terkait. Kerangka hukum ini terdiri dari beberapa langkah individual dan memungkinkan pemegang dan pengeksploitasi hak kekayaan intelektual atas karya yang dilindungi untuk memanfaatkan hak eksklusivitas untuk lisensi komersial atas konten. Perjanjian ini juga menetapkan jangka waktu perlindungan terhadap eksploitasi tersebut, dan menetapkan batasan-batasan utama terhadap hak cipta.

Tujuan dari Petunjuk InfoSoc tahun 2001 adalah untuk mengadaptasi undang-undang yang mengatur aset tak berwujud terhadap konsekuensi digitalisasi, komunikasi online, dan peningkatan konvergensi media. Petunjuk InfoSoc menyelaraskan hak reproduksi, hak komunikasi kepada publik, dan hak distribusi sesuai dengan perjanjian WIPO. Area fokus selanjutnya adalah menentukan pembatasan hak cipta dan kondisi serta cakupannya jika pembatasan tersebut dimasukkan ke dalam undang-undang hak cipta nasional oleh Negara-negara Anggota. Perjanjian ini juga menetapkan kerangka kerja untuk pengelakkan tindakan

perlindungan teknis yang diizinkan, dengan pengaturan yang tepat mengenai tindakan tersebut diserahkan kepada Negara-negara Anggota.

Reformasi undang-undang hak cipta UE yang terbaru terjadi melalui Digital Single Market Directive (DSM Directive), yang memodernisasi InfoSoc Directive di sejumlah bidang. Petunjuk DSM diadopsi pada bulan April 2019 ketika menghadapi banyak protes ("Selamatkan Internet"). Fokusnya adalah izin hukum untuk penambangan teks dan data (TDM), lisensi kolektif untuk karya seni visual di domain publik dan penetapan hak yang berdekatan untuk penerbit pers, serta hukum kontrak terkait kekayaan intelektual dan tanggung jawab online. penyedia layanan berbagi konten. Dalam hal ini ketentuan dalam Art. 15 yang memperkenalkan hak terkait baru bagi penerbit pers, dan Art. 17 yang menetapkan spesifikasi mengenai kewajiban perizinan dan tanggung jawab platform dengan konten buatan pengguna untuk membuat konten online yang dilindungi hak cipta dapat diakses memiliki relevansi khusus untuk komunikasi publik.

Petunjuk SatCab berupaya untuk menyelaraskan hak cipta nasional sehubungan dengan penyiaran lintas batas melalui kabel atau satelit. Kebebasan untuk menyediakan layanan yang dijamin dalam Perjanjian UE di seluruh pasar internal Negara-negara Anggota UE dimaksudkan untuk diwujudkan untuk penyiaran lintas batas melalui Petunjuk ini. Untuk itu, peraturan ini menetapkan ketentuan hukum terkait yang dimaksudkan untuk memudahkan operator jaringan satelit dan kabel memperoleh hak siar yang diperlukan. Untuk memperjelas hak kekayaan intelektual dan hak lisensi terkait, perusahaan ini juga mengadopsi prinsip negara asal dan pembatasan tertentu pada prinsip kebebasan kontrak sebagai standar. Meskipun terdapat kata-kata spesifik, Petunjuk Online-SatCab yang baru tidak hanya terbatas pada sosialisasi online. Tujuannya adalah untuk mempromosikan penyebaran program televisi dan radio Eropa lintas batas, termasuk melalui jaringan IP. Subyek peraturan yang dibahas mencakup tiga bidang utama. Hal ini adalah dengan mempertimbangkan prinsip negara asal penyebaran online jenis program TV dan radio tertentu di Negara Anggota UE lainnya oleh perusahaan penyiaran itu sendiri; transmisi ulang program TV dan radio dari Negara-negara Anggota oleh pihak ketiga (di mana berlaku pengelolaan hak kolektif yang bersifat wajib untuk menyederhanakan perolehan hak oleh operator jaringan dan platform); dan terakhir, transmisi program menggunakan "injeksi langsung", yang menerapkan prinsip bahwa ini hanyalah satu contoh komunikasi publik.

Petunjuk Pengelolaan Hak Kolektif (Petunjuk CRM) ditujukan untuk mengkoordinasikan peraturan nasional terkait organisasi yang melakukan aktivitas pengelolaan kolektif atas hak cipta dan hak terkait, cara kerja internalnya, dan pengawasan terhadap organisasi tersebut. Secara khusus, Petunjuk ini menetapkan persyaratan untuk pengorganisasian pengelolaan hak lintas batas secara kolektif, yang sebelumnya sering dilakukan oleh monopoli nasional. Bagi pemegang lisensi yang ingin menawarkan layanan di seluruh UE, prosedur perizinan nasional dapat disederhanakan secara signifikan, yang dalam beberapa kasus menjadi sangat rumit. Hal ini memungkinkan masuknya pasar UE secara signifikan lebih mudah untuk layanan musik dan streaming online baru.

Selain undang-undang hukum khusus media, yang sebagian merupakan reaksi terhadap perkembangan teknis dan digital saat ini, tatanan komunikasi UE juga mencakup spesifikasi umum di berbagai bidang hukum yang berbeda-beda. Di samping banyak bidang kehidupan dan situasi lainnya, hal ini juga dapat diterapkan pada layanan dan aktivitas media.

8.3 REFORMASI TATANAN MEDIA EROPA

Reformasi tatanan media adalah serangkaian perubahan dan penyesuaian dalam struktur, regulasi, dan praktek-praktek media untuk meningkatkan kebebasan pers, akuntabilitas, dan kualitas berita. Reformasi semacam itu bisa dilakukan untuk mengatasi isu-isu seperti ketergantungan pada kepentingan bisnis tertentu, bias berita, kurangnya representasi yang adil, dan tantangan lain yang dihadapi oleh industri media. Berikut beberapa aspek yang sering terlibat dalam reformasi tatanan media:

1. **Kebebasan Pers:** Reformasi media seringkali bertujuan untuk memperkuat kebebasan pers. Ini bisa mencakup perlindungan terhadap jurnalis dari tekanan politik atau ekonomi, serta pemastian bahwa media memiliki kebebasan untuk menyampaikan informasi tanpa takut represalias.
2. **Keragaman Media:** Untuk menghindari konsentrasi kekuasaan yang berlebihan di tangan beberapa pemilik media, reformasi mungkin ditujukan untuk meningkatkan keragaman kepemilikan dan perspektif dalam industri media. Ini bisa melibatkan regulasi yang membatasi jumlah kepemilikan media oleh satu entitas.
3. **Transparansi dan Akuntabilitas:** Reformasi tatanan media mungkin juga berfokus pada meningkatkan transparansi dalam kepemilikan media dan sumber pendanaan. Hal ini bertujuan untuk meningkatkan akuntabilitas dan mencegah praktik-praktik yang tidak etis.
4. **Pendidikan Jurnalisme:** Peningkatan kualitas berita seringkali berkaitan dengan pendidikan dan pelatihan bagi para wartawan. Reformasi media dapat mencakup upaya untuk meningkatkan standar pendidikan jurnalisme dan memastikan wartawan memiliki pengetahuan dan keterampilan yang memadai.
5. **Etika dan Standar Jurnalisme:** Mendorong penerapan etika jurnalisme yang tinggi dan standar kualitas dalam pemberitaan adalah bagian penting dari reformasi media. Ini bisa melibatkan pembentukan atau penguatan lembaga independen yang memantau etika dan standar jurnalisme.
6. **Partisipasi Masyarakat:** Memperkuat peran masyarakat dalam pembentukan dan evaluasi isi media adalah aspek penting dari reformasi. Ini bisa melibatkan partisipasi dalam proses regulasi, pengembangan media berbasis masyarakat, dan upaya-upaya untuk meningkatkan literasi media di kalangan masyarakat.
7. **Pengaturan yang Efektif:** Reformasi mungkin juga melibatkan evaluasi dan peningkatan peraturan yang mengatur industri media. Penting untuk menemukan keseimbangan yang tepat antara kebebasan pers dan perlindungan masyarakat dari praktek-praktek yang merugikan atau tidak etis.

Reformasi tatanan media dapat melibatkan kerja sama antara pemerintah, industri media, LSM, dan masyarakat sipil untuk menciptakan lingkungan media yang sehat dan berdampak positif.

Tahun Reformasi di Eropa

Tahun 2022 akan menjadi tahun yang besar bagi regulasi internet Eropa karena undang-undang mengenai Layanan Digital dan Pasar Digital (yang kemungkinan akan diadopsi pada saat itu) mewakili pendekatan regulasi Eropa yang komprehensif terhadap ekonomi platform. Nilai-nilai yang mendasari reformasi ini mempertahankan pengecualian dari tanggung jawab atas konten pihak ketiga sekaligus menerapkan kewajiban transparansi, lebih banyak hak bagi pengguna, dan lebih banyak tanggung jawab bagi platform tidak dapat disangkal. Angin normatif bertiup ke arah ini (bahkan undang-undang California, yang diberlakukan dalam bidang hukum yang serupa dengan hukum Eropa, telah lama berorientasi ke arah ini). Namun apakah tindakan hukum tersebut memenuhi tuntutan mereka? Ataukah klaim itu sendiri berlebihan? Dapatkah nilai-nilai penting kemasyarakatan dijamin dengan desain ulang transparansi dan undang-undang antimonopoli platform khusus, dan dapatkah platform dikontrol dengan lebih baik (dan risiko yang melekat pada desain dan properti penggunaan dapat dinilai)? Atau apakah kita mempunyai undang-undang dalam bentuk rancangan yang potensi normatifnya masih belum terealisasi?

Analisis terhadap draf tersebut sangat banyak, dan penilaian awal juga telah dipublikasikan. Pengalaman di bidang hukum telekomunikasi dan teori peraturan menunjukkan bahwa pengaturan layanan dan pasar yang kompleks sangat bergantung pada pengetahuan. Berkenaan dengan pasar digital, hal ini berlaku untuk pengetahuan tentang struktur pasar sebagai dasar untuk melakukan tindakan yang tepat, konsisten dan tepat. peraturan yang transparan. Dalam hal ini, riset pasar harus dilakukan sedemikian rupa sehingga memperluas pengetahuan tentang struktur pasar dan dampak jaringan dan membuatnya lebih mudah untuk mengidentifikasi sub-pasar mana yang memungkinkan masuknya pasar dan bagaimana memfasilitasinya. Namun, ketergantungan pengetahuan juga mempengaruhi pengetahuan pelaku pasar mengenai konsep di balik keputusan peraturan Komisi. Salah satu cara untuk mendorong peraturan yang lebih konsisten dan dapat diprediksi adalah melalui instrumen seperti “konsep peraturan” yang eksplisit (lih. Pasal 15a Undang-Undang Telekomunikasi Jerman), yang diterbitkan oleh Komisi dan menjadi dasar pengambilan keputusan di masa depan. Bagaimanapun, tampaknya tidak tepat untuk mengatur pasar yang kompleks dengan mengenakan denda.

Demikian pula, ambiguitas konsep peraturan tampaknya menimbulkan masalah dalam DSA. Konsep peraturan yang didasarkan pada pendefinisian secara hukum jenis layanan tertentu dan kemudian melampirkan kewajiban yang sesuai pada jenis layanan tersebut mencapai batasnya dalam ekosistem sosioteknik digital. Contohnya adalah pertanyaan apakah fungsi pencarian pada platform media sosial merupakan layanan pencarian atau bagian dari platform media sosial. Skala masalahnya dapat dilihat bahkan ketika para ahli terlatih mengalami kesulitan dalam mengklasifikasikan layanan internet pusat seperti Wikipedia dalam konsep dan logika peraturan DSA. Batasan berbagai jenis layanan sulit ditentukan berdasarkan undang-undang Eropa dan Negara Anggota situasi yang diperburuk oleh DMA.

Secara teori, prinsip subsidiaritas memerlukan alasan yang kuat untuk menggunakan instrumen hukum dari peraturan yang berlaku langsung dan dengan demikian melakukan harmonisasi yang luas. Dengan latar belakang ini, praktik penggunaan instrumen ini yang semakin sering harus dipandang secara kritis. Bahkan penetapan sebagai tindakan hukum (aktifikasi) tidak melindungi terhadap kritik ini. Pilihan peraturan sebagai instrumen hukum jelas membatasi kemampuan Negara-negara Anggota untuk memasukkan tradisi hukum, latar belakang budaya dan kekhasan pasar lokal mereka ke dalam struktur peraturan. Namun demikian, ada banyak hal yang bisa dikatakan mendukung regulasi dalam kasus DSM setidaknya pada pandangan pertama karena perusahaan-perusahaan yang aktif secara globallah yang menjadi subjek utama regulasi. Pada prinsipnya hal ini menimbulkan tantangan yang sama terhadap berfungsinya pasar di semua Negara Anggota. Selain itu, mengingat pentingnya platform komunikasi untuk semua tindakan yang diambil berdasarkan DMA dan juga DSA kajian dampak terkait hak komunikasi harus dilakukan. Penilaian tersebut harus mengkaji potensi dampak tindakan tersebut terhadap penyedia media. Hal ini juga harus secara khusus mencakup manfaat yang diberikan platform itu sendiri untuk komunikasi dan akses terhadap informasi. Hal ini perlu mencakup semua tindakan yang didelegasikan dan tindakan spesifik apa pun berdasarkan DSA. Jika penilaian menunjukkan bahwa mungkin terdapat dampak yang signifikan, maka perlu berkonsultasi dengan ahli independen untuk melakukan penilaian dampak sebelum keputusan diambil. Demikian pula dengan kepentingan hukum yang tertuang dalam Art. Piagam Hak-Hak Dasar Uni Eropa harus dimasukkan dalam daftar Art. 9(2) DSA (pengecualian karena alasan utama yang berkaitan dengan kepentingan publik).

Tindakan yang didelegasikan membawa tantangan dalam hal legitimasi demokratis atas keputusan yang didasarkan pada tindakan tersebut. Namun, hampir tidak ada alternatif lain ketika mengatur pasar yang kompleks dan cepat berubah di seluruh UE. Dalam hal ini, defisit legitimasi harus dikompensasikan dengan mekanisme lain. Dengan latar belakang ini, penting bagi Komisi untuk secara teratur menginformasikan kepada publik, Negara-negara Anggota, dan Parlemen Eropa mengenai tindakan-tindakan mereka berdasarkan DMA (hal ini juga berlaku untuk DSA).

Layanan Digital

Di Eropa pada akhir Januari 2021, Menteri Kehakiman Jerman Christine Lambrecht menyatakan bahwa batasan wacana publik kita tidak ditentukan di Silicon Valley: Kita, orang Eropa, yang menentukannya sendiri. Jadi aturan apa yang ingin didefinisikan oleh batas-batas ini? Pertama, rancangan DSA (satu ukuran tidak cocok untuk semua) membagi layanan internet menjadi empat kategori. Ini adalah (dalam urutan menurun): layanan perantara yang memiliki jaringan infrastruktur seperti ISP, pendaftar nama domain; layanan hosting, seperti layanan cloud dan web hosting; platform online yang mempertemukan penjual dan konsumen, seperti pasar online, toko aplikasi, platform ekonomi kolaboratif, dan platform media sosial; dan “VLOPs”, yaitu platform online berukuran sangat besar yang mempunyai risiko distribusi konten ilegal dan kerugian bagi masyarakat. Untuk layanan hosting, terdapat juga kewajiban untuk memperbaiki situasi ilegal dan memberi informasi kepada pengguna.

Kewajiban yang dibebankan pada layanan digital (beberapa di antaranya baru) dinilai berdasarkan keanggotaan kelompok. Keempat layanan tersebut, misalnya, harus menyampaikan laporan transparansi, mematuhi hak-hak dasar dalam hal penggunaan, bekerja sama dengan otoritas nasional berdasarkan perintah, dan menyediakan titik kontak dan perwakilan hukum jika diperlukan. Platform online di bawah ambang batas VLOP mempunyai empat kewajiban tambahan. Mereka harus membangun dan memelihara: mekanisme pengaduan dan ganti rugi serta penyelesaian sengketa di luar pengadilan, perlindungan bagi pelapor, pelaporan kejahatan dan transparansi iklan online. Terdapat kewajiban tambahan untuk VLOP, seperti transparansi sistem pemberi rekomendasi dan pilihan bagi pengguna dalam mengakses informasi, kewajiban manajemen risiko dan kewajiban audit, serta penunjukan petugas kepatuhan.

Meskipun rancangan saat ini, yang menetapkan kriteria transparansi untuk moderasi konten, periklanan online, atau pemeliharaan konten algoritmik, merupakan awal yang masuk akal, namun tidak satu pun dari pendekatan ini yang menjadi tujuan. Jika transparansi digunakan sebagai alat regulasi, maka harus jelas siapa yang perlu memahami secara pasti apa yang harus dilakukan untuk mencapai tujuan regulasi apakah mengenai informasi bagi pengguna, regulator, atau pelaku pasar lainnya? Konsep transparansi kemudian harus dirancang dan diterapkan untuk meningkatkan kemungkinan mencapai tujuan yang diinginkan. Hal ini kemudian dapat ditinjau dan koordinator layanan digital harus diberi wewenang untuk melakukan pengetatan jika ternyata tujuan transparansi tidak tercapai. Hak akses data yang kini diatur (Pasal 31) sudah cukup rinci, namun LSM mengkritik fakta bahwa hak tersebut hanya tersedia bagi peneliti. Pihak yang terakhir ini juga harus memperjuangkan akses secara individual. Perkembangan positif mulai bermunculan, namun mengingat tantangan praktis yang muncul, misalnya, dalam proyek “Social Science One”, masih harus dilihat apakah sistem tersebut dapat berfungsi tanpa perantara data yang bersifat altruistik, atau setidaknya publik.

Transparansi yang bermakna merupakan kriteria penting bagi akuntabilitas platform, namun diperlukan langkah-langkah lain yang tidak tercantum dalam rancangan tersebut. Beberapa praktik industri teknologi periklanan menimbulkan ancaman sistemik terhadap hak asasi manusia, terutama ketika dilakukan oleh platform online yang sangat besar.

Mekanisme pemberitahuan dan tindakan yang diusulkan tidak disesuaikan dengan kategori spesifik konten online yang dicurigai ilegal dan perlu dikembangkan lebih lanjut. Penilaian legalitas berdasarkan hukum nasional atas konten yang dilaporkan tetap menjadi tanggung jawab platform online. Dari perspektif masyarakat sipil, Access Now mengingatkan Komisi Eropa bahwa DSA akan menjadi preseden bagi pengendalian konten di luar Uni Eropa. Jika hal ini tidak dilakukan dengan benar, dampak negatif dari undang-undang ini dapat berdampak luas terhadap perlindungan hak asasi manusia. dalam ekosistem online global.

Tidak ada keharusan bagi penyedia konten untuk diberitahu sebelum tindakan apa pun diambil sehubungan dengan konten yang dilaporkan. Tindakan seperti ini akan memperkenalkan perlindungan proses yang wajar ke dalam proses pemberitahuan dan

tindakan. Tujuan memberitahukan penyedia konten akan memperkenalkan unsur keadilan prosedural. Penerapan penilaian risiko sistemik yang dilakukan oleh platform online yang sangat besar nampaknya bermasalah jika dilakukan saat ini karena didasarkan pada penilaian mandiri yang dilakukan oleh platform tersebut ditambah dengan pengawasan independen publik yang sangat terbatas. Model publik mungkin akan lebih baik di sini, misalnya di bawah kendali Koordinator Layanan Digital.

Dari segi mekanisme penegakan hukum, rancangan Peraturan ini mengikuti prinsip keutamaan koordinasi oleh lembaga-lembaga di negara tempat berdirinya. Pendekatan ini tampaknya mengikuti logika yang sama dengan mekanisme one-stop-shop dalam GDPR. Struktur pengawasan bukanlah keunggulan GDPR, dan meskipun terdapat harmonisasi menyeluruh (yang ekstensif) pada tingkat substantif, perbedaan antar negara kembali muncul dalam hal pengawasan. Ada juga pertanyaan tentang bagaimana para koordinator berhubungan dengan lembaga pengawasan lain yang sudah ada. badan-badan di Negara Anggota, seperti Otoritas Media Negara di Jerman (dan komisaris perlindungan data di negara bagian federal), yang diberi kewenangan lebih besar oleh Perjanjian Media Negara untuk komunikasi platform digital. Hal ini dapat dilihat sebagai sebuah tantangan, namun juga merupakan insentif untuk memulai reformasi yang sudah terlambat di bidang ini.

Indonesia mengalami perkembangan yang pesat dalam layanan digital di berbagai sektor. Berikut adalah beberapa layanan digital yang cukup umum dan berkembang di Indonesia:

1. **E-commerce:** E-commerce atau perdagangan elektronik telah berkembang pesat di Indonesia. Platform seperti Tokopedia, Bukalapak, Shopee, dan Lazada menyediakan berbagai produk mulai dari fashion, elektronik, hingga makanan dan minuman.
2. **Ojek Online:** Layanan ojek online seperti Gojek dan Grab telah menjadi bagian integral dari kehidupan sehari-hari di Indonesia. Selain layanan transportasi, mereka juga menawarkan layanan pesan antar makanan, pengiriman barang, dan layanan keuangan.
3. **Pembayaran Digital:** Layanan pembayaran digital semakin populer di Indonesia. Dompet digital seperti GoPay, OVO, dan LinkAja memungkinkan pengguna untuk melakukan pembayaran online, mulai dari pembelian barang dan jasa hingga pembayaran tagihan.
4. **Streaming Musik dan Video:** Platform streaming musik seperti Spotify dan Joox serta platform streaming video seperti Netflix, Disney+, dan Vidio semakin banyak digunakan di Indonesia, menawarkan beragam konten hiburan.
5. **Media Sosial:** Penggunaan media sosial seperti Facebook, Instagram, Twitter, dan WhatsApp sangat luas di Indonesia. Media sosial tidak hanya digunakan untuk berinteraksi sosial tetapi juga untuk berbagi informasi dan memasarkan produk atau layanan.
6. **Pendidikan Online:** Platform pendidikan online seperti Ruangguru, Quipper, dan Kelas Pintar memberikan akses ke materi pembelajaran dan kelas daring, memungkinkan siswa untuk belajar secara fleksibel.

7. **Telemedicine:** Layanan kesehatan digital, termasuk telekonsultasi dan aplikasi kesehatan seperti Halodoc dan Alodokter, memungkinkan pengguna untuk berkonsultasi dengan dokter secara online dan memesan obat secara elektronik.
8. **Pemesanan Tiket dan Hotel:** Platform seperti Traveloka dan Tiket.com menyediakan layanan pemesanan tiket pesawat, kereta api, dan hotel secara online, memudahkan perjalanan dan akomodasi.
9. **Asuransi Digital:** Asuransi digital semakin banyak ditawarkan di Indonesia. Perusahaan fintech dan asuransi menawarkan produk asuransi tanpa perlu mengunjungi kantor fisik.
10. **Pekerjaan Freelance dan Pekerjaan Jarak Jauh:** Platform seperti Freelancer dan Upwork memberikan peluang bagi pekerja freelance, sementara beberapa perusahaan lokal menyediakan opsi pekerjaan jarak jauh.

Layanan-layanan digital ini mencerminkan transformasi digital yang sedang berlangsung di Indonesia, menciptakan peluang baru dan meningkatkan aksesibilitas bagi masyarakat. Perkembangan ini juga memberikan kontribusi positif terhadap pertumbuhan ekonomi digital di negara ini.

Pasar Digital

Di pasar digital, beberapa platform online besar bertindak sebagai penjaga gerbang. Undang-Undang Pasar Digital bertujuan untuk memastikan bahwa segala sesuatunya berjalan adil di platform-platform ini dan, bersama dengan Undang-undang Layanan Digital, merupakan salah satu elemen inti dari strategi digital UE.

Undang-Undang Pasar Digital menetapkan serangkaian kriteria obyektif yang didefinisikan secara sempit untuk mengklasifikasikan platform online besar sebagai penjaga gerbang. Oleh karena itu, undang-undang tersebut tetap fokus pada permasalahan yang ingin diatasi sehubungan dengan platform online yang besar dan sistemik. Pada prinsipnya, peraturan pasar yang spesifik pada sektor tertentu di bidang ini tampaknya masuk akal karena adanya struktur pasar. Telah terbukti bahwa persaingan tidak terjamin di pasar-pasar tertentu dimana para pemain kuat telah lama diperbolehkan melakukan akuisisi strategis, terutama dalam jangka panjang. Hal ini disebabkan oleh berbagai efek jaringan yang menyulitkan untuk menantang posisi pasar yang sudah mapan. Tampaknya ini merupakan konsep yang tahan terhadap masa depan, karena rancangan DMA memberikan penyesuaian surut terhadap praktik bisnis tidak adil di masa depan dan bagi perusahaan yang belum menjadi penjaga gerbang. Karena pasar platform jelas cenderung tidak kompetitif bahkan dalam jangka panjang, maka masuk akal untuk mengembangkan undang-undang persaingan usaha yang spesifik pada sektor serupa dengan undang-undang telekomunikasi.

Kriteria penjaga gerbang terpenuhi ketika suatu entitas

- Memiliki posisi ekonomi yang kuat dengan dampak signifikan terhadap pasar internal dan aktif di beberapa negara UE,
- Memiliki posisi perantara yang kuat (yaitu menghubungkan basis pengguna yang besar dengan sejumlah besar perusahaan),
- Memiliki (atau akan segera memiliki) posisi pasar yang terkonsolidasi dan bertahan lama (yaitu stabil dalam jangka panjang).

Biasanya, layanan yang termasuk dalam lingkup DMA digunakan untuk transaksi, tetapi juga untuk komunikasi. Tumpang tindih ini memunculkan pertanyaan sentral yang muncul dalam setiap peraturan baru di bidang ini, yaitu bagaimana perangkat hukum yang digunakan di tingkat UE karena alasan ekonomi berhubungan dengan peraturan yang ditetapkan oleh Negara-negara Anggota untuk menjaga kebebasan dan keragaman berekspresi. Akan sangat membantu di sini untuk memperjelas Art. 1(5) yang menyatakan bahwa langkah-langkah untuk menjaga kebebasan berekspresi dan keberagaman secara eksplisit ditetapkan sebagai kepentingan publik yang dapat dicapai oleh Negara-negara Anggota sebagai bagian dari kebijakan budaya mereka tanpa mengurangi DMA. Selain itu, mekanisme prosedural seperti opsi partisipasi dan inisiatif bagi Negara-negara Anggota berguna dalam kasus di mana pemisahan kompetensi regulasi yang jelas sulit atau tidak mungkin dicapai.

Denda yang sensitif (misalnya denda hingga 10% dari omzet global tahunan) adalah bagian dari konsep ini dan dapat memberikan efek jera yang cukup besar bahkan terhadap perusahaan teknologi besar. Namun, tidak mudah untuk menentukan dalam kondisi apa penjualan paksa bagian-bagian suatu perusahaan benar-benar menyelesaikan masalah yang ada karena hanya ada sedikit contoh dalam sejarah regulasi pasar. Pendekatan dasar untuk mengatasi kekuasaan penjaga gerbang berdasarkan kepemilikan data tampaknya menanggapi masalah nyata yang berkaitan dengan larangan penggunaan data oleh pelanggan bisnis untuk menghasilkan produk pesaing. Apakah larangan umum terhadap pengumpulan data dari sektor bisnis yang berbeda dan larangan login otomatis ke beberapa layanan benar-benar merupakan kepentingan konsumen dan, terlebih lagi, merupakan tindakan yang proporsional, tidak dapat dinilai di sini (tetapi masih terbuka untuk dipertanyakan). Larangan umum terhadap iklan yang dipersonalisasi seperti yang diusulkan oleh beberapa pemangku kepentingan sebagai bagian dari DMA hanya boleh dipertimbangkan setelah mempertimbangkan secara cermat potensi dampaknya terhadap layanan informasi dan komunikasi. Betapapun pentingnya masalah privasi, hal ini harus diimbangi dengan masalah kebebasan berkomunikasi dan kebebasan akses terhadap informasi. Ditambah lagi, sebagian besar media milik swasta bergantung pada pendanaan iklan.

Regulasi layanan digital mencakup kerangka kerja hukum yang mengatur berbagai aspek dari ekosistem layanan digital, termasuk perlindungan konsumen, privasi data, keamanan, persaingan, dan aspek-aspek lainnya. Regulasi ini dapat bervariasi di setiap negara, dan beberapa negara mungkin memiliki lembaga atau badan khusus yang bertanggung jawab untuk mengawasi dan menegakkan peraturan-peraturan tersebut. Di Indonesia, misalnya, Badan Regulasi Telekomunikasi Indonesia (BRTI) dan Kementerian Komunikasi dan Informatika memiliki peran dalam mengatur sektor telekomunikasi dan informatika. Berikut adalah beberapa area regulasi utama yang sering terkait dengan layanan digital:

1. **Perlindungan Konsumen:** Regulasi ini menetapkan hak dan kewajiban penyedia layanan digital dalam melindungi konsumen. Ini mencakup transparansi biaya, jaminan produk dan layanan, dan prosedur penyelesaian sengketa konsumen.
2. **Privasi Data:** Regulasi privasi data menetapkan standar perlindungan data pribadi pengguna layanan digital. Undang-undang atau peraturan ini biasanya mengatur cara pengumpulan, pengolahan, penyimpanan, dan berbagi data pribadi.
3. **Keamanan Cyber:** Regulasi keamanan siber mengatur langkah-langkah yang harus diambil oleh penyedia layanan digital untuk melindungi data dan infrastruktur mereka dari serangan siber. Ini mencakup persyaratan keamanan teknis, prosedur pelaporan insiden keamanan, dan kewajiban untuk melindungi data pengguna.
4. **Pajak Digital:** Pajak digital mencakup regulasi terkait perpajakan untuk transaksi dan penghasilan yang terkait dengan layanan digital. Beberapa negara telah menerapkan aturan khusus untuk mengenakan pajak pada perusahaan teknologi besar yang beroperasi di wilayah mereka.
5. **Hak Kekayaan Intelektual:** Regulasi ini melibatkan perlindungan hak kekayaan intelektual, termasuk paten, merek dagang, dan hak cipta. Ini memastikan bahwa inovasi dan karya kreatif dilindungi, mendorong investasi dalam penelitian dan pengembangan.
6. **Persaingan:** Regulasi persaingan mengatur perilaku bisnis dalam rangka mencegah praktek-praktek anti-persaingan yang tidak sehat. Hal ini bertujuan untuk mendorong persaingan yang adil dan inovasi di pasar layanan digital.
7. **Layanan Keuangan Digital:** Ketika melibatkan transaksi keuangan dan layanan keuangan digital, regulasi yang ketat diterapkan untuk melindungi konsumen, mencegah pencucian uang, dan memastikan stabilitas sektor keuangan.
8. **Aspek Lainnya:** Beberapa negara juga memiliki regulasi khusus terkait dengan sektor-sektor tertentu, seperti regulasi kesehatan untuk layanan kesehatan digital, atau regulasi pendidikan untuk platform pendidikan online.

Penting untuk dicatat bahwa regulasi di ruang layanan digital terus berkembang seiring dengan perubahan teknologi dan tuntutan masyarakat. Pemerintah dan lembaga terkait harus secara terus-menerus mengevaluasi dan memperbarui regulasi untuk mencerminkan dinamika yang terjadi di dunia digital.

Beberapa undang-undang dan regulasi yang relevan dengan sektor pasar digital di Indonesia termasuk:

1. **Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE):** UU ITE mencakup aspek-aspek hukum terkait dengan transaksi elektronik, termasuk keamanan dan perlindungan data.
2. **Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen:** Meskipun undang-undang ini bukan khusus untuk pasar digital, namun beberapa ketentuannya relevan dengan perlindungan konsumen dalam konteks bisnis online.
3. **Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Elektronik:** Regulasi ini mengatur tentang penyelenggaraan sistem elektronik, yang mencakup aspek-aspek teknis dan operasional dari bisnis elektronik.

4. **Kementerian Perdagangan Republik Indonesia:** Kementerian Perdagangan memiliki peran dalam mengawasi perdagangan elektronik dan e-commerce di Indonesia. Beberapa pedoman dan regulasi terkait e-commerce telah diterbitkan oleh kementerian ini.
5. **Badan Regulasi Telekomunikasi Indonesia (BRTI):** BRTI memainkan peran penting dalam mengatur sektor telekomunikasi dan informatika di Indonesia. Mereka dapat terlibat dalam pengawasan dan regulasi terkait dengan layanan digital.
6. **Badan Pengawas Perdagangan Berjangka Komoditi (BAPPEBTI):** BAPPEBTI adalah badan yang mengawasi perdagangan berjangka, termasuk kegiatan perdagangan kripto atau mata uang digital.

Namun, karena dinamika cepat pasar digital dan ekonomi digital, pemerintah mungkin terus mempertimbangkan pembuatan undang-undang yang lebih khusus untuk mengatur sektor ini. Oleh karena itu, sangat penting untuk memeriksa sumber-sumber hukum terkini dan pembaruan resmi dari pemerintah Indonesia atau lembaga-lembaga terkait untuk mendapatkan informasi yang paling akurat dan terkini.

Kesimpulan

Hukum media di Eropa terfragmentasi dan tidak sepenuhnya koheren. Ketentuan-ketentuan yang berdampak pada hukum media sebagaimana dipahami secara luas berasal dari berbagai bidang hukum Eropa, berdiri dalam tradisi peraturan yang berbeda, dan mengikuti logika (dan istilah-istilah yang digunakan) yang terkadang tidak sesuai dengan hukum media. satu sama lain. Hal ini dapat menimbulkan konflik. Undang-undang media Eropa mengenai “digitalitas” hanya dapat dianggap sebagai undang-undang Eropa jika ketentuan legislatifnya bertujuan untuk melakukan harmonisasi terkait pasar yang bertujuan untuk melengkapi pasar internal (Pasal 26 TFEU). Hal ini membuat hukum media di Eropa cenderung berorientasi pasar dan diimbangi dengan Piagam Hak-Hak Fundamental UE.

Salah satu karakteristik hukum media Eropa adalah seringnya diperkenalkannya terminologi-terminologi baru, cakupan penerapan yang berbeda, dan peraturan yang cenderung bersifat “empiris” dan didorong oleh fenomena. Penilaian dampak dapat menghindari beberapa kendala peraturan, namun biasanya dilakukan jauh sebelum instrumen hukum baru “dimasukkan ke pasar”.

Baru-baru ini, undang-undang media Eropa ditandai dengan adanya dorongan yang lebih kuat untuk memastikan tata kelola publik bagi para pelaku media swasta, khususnya platform. Rancangan Undang-Undang Layanan Digital dan Undang-Undang Pasar Digital, ditambah dengan Undang-Undang Tata Kelola Data dan Undang-Undang AI, akan memberikan kerangka kerja yang benar-benar baru dan mencakup undang-undang media Eropa yang dapat menghilangkan beberapa kekhawatiran mengenai koherensi dan orientasi pasar dari peraturan sebelumnya.

Berbeda dengan di AS, di mana reformasi yang berarti dari Sec. 230 tampaknya gagal karena banyaknya proposal yang bersaing, model konsolidasi (dan konsolidasi) Komisi didasarkan pada penelitian substansial mengenai praktik terbaik tata kelola platform. Salah satu keberhasilan pendekatan regulasi adalah jika pendekatan ini direplikasi di tempat lain. Kami melihat “efek Brussels” awal juga terjadi di sini. Eropa tampil sebagai kekuatan

normatif dan telah mengambil bagian-bagian penting dari keterlibatan selama bertahun-tahun dengan ide-ide paling penting dari penelitian platform kritis yang dilakukan oleh staf Komisi. Tampaknya Komisi juga ingin memberikan kekuasaan yang besar untuk memperkuat tatanan media Eropa yang baru dengan menyediakan sejumlah besar tindakan hukum sekunder dalam kerangka komitologi. Dalam hal apa pun, mekanisme kompensasi harus disediakan di sini (hal ini juga demi kepentingan penerimaan peraturan baru di pihak Negara-negara Anggota serta perusahaan-perusahaan yang terkena dampak).

Mencapai koherensi peraturan di tingkat Eropa, antara tingkat UE dan Negara-negara Anggota, dan secara global semakin menantang. Koherensi dapat memperoleh manfaat dari kerangka kerja jangka menengah yang berisi prinsip-prinsip yang akan diikuti UE di seluruh sektor dan kebijakan dalam menciptakan tatanan normatif masa depan untuk layanan digital. Pada saat yang sama, upaya reorganisasi tata kelola platform Eropa tidak boleh dibebani dengan ekspektasi yang tidak dapat diwujudkan. Baik peraturan akuntabilitas dan transparansi yang baru, maupun undang-undang antimonopoli platform khusus, peraturan data baru, atau pembatasan penggunaan kecerdasan buatan tidak akan baik secara terpisah atau secara keseluruhan membalikkan tren sosial (seperti gerakan menuju individualisasi atau fragmentasi sosial atau perpecahan politik) , atau proses perubahan media atau perubahan perilaku penggunaan media. Oleh karena itu, upaya menuju demokrasi yang "tahan terhadap platform" harus selalu disertai dengan langkah-langkah struktural lainnya. Dari sudut pandang ini, mendesain ulang kerangka hukum untuk platform adalah suatu awal yang perlu dan dapat dilihat sebagai landasan undang-undang komunikasi Eropa yang baru. digitalitas, namun hal ini jelas bukan akhir dari proses menjamin kebebasan demokratis dan menentukan nasib sendiri secara berkelanjutan. Tugas memperbarui demokrasi dimulai dari awal setiap hari.

Bagian V

Peraturan Keuangan dan Hukum Pidana

BAB 9
REGULASI MATA UANG VIRTUAL

9.1 MATA UANG DIGITAL SEBAGAI BENTUK DIGITALITAS GLOBAL

Mata uang digital merupakan fenomena digital dan global. Mata uang digital dengan perbedaan tergantung pada bentuk konkritnya dibentuk melalui operasi berbasis algoritma dan ditransfer melalui operasi berbasis algoritma. Dengan blockchain, mata uang digital didasarkan pada teknologi yang tidak hanya mentransfer proses yang ada di dunia analog ke dunia digital, namun juga menciptakan properti yang tidak dimiliki alat pembayaran konvensional. Mekanisme untuk memvalidasi suatu transaksi, yang menciptakan kepercayaan terhadap legitimasi pihak yang mengadakan kontrak dan kelanggengan transaksi, didasarkan pada metode enkripsi asimetris dan penyimpanan redundan yang terdesentralisasi, yang tidak mungkin dilakukan di dunia analog.

Nilai Tambah Data Pembayaran

Karakteristik ekonomi mata uang digital juga penting karena karakter digitalnya yang spesifik. Data yang dihasilkan oleh transaksi keuangan digital memiliki nilai komersial yang cukup besar. Oleh karena itu, layanan pembayaran digital menjadi pendorong model bisnis lintas pasar yang kompleks. Pada saat yang sama, mereka merupakan elemen sentral dari platform dan ekosistem digital.

Transaksi keuangan digital menyediakan data tentang objek dan orang-orang yang terlibat dalam transaksi tersebut. Mirip dengan model bisnis lain di pasar digital, data ini dapat dikomersialkan dalam berbagai konteks. Ciri khas komersialisasi ini adalah item data dari sejumlah sumber berbeda diperiksa korelasinya. Basis data yang terklaster memungkinkan perkiraan dalam kasus-kasus yang tidak diketahui dan model bisnis berdasarkan probabilitas statistik. Relevansi komersial data pribadi ini memunculkan model bisnis multilateral yang mensubsidi layanan di bursa tertentu untuk memperoleh data pribadi sehingga data tersebut dapat digunakan di tempat lain. Akses terhadap data, dan khususnya data pembayaran, akan menjadi kunci faktor untuk posisi pasar di pasar masing-masing.

Dampak Terhadap Layanan Pembayaran Digital Dan Mata Uang

Pentingnya data juga menyangkut layanan pembayaran digital dan mata uang digital. Saat menggunakan layanan pembayaran digital, setiap transaksi secara otomatis menghasilkan data pribadi tentang keadaan transaksi, yang dapat digunakan sebagai dasar untuk profil orang tersebut dan untuk korelasi lebih lanjut. Oleh karena itu, data pembayaran sangat cocok sebagai dasar analisis berbasis korelasi. Nilai tambah data ini adalah alasan utama mengapa operator platform yang paham data seperti Apple, Google,

Amazon, dan Microsoft mengembangkan layanan pembayaran mereka sendiri untuk pembayaran seluler dan digital.

Perkembangan Ekosistem Digital Pada Jasa Keuangan Digital

Layanan pembayaran digital dan mata uang menjadi elemen ekosistem digital. Dalam hal layanan pembayaran, pengolahan data terkait transaksi menjadi dasar informasi yang dapat digunakan, antara lain, untuk mengoptimalkan produk keuangan dan menilai orang-orang yang terlibat. Objek umum dari analisis berbasis algoritma ini adalah kelayakan kredit seseorang, preferensi mereka terhadap produk tertentu atau risiko asuransi. Karena analisis berdasarkan korelasi berasal dari probabilitas yang ditentukan secara statistik dan dapat ditransfer dalam prosedur ini, kontak pelanggan juga memungkinkan perkiraan dibuat untuk orang-orang yang hampir tidak dikenal. Oleh karena itu, data terkait pembayaran mempunyai potensi efek sinergi yang besar.

Contohnya adalah portofolio produk dan layanan Ant Financial Services Group, sebuah perusahaan fintech yang muncul sebagai anak perusahaan dari Alibaba Group asal Tiongkok. Meskipun perusahaan ini awalnya didirikan untuk memberikan dukungan dalam bentuk layanan pembayaran untuk platform perdagangan Alibaba, Alipay telah berkembang lebih jauh dari konteks ini menjadi platform pembayaran digital. Selain itu, sistem pemeringkatan kredit (Sesame Credit) memfasilitasi pemberian kredit dan dana pasar uang (Yu'e Bao), yang juga termasuk dalam grup, memfasilitasi akses terhadap dana likuid sebagai alternatif terhadap lembaga kredit yang sudah mapan. Contoh Ant Financial Services Group sebagian besar didasarkan pada karakteristik spesifik konteks Tiongkok. Di satu sisi, terdapat kebutuhan yang besar terhadap layanan pembayaran bagi konsumen akhir dan pinjaman untuk usaha kecil dan menengah. Di sisi lain, kerangka hukum perlindungan data serta penerimaan sosial untuk pemrosesan data pribadi menguntungkan untuk aplikasi yang membutuhkan banyak data. Namun demikian, tidak dapat diabaikan bahwa sinergi berbasis data di masing-masing bidang bisnis telah meningkatkan kinerja Grup dan masing-masing perusahaan secara signifikan, dan khususnya kemampuan mereka untuk beradaptasi dengan cepat terhadap perubahan ekonomi, peraturan atau teknis. Kapitalisasi pasar yang diharapkan dari IPO Ant Financial Group, yang baru-baru ini ditunda karena kekhawatiran lain, mencerminkan potensi pasar perusahaan berbasis data konglomerat, yang juga berlaku, terlepas dari semua perbedaan, pada pasar terkait di benua lain.

Oleh karena itu, otoritas pengawas Eropa membedakan tipifikasi perusahaan fintech antara fintech tersebut, yang sebagai perusahaan start-up biasanya fokus pada penawaran berbasis teknologi tertentu, dan yang disebut perusahaan Big Tech. Perusahaan-perusahaan Teknologi Besar ini dicirikan oleh fakta bahwa mereka telah mengembangkan pengetahuan dalam menganalisis data dalam jumlah besar dan eksploitasi komersialnya di sejumlah pasar berbeda dan memasuki pasar keuangan baru. Mereka mengkompensasi kelemahan mereka, yang biasanya disebabkan oleh terbatasnya pengetahuan mereka mengenai industri ini, termasuk persyaratan peraturannya, dengan kekuatan mereka dalam mengakses dan memproses data yang relevan. Dari sudut pandang mereka, nilai tambah dari penawaran finansial layanan biasanya terletak lebih sedikit pada pendapatan yang dapat dihasilkan

secara langsung dibandingkan pada peningkatan basis data dengan data pribadi dengan referensi keuangan.

Ekosistem Dalam Mata Uang Digital

Relevansi basis pengetahuan berbasis data untuk ekosistem digital juga menjadi ciri sifat ekonomi mata uang digital. Mata uang digital memiliki karakteristik yang mirip dengan platform digital. Operator infrastruktur mata uang digital menerima data transaksi tidak hanya terkait dengan transaksi yang melibatkan operator secara langsung. Sebaliknya, data dihasilkan dari semua transaksi yang dilakukan dalam mata uang masing-masing.

Mata uang "Diem", yang diumumkan beberapa waktu lalu dan kemudian ditinggalkan, antara lain karena tujuan regulasi, mengikuti strategi yang secara eksplisit dirancang untuk terhubung dengan platform yang ada. Dalam kasus Libra, posisi pasar jejaring sosial Meta akan digunakan untuk mencapai tingkat penyebaran yang signifikan dengan diperkenalkannya mata uang virtual. Materi yang disediakan oleh konsorsium juga menunjukkan bahwa berbagai anggota konsorsium akan secara aktif mempromosikan penggunaan dan penyebaran mata uang virtual dengan memberikan persyaratan khusus dalam penawaran mereka. Dari sudut pandang antimonopoli, Diem telah telah dikaitkan dengan posisi dominan sejak awal diperkenalkan karena latar belakang jaringan sosial Facebook. Sebaliknya, pengenalan mata uang virtual tersebut memperkuat posisi pasar jaringan sosial atau ekosistem digital. Penggunaan mata uang virtual tidak hanya menghasilkan sejumlah besar data terkait transaksi, namun efek jaringan yang terkait dengan mata uang virtual semakin memperkuat efek jaringan yang menjadi ciri jaringan sosial. Dengan kata lain, bentuk mata uang digital ini memadukan karakteristik layanan pembayaran digital dengan karakteristik ekonomi platform digital.

9.2 MATA UANG DIGITAL SEBAGAI FENOMENA GLOBAL

Karena karakteristiknya, mata uang virtual tidak hanya merupakan fenomena digital tertentu, namun juga merupakan fenomena global. Dari sudut pandang ekonomi, globalitas terlihat jelas terutama pada volume mata uang virtual dan penyebaran global yang terkait. Bank for International Settlements telah memperkenalkan istilah "koin stabil global" untuk menggambarkan kategori mata uang virtual yang, di satu sisi, dicirikan oleh efek jaringan yang besar karena berbagai alasan dan, di sisi lain, dapat memiliki efek yang signifikan. misalnya mengenai langkah-langkah kebijakan moneter atau stabilitas pasar keuangan. Dimensi global mata uang digital yang bersifat lintas batas adalah hasil dari beberapa faktor teknis dan ekonomi yang independen.

Faktor Teknis Globalitas

Sisi teknis dari globalitas mata uang digital terlihat jelas dalam bentuk teknologi blockchain yang terdesentralisasi, sebagaimana dikenal dari mata uang virtual "Bitcoin". Di satu sisi, mekanisme desentralisasi validasi transaksi individu mengarah pada fakta bahwa Bitcoin individu ada secara independen dari pengakuan hukum oleh satu negara. Mata uang virtual, yang menciptakan unit secara eksklusif berdasarkan kode, sehingga sejak awal menghindari klasifikasi sebagai mata uang nasional atau internasional. Mata uang virtual

tersebut tidak lagi dapat ditetapkan ke negara tertentu. Biasanya bahkan tidak memiliki pusat lokal tertentu. Oleh karena itu, keuntungan ekonomi utama dari mata uang virtual terletak pada kemampuan transfernya yang cepat, mendunia, dan hemat biaya. Karena mata uang virtual hanya memerlukan akses ke internet, maka mata uang virtual menawarkan ketersediaan dan kemampuan transfer global, yang dalam hal mata uang negara harus disediakan oleh infrastruktur. Infrastruktur tersebut biasanya didasarkan pada kerja sama antara bank sentral yang berpartisipasi dan lembaga kredit swasta atau penyedia komersial lainnya yang layanannya didasarkan pada infrastruktur yang disediakan. Dengan kata lain, globalisasi mata uang negara yang sudah mapan, bahkan dalam bentuk digital seperti uang kitab suci, biasanya bergantung pada layanan perantara dari perantara swasta, sehingga menimbulkan biaya tambahan. Oleh karena itu, biaya transaksi internasional adalah salah satu alasan mengapa bank sentral (yaitu mata uang digital bank sentral) mempertimbangkan untuk menerbitkan mata uang digital.

Di sisi lain, sistem blockchain yang dirancang secara desentralisasi mengandalkan distribusi node yang terdesentralisasi untuk memastikan keamanan terhadap manipulasi. Kepercayaan terhadap integritas blockchain justru didasarkan pada sifat node yang terdesentralisasi, yang dirancang dan dikoordinasikan sebagai unit independen dalam algoritma. Varian desain, di mana satu aktor atau kelompok aktor tertentu mempertahankan kepentingan tunggal atau kendali yang tegas atas pengembangan blockchain yang sedang berlangsung (yaitu transaksi tidak divalidasi oleh operasi yang terdesentralisasi, independen, namun terkoordinasi) memerlukan lebih sedikit upaya dalam koordinasi. Terutama dengan peningkatan volume, upaya, termasuk energi dan daya komputasi, untuk validasi transaksi individual menjadi jauh lebih rendah. Selain itu, konfirmasi dan registrasi transaksi memerlukan waktu yang lebih singkat. Namun demikian, sistem yang memusatkan pengaruh dan kendali pada satu titik secara otomatis lebih rentan terhadap manipulasi eksternal.

Faktor Ekonomi Globalitas

Mata uang virtual, seperti stablecoin, yang menghubungkan unit virtual dengan jaminan nyata seperti sekuritas atau mata uang negara, bergantung pada integrasinya ke dalam sistem hukum melalui hubungan ini. Meskipun umumnya bersifat global, hubungan ini menjadikan mata uang virtual sebagai objek peraturan nasional, dan akibatnya menimbulkan sejumlah permasalahan dalam penanganan situasi lintas batas, seperti hukum perdata internasional, kerja sama pengawasan, atau saling pengakuan. Menghubungkan mata uang virtual dengan keamanan nyata mengikat mata uang virtual ke sistem hukum dan dengan demikian memperkenalkan kembali perbedaan antara nasional dan internasional. Terlepas dari faktor hukum globalitas, mata uang virtual, terutama jika ada platform atau jaringan di balik masalah ini, didistribusikan secara global karena alasan ekonomi.

Biaya Tukar Dan Fungsi Ekonomi Uang

Dampak jaringan langsung dan tidak langsung yang terkait dengan platform ini menimbulkan biaya peralihan bagi pengguna. Biaya peralihan tersebut dapat timbul dari fakta bahwa sejumlah besar mitra transaksi menggunakan mata uang virtual masing-masing secara berkelanjutan atau bahwa sejumlah besar mitra transaksi disimpan di masing-masing

mata uang virtual tersebut. mata uang. Lebih tepatnya, jenis dan intensitas biaya pertukaran dihasilkan dari fungsi penggunaan mata uang virtual dalam kasus individual dan kondisi kerangka masing-masing. Meskipun mata uang konvensional yang dikeluarkan oleh negara, dari sudut pandang ekonomi, mempunyai tiga fungsi, yaitu penyimpanan nilai, unit hitung, dan transfer nilai, mata uang virtual memenuhi fungsi-fungsi ini dalam tingkat yang berbeda-beda tergantung pada karakteristiknya.

Mata uang virtual dengan volatilitas tinggi, misalnya, kurang cocok untuk menyimpan nilai. Sebaliknya, kesesuaiannya untuk transfer jangka pendek sangat bergantung pada penerimaan mata uang virtual oleh mitra transaksi potensial lainnya dan biaya satu transfer. Mata uang virtual, yang biasanya ditransfer dengan biaya rendah dan diterima oleh banyak pemain, dalam hal ini juga cocok untuk mentransfer nilai meskipun nilainya mengalami fluktuasi besar dalam jangka menengah. Dalam hal ini, pengguna akan menggunakan mata uang virtual secara eksklusif untuk transfer dan kemudian mengubah unit virtual ke unit yang tidak terlalu fluktuatif sesuai kebutuhan. Jika konversi unit virtual dapat dilakukan dengan biaya transaksi yang rendah, maka digitalisasi mata uang akan menyebabkan pemisahan fungsi yang, dalam kasus mata uang konvensional, terjadi bersamaan. Mata uang virtual mungkin hanya cocok untuk beberapa fungsi saja. dan digunakan untuk fungsi-fungsi tersebut karena kemudahan konvertibilitasnya. Selain itu, karakteristik mata uang virtual, khususnya kesesuaiannya untuk satu fungsi atau lainnya, sangat bergantung pada desain teknis dan koneksi ekonomi ke suatu platform. Dalam kasus stablecoin, yang terpenting adalah menghubungkan unit ke keamanan nyata yang meningkatkan stabilitas nilai. Selain kondisi kerangka teknis validasi, kesesuaian transfer nilai pada dasarnya bergantung pada penerimaan unit tersebut, yang dapat ditingkatkan secara signifikan dengan menghubungkannya ke platform sosial yang ada.

Bagian Dari Jaringan Bukan Wilayah Geografis

Sebagai konsekuensi dari biaya pertukaran ini, pengguna mata uang virtual membentuk jaringan yang, berbeda dengan mata uang yang dikeluarkan oleh negara, tidak terkonsentrasi di wilayah lokal tertentu namun ditandai dengan partisipasi dalam ekosistem digital dan dengan demikian oleh efek jaringan. Mirip dengan platform digital lainnya, hubungan antara pengguna mata uang virtual dan koneksi mereka ke ekosistem digital tercipta melalui penggunaan, meskipun intensitas tautan bervariasi tergantung pada desain platform.

9.3 KERANGKA HUKUM MATA UANG VIRTUAL

Karakteristik khusus mata uang digital ini menimbulkan sejumlah konsekuensi berbeda terhadap kerangka hukum. Di satu sisi, fakta hukum biasanya disesuaikan dengan situasi yang menyiratkan karakteristik teknis tertentu dari transaksi atau modalitas komunikasi tertentu. Klasifikasi hukum atas fakta yang diterapkan dalam lingkungan digital biasanya memerlukan adaptasi atau penerjemahan. Perlunya upaya adaptasi yang dipicu oleh fenomena digitalisasi tidak terbatas pada bidang layanan pembayaran atau mata uang virtual.

Di sisi lain, karakteristik khusus mata uang digital menimbulkan permasalahan peraturan yang memerlukan tindakan khusus. Kekhususan tersebut menyangkut risiko tertentu yang melekat pada karakteristik mata uang digital, misalnya dalam bidang pemberantasan pencucian uang atau pendanaan teroris, perlindungan investor dan konsumen, serta stabilitas pasar keuangan.

ADAPTASI

Undang-Undang Pengawasan Perbankan

Kebutuhan akan adaptasi hukum dalam pengaturan mata uang virtual berdasarkan undang-undang pasar keuangan pada dasarnya muncul dari kenyataan bahwa digitalisasi unit nilai, baik dalam hal penerbitan dan transfernya antar individu, berbeda dalam beberapa hal, khususnya poin teknis. Bagi pelaku pasar, mata uang virtual merupakan fungsi yang setara dengan mata uang negara. Salah satu kesulitan dalam penerapan kehati-hatian adalah menilai sejauh mana aktivitas individu sesuai dengan fakta dan kategori undang-undang pengawasan perbankan.

Mata Uang Virtual Sebagai Kategori: Unit Akun Atau Nilai Kripto

Paradigma kesulitan dalam kategorisasi dalam hukum Jerman adalah klasifikasi unit individu mata uang virtual sebagai instrumen keuangan dalam pengertian pengawasan perbankan. Baik kualifikasi sebagai lembaga kredit maupun sebagai lembaga jasa keuangan saling terkait, dengan konsekuensi yang sesuai dengan persyaratan peraturan, dengan serangkaian kegiatan yang sebagian besar berhubungan langsung atau tidak langsung dengan instrumen keuangan.

Otoritas pengawas Jerman memahami konsep “unit akun” sebagai semacam konsep yang mencakup semua hal, yang juga mencakup mata uang buatan seperti hak penarikan khusus, atau mata uang yang diterbitkan di sektor swasta, terutama mata uang virtual. Dalam literatur penafsiran ini cukup kontroversial. Penafsiran ini juga telah ditolak dalam keputusan Pengadilan Tinggi Daerah (Kammergericht) Berlin sehubungan dengan penerapan ketentuan pidana yang terdapat dalam Undang-Undang Perbankan Jerman (KWG), yang cukup menarik perhatian di Jerman.

Penilaian ini, di satu sisi, didasarkan pada asumsi bahwa konsep “unit hitung” juga memerlukan stabilitas nilai tertentu dan pengakuan umum untuk menjamin keterbandingan. Di sisi lain, hukum konstitusional Jerman menuntut lebih banyak penafsiran dalam kasus tindak pidana. Kata-katanya merupakan batas varian penafsiran yang diperbolehkan. Analogi yang menetapkan pertanggungjawaban pidana dilarang. Karena otoritas pengawas Jerman tetap mempertahankan penafsiran hukumnya terhadap konsep satuan hitung, literatur telah menganalisis sejauh mana “penafsiran terpisah” ini dapat dibenarkan dengan perbedaan metodologis antara pengawasan dan pengawasan. hukum di satu sisi dan hukum pidana di sisi lain. Penelitian ini merupakan konsekuensi khas dari kebutuhan untuk mengkualifikasikan secara hukum fakta-fakta yang sebelumnya tidak diketahui yang melibatkan objek digital ke dalam kategori hukum yang ada. Kategorisasi memerlukan pemeriksaan premis metodologis dan hubungannya dengan elemen konteks individual.

Selain penyesuaian kategorisasi ini, legislator Jerman juga telah memperkenalkan kategori baru, “nilai kriptografi”, dan kategori baru yang terkait dengan “bisnis penyimpanan kripto” ke dalam katalog fakta pengawasan. Dengan diperkenalkannya kategori nilai kripto sebagai instrumen keuangan, otoritas pengawas kini memiliki sarana referensi yang independen terhadap kualifikasi sebagai “unit akuntansi”.

Penilaian Peraturan Kegiatan

Di luar klasifikasi unit virtual sebagai instrumen keuangan, ruang lingkup penerapan pengawasan perbankan mengandaikan bahwa aktivitas yang dimaksud memenuhi definisi bentuk transaksi perbankan atau jasa keuangan tertentu. Misalnya, penciptaan mata uang virtual, seperti penambangan Bitcoin, dan penggunaannya selanjutnya untuk tujuan perusahaan sendiri tidak dengan sendirinya merupakan pengambilalihan instrumen keuangan untuk ditempatkan atas risiko yang ditanggung perusahaan dan dengan demikian belum merupakan penerbitan. transaksi. Juga bukan merupakan jasa keuangan dalam bentuk penempatan instrumen keuangan tanpa komitmen penjaminan emisi yang kuat, yang disebut bisnis penempatan.

Terakhir, penggunaan unit virtual sebagai alat pertukaran atau pembayaran selanjutnya tidak bukan merupakan perantara transaksi perolehan atau penjualan instrumen keuangan (perantara investasi) atau perolehan atau penjualannya atas nama pihak ketiga (perantara akuisisi). Penciptaan unit virtual, meskipun unit itu sendiri akan diklasifikasikan sebagai instrumen keuangan, pada prinsipnya tidak diatur, karena aturan pengawasannya mengacu pada aktivitas lebih lanjut yang relevan dengan pasar keuangan. Namun, ada hal lain yang mungkin timbul dari struktur proses penciptaannya, misalnya, jika beberapa partisipan bergabung bersama dalam yang disebut kumpulan penambangan, bersama-sama menyediakan daya komputasi yang diperlukan untuk pembuatan suatu unit dan kerja sama tersebut melibatkan administrasi dana atau unit untuk pihak lain.

Yang terakhir, kesenjangan dalam kerangka kehati-hatian untuk mata uang digital mungkin timbul dari kenyataan bahwa aktivitas yang memerlukan regulasi berbeda antara mata uang digital dan konvensional dan bahwa perbedaan tersebut tidak dapat diatasi bahkan dengan interpretasi teleologis. Kesenjangan tersebut memerlukan amandemen atau penyesuaian terhadap kerangka hukum. Misalnya, bisnis penyimpanan kripto yang baru diperkenalkan mencakup aktivitas tertentu yang tidak memerlukan regulasi ketika berhadapan dengan mata uang konvensional, yaitu pengelolaan dan perlindungan aset kriptografi termasuk kunci kriptografi pribadi. Fakta-fakta dalam kasus ini merupakan tambahan khusus terhadap peraturan yang ada mengenai masalah digital.

Stablecoin sebagai E-Money?

Dalam undang-undang tentang layanan pembayaran, aspek kategorisasi serupa berkaitan dengan pertanyaan apakah stablecoin dapat diklasifikasikan sebagai uang elektronik. Peraturan nasional mengenai uang elektronik didasarkan pada Petunjuk Uni Eropa yang telah mendefinisikan pengertian uang elektronik. Peraturan tersebut mendefinisikan uang elektronik sebagai setiap nilai moneter yang disimpan secara elektronik dalam bentuk tagihan kepada penerbit yang diterbitkan dengan imbalan sejumlah uang

elektronik. uang dengan tujuan untuk melakukan transaksi pembayaran tertentu dan yang diterima oleh perorangan atau badan hukum selain penerbit uang elektronik. Sedangkan dalam kasus mata uang virtual yang secara eksklusif terdiri dari unit berbasis blockchain, tidak ada tuntutan terhadap penerbit dari permulaan; dalam kasus stablecoin, penautan unit virtual ke suatu sekuritas dapat menyebabkan klaim pembayaran oleh pemegang stablecoin jika pemegangnya meminta pertukaran ke dalam mata uang negara. Apakah klaim tersebut ada, tentu saja, merupakan pertanyaan mengenai pengaturan kontrak.

Terlebih lagi, masih menjadi pertanyaan apakah cukup jika klaim pembayaran tidak ditujukan kepada badan hukum yang menerbitkan mata uang virtual, namun terhadap orang lain, biasanya pengecer resmi. Yang terpenting, konsep uang elektronik adalah dirancang untuk mewakili nilai mata uang negara secara digital. Oleh karena itu, uang elektronik harus memiliki nilai nominal dan dapat ditukar kapan saja dengan nilai nominal tersebut. Tidak ada nilai nominal untuk stablecoin, yang syarat penukarannya bergantung pada perkembangan pasar. Nilai pasarnya didasarkan pada penawaran dan permintaan stablecoin di satu sisi dan perkembangan pasar dari agunan yang mendasarinya di sisi lain. Oleh karena itu, alasan yang lebih baik menunjukkan bahwa stablecoin tidak termasuk dalam kategori uang elektronik, setidaknya secara de lege lata. Namun demikian, klasifikasi stablecoin sebagai uang elektronik masih kontroversial. Perbedaan dalam kategorisasi ini menggambarkan kesulitan dan kesulitan yang dihadapi. kelonggaran dalam mengkonkretkan konsep hukum seperti uang elektronik dan dampaknya terhadap kualifikasi mata uang digital.

Komisi Eropa memandang ketidakpastian hukum dan keterbatasan ruang lingkup peraturan mengenai uang elektronik sebagai kesenjangan dalam perlindungan pengguna. Intinya, adanya klaim oleh pemegang unit virtual untuk pembayaran dalam mata uang nominal merupakan prasyarat konseptual bagi keberadaan e-money berdasarkan aturan yang berlaku saat ini. Unit virtual, yang disebut stablecoin dijamin dengan mata uang nominal, namun klaim pembayarannya tidak diberikan sama sekali atau hanya sampai batas tertentu, oleh karena itu tidak termasuk dalam definisi stablecoin. Namun, pembatasan ini justru menimbulkan risiko bagi pengguna.

Oleh karena itu, usulan Komisi mengenai Peraturan Pasar dalam Aset Kripto mengatur pengenalan kategori baru “token uang elektronik”, yang secara umum menetapkan nilai kripto berdasarkan mata uang negara sesuai dengan persyaratan peraturan. Menurut usulan tersebut, e -Token uang harus didefinisikan sebagai jenis aset kripto, yang tujuan utamanya adalah untuk digunakan sebagai alat pertukaran dan dimaksudkan untuk mempertahankan nilai yang stabil dengan mengacu pada nilai mata uang fiat yang merupakan alat pembayaran yang sah.

Berdasarkan peraturan baru yang diusulkan, baik penawaran umum token uang elektronik maupun perdagangannya pada platform perdagangan kriptografi di Uni Eropa pada prinsipnya memerlukan izin, termasuk izin sebelumnya sebagai bank atau lembaga uang elektronik. Selain itu, penawaran umum token uang elektronik dan izin perdagangan di masa depan akan memerlukan publikasi kertas putih aset kripto terlebih dahulu oleh penerbit, termasuk penjelasan rinci tentang aktor yang terlibat, hak dan kewajiban yang

terkait dengan token e-money dan risikonya. Terakhir, pemegang token e-money di masa depan akan memiliki klaim wajib terhadap penerbit berdasarkan nilai nominal token.

Hukum Perdata

Karakter virtual mata uang digital juga menyebabkan kesulitan besar dalam kategorisasi dalam hukum perdata. Karena mata uang virtual, tidak seperti uang tunai, bukanlah objek fisik, maka disepakati secara bulat bahwa mata uang tersebut bukan merupakan objek dalam pengertian hukum perdata Jerman. Selain itu, berbeda dengan uang alkitabiah, misalnya, kepemilikan unit individu mata uang virtual pada prinsipnya tidak terkait dengan klaim individu mana pun. Terakhir, unit individual mata uang virtual dapat dikualifikasikan sebagai bentuk hak kekayaan intelektual. Namun, dalam kasus hak cipta sebagai hak kekayaan intelektual yang paling layak, penciptaan suatu unit, seperti penambangan Bitcoin, tidak memerlukan upaya kreatif pribadi yang diperlukan oleh seseorang. Unit mata uang virtual bukanlah suatu benda atau klaim, meskipun secara de facto uang tersebut digunakan secara fungsional setara dengan uang tunai atau uang kitab suci. Mereka hanya dapat diklasifikasikan sebagai objek lain dalam sistem hukum perdata Jerman. Perbedaan hukum dalam kategorisasi ini mempunyai konsekuensi baik dalam pengalihan maupun integrasi ke dalam kewajiban kontrak dan hukum.

Jika tidak ada objek fisik, maka kepemilikan mata uang virtual tidak dapat dialihkan sesuai dengan aturan mengenai pengalihan harta bergerak. Demikian pula, aturan mengenai pengalihan hak tagih tidak secara langsung mencakup pengalihan posisi aktual semata. Oleh karena itu, pandangan utama dalam literatur mengasumsikan transfer unit mata uang virtual sesuai dengan aturan untuk item lainnya. Ketika menerapkan aturan mengenai kewajiban kontraktual, satuan mata uang virtual tidak dapat dipahami sebagai “uang” dalam pengertian hukum perdata karena unit tersebut tidak diakui secara resmi. Akibatnya, kontrak seperti, khususnya, kontrak penjualan yang melibatkan pembayaran imbalan uang tidak dapat langsung diterapkan pada situasi di mana mata uang virtual akan digunakan sebagai pertimbangan. Namun demikian, situasi seperti ini secara umum dapat direpresentasikan sebagai kontrak pertukaran dengan implikasinya masing-masing, misalnya, terhadap undang-undang jaminan.

Yang lebih sulit untuk dilakukan adalah perlindungan hukum unit virtual terhadap orang-orang yang bukan merupakan mitra kontrak. Klausul umum undang-undang tort dalam undang-undang tort Jerman mengandaikan bahwa kepemilikan objek fisik atau hak lainnya terpengaruh. Sebagai akibat dari pembatasan ini, kasus hukum dalam sejumlah contoh mengenai masalah digital mengacu pada media penyimpanan data yang sesuai. Tuntutan pelanggaran kepemilikan media penyimpanan data fisik juga mencakup kerusakan yang terjadi terhadap data yang tersimpan di dalamnya. Namun, konstruksi dogmatis ini tidak berlaku untuk mata uang virtual, yang tidak dapat dikaitkan dengan perangkat keras fisik tertentu. Kerusakan pada unit mata uang virtual biasanya tidak dapat dipahami sebagai kerusakan tidak langsung akibat pelanggaran properti fisik. Atribusi unit virtual sebagai hak lain dalam pengertian klausul umum Jerman tentang hukum gugatan juga mengandaikan adanya atribusi hukum yang sebanding atas unit digital kepada pemiliknya, yang tidak ada

atau setidaknya diragukan karena tidak adanya peraturan hukum. Kesenjangan serupa pada dasarnya muncul dalam dasar-dasar tuntutan kewajiban hukum lebih lanjut, khususnya dalam hukum pengayaan yang tidak adil.

Pada umumnya, hukum perdata mata uang digital, seperti Bitcoin atau mata uang kripto lainnya, melibatkan prinsip-prinsip hukum perdata yang berlaku pada transaksi keuangan dan pertukaran harta. Namun, perlu diingat bahwa ketentuan hukum terkait mata uang digital dapat bervariasi dari satu yurisdiksi ke yurisdiksi lainnya.

Berikut adalah beberapa prinsip hukum perdata yang mungkin relevan dalam konteks mata uang digital:

1. **Kontrak:** Transaksi yang melibatkan mata uang digital seringkali didasarkan pada kontrak antara pihak-pihak yang terlibat. Hukum kontrak mengatur pembentukan, pelaksanaan, dan pelanggaran kontrak. Kontrak yang menggunakan mata uang digital harus mematuhi prinsip-prinsip umum hukum kontrak.
2. **Pemilikan dan Transfer Harta:** Prinsip hukum perdata yang mengatur pemilikan dan transfer harta benda juga berlaku untuk mata uang digital. Transaksi transfer mata uang digital harus mematuhi prinsip-prinsip pemilikan dan transfer properti.
3. **Ketidaksahteraan atau Kekurangan Kesepakatan:** Seperti dalam transaksi keuangan lainnya, prinsip ketidaksahteraan atau kekurangan kesepakatan dapat digunakan untuk membatalkan kontrak jika ada kelalaian atau ketidaksetujuan antara pihak-pihak yang terlibat.
4. **Perlindungan Konsumen:** Prinsip-prinsip perlindungan konsumen juga dapat menjadi relevan, terutama jika mata uang digital digunakan dalam transaksi konsumen. Pihak yang menyediakan layanan pembayaran atau pertukaran mata uang digital mungkin harus mematuhi peraturan perlindungan konsumen yang berlaku.
5. **Pajak:** Pajak pada transaksi mata uang digital juga menjadi bagian penting dari hukum perdata. Pemerintah biasanya mengatur tata cara perpajakan untuk transaksi menggunakan mata uang digital.
6. **Perlindungan Privasi dan Keamanan Data:** Hukum perdata yang berkaitan dengan privasi dan keamanan data juga dapat menjadi relevan, terutama mengingat sifat teknis mata uang digital dan penggunaan teknologi blockchain.
7. **Kepatuhan Regulasi:** Mata uang digital sering kali terpengaruh oleh regulasi keuangan dan perbankan yang berlaku. Pihak yang terlibat dalam ekosistem mata uang digital harus mematuhi regulasi yang berlaku di yurisdiksi mereka.

Sangat penting untuk diingat bahwa hukum perdata mata uang digital sedang mengalami perkembangan seiring dengan berkembangnya teknologi dan meningkatnya penerimaan mata uang digital oleh masyarakat dan pemerintah. Oleh karena itu, untuk memahami dengan akurat konsekuensi hukumnya, penting untuk berkonsultasi dengan ahli hukum yang memiliki pemahaman mendalam tentang hukum perdata dan regulasi keuangan di wilayah tertentu.

Sebagai hasil sementara dari perlindungan hukum perdata atas mata uang virtual, dapat dikatakan bahwa hukum kontrak cukup fleksibel dalam menangani unit virtual yang tidak dapat diklasifikasikan dalam kategori alat pembayaran fisik dan digital yang lazim. Namun, kerangka hukum perdata mata uang virtual memiliki kesenjangan dalam kaitannya dengan pihak ketiga yang tidak memiliki hubungan kontrak, dan khususnya dalam

perlindungan terhadap akses atau manipulasi yang tidak sah. Dengan mata uang virtual seperti Bitcoin, kesenjangan ini dapat dipahami sebagai melekat dalam konsep tersebut. Entitas virtual, yang memandang dirinya independen dari sistem hukum tertentu, memberikan perlindungan terhadap akses tidak sah sesuai dengan pemahamannya sendiri melalui desain algoritme, terutama melalui mekanisme validasi transaksi di blockchain. Namun, jika, di satu sisi, mata uang virtual harus diintegrasikan ke dalam instrumen yang ada seperti undang-undang perlindungan konsumen atau undang-undang sekuritas dan, di sisi lain, harus dikaitkan dengan jaminan lain seperti stablecoin, pengakuan hukum perdata yang lebih luas atas unit virtual akan bermanfaat. Pengakuan sipil tersebut dapat berupa pengenalan kategori properti terpisah untuk mata uang virtual dan memperlakukannya sebagai objek fisik. Solusi seperti itu dalam banyak kasus akan memperlakukan mata uang virtual seperti uang tunai. Namun, dalam beberapa kasus, seperti transfer, peraturan secara eksplisit menghubungkannya dengan kepemilikan benda fisik. Solusi lain adalah dengan membuat transfer dan hak atas mata uang virtual tergantung pada pendaftaran di register.

Hukum Sekuritas

Hukum pidana mata uang digital berkaitan dengan aspek-aspek kriminal yang terkait dengan penggunaan, perdagangan, atau aktivitas lain yang melibatkan mata uang digital, seperti Bitcoin atau mata uang kripto lainnya. Berikut adalah beberapa aspek hukum pidana yang mungkin terkait dengan mata uang digital:

1. **Pencucian Uang (Money Laundering):** Penggunaan mata uang digital untuk mencuci uang adalah perhatian utama dalam hukum pidana. Pemerintah di berbagai negara memiliki undang-undang yang mengatur pencegahan dan penindakan pencucian uang, dan penggunaan mata uang digital dapat menjadi subjek pengawasan ketat.
2. **Pencurian dan Kecurangan (Theft and Fraud):** Transaksi dengan mata uang digital dapat menjadi sasaran pencurian atau kecurangan. Tindakan ini dapat mencakup akses tanpa izin ke dompet digital atau pertukaran mata uang kripto.
3. **Pemerasan dengan Tebusan (Ransomware):** Pemerasan dengan tebusan yang melibatkan pembayaran menggunakan mata uang digital telah menjadi masalah serius. Penjahat sering menggunakan kriptografi untuk menyandera data atau sistem dan kemudian meminta tebusan dalam bentuk mata uang digital.
4. **Penghindaran Pajak:** Beberapa orang mungkin mencoba menggunakan mata uang digital untuk menghindari pembayaran pajak atau menyembunyikan pendapatan yang diperoleh secara ilegal. Oleh karena itu, ada ketentuan hukum pidana yang mengatur penghindaran pajak menggunakan mata uang digital.
5. **Keamanan Siber (Cybersecurity):** Serangan siber terhadap platform perdagangan atau dompet digital dapat melibatkan pelanggaran hukum pidana, terutama jika data pribadi atau keuangan pengguna diakses atau disalahgunakan.
6. **Penggelapan Aset (Asset Misappropriation):** Penggunaan mata uang digital untuk menggelapkan aset atau mengubah kepemilikan secara ilegal dapat melibatkan tindakan pidana.
7. **Penyalahgunaan Pasar (Market Manipulation):** Praktik penipuan atau manipulasi pasar, seperti "pump and dump" di pasar kripto, dapat menimbulkan tindakan pidana.

8. **Kejahatan Siber Terorganisir:** Kejahatan siber yang melibatkan mata uang digital kadang-kadang dilakukan oleh kelompok terorganisir. Ini dapat mencakup pencurian besar-besaran atau serangan terhadap infrastruktur kripto.

Penting untuk dicatat bahwa regulasi dan ketentuan hukum pidana terkait mata uang digital dapat berbeda di setiap yurisdiksi. Beberapa negara telah mengembangkan undang-undang khusus untuk mengatasi aspek-aspek pidana mata uang digital, sedangkan yang lain masih dalam proses mengembangkan regulasi yang lebih rinci. Jika Anda terlibat dalam aktivitas dengan mata uang digital, sangat penting untuk memahami hukum pidana yang berlaku di wilayah hukum Anda dan mendapatkan nasihat hukum jika diperlukan.

Dalam kasus obligasi, misalnya, legislator Jerman baru-baru ini memperkenalkan daftar sekuritas di mana pendaftaran menggantikan persyaratan yang ada untuk sertifikat sekuritas, sekaligus memastikan perlindungan kepemilikan dan kepastian hukum dalam transaksi hukum. Selain daftar pusat sekuritas elektronik, kategori “daftar aset kripto” harus ditetapkan sebagai daftar sekuritas elektronik untuk aset kripto, di mana data terkait transaksi disimpan secara desentralisasi, kronologis, dan anti-rusak. Administrator pencatatan ditunjuk oleh penerbit aset kripto dan oleh karena itu, berbeda dengan pencatatan pusat untuk sekuritas elektronik, dapat dipilih dari berbagai pihak swasta. Peraturan hukum memberlakukan persyaratan tertentu, khususnya pada pengoperasian register termasuk tanggung jawab, isi register termasuk konsultasi, pengawasan dan publikasi terbitannya. Setelah pendaftaran dalam register, undang-undang menetapkan aturan terpisah untuk pelepasan efek elektronik, termasuk aturan transfer dan akuisisi dengan itikad baik.

9.4 TANTANGAN KHUSUS DIGITALITAS

Selain permasalahan pengklasifikasian fakta digital ke dalam kategori hukum, karakteristik mata uang digital menimbulkan tantangan yang signifikan terkait pengawasan. Undang-undang pengawasan perbankan terkadang bereaksi dengan rezim khusus terhadap mata uang virtual.

Pencegahan Pencucian Uang dan Pendanaan Terorisme

Rezim khusus ini pertama-tama menyangkut pencegahan pencucian uang dan pendanaan teroris. Mata uang virtual yang dikeluarkan secara pribadi sangat rentan terhadap penyalahgunaan, terutama jika mata uang tersebut dapat dioperasikan di seluruh dunia, terlepas dari pengakuan pemerintah, dan memungkinkan transaksi anonim. Namun demikian, karakteristik teknis mata uang virtual juga menawarkan peluang untuk memerangi aktivitas pencucian uang yang tidak ada dalam bentuk uang tunai atau uang kitab suci. Misalnya, asal usul dan perkembangan dana yang disita dapat dilacak secara permanen melalui blockchain, meskipun pelaku di balik alamat individu mungkin tidak diketahui. Oleh karena itu, profil risiko spesifik serta langkah-langkah yang diperlukan oleh otoritas pengawas sangat bergantung pada karakteristik teknis mata uang virtual yang bersangkutan. Aplikasi seperti mixer atau thumbler, yang, dengan mencampurkan alur transaksi, dimaksudkan untuk mengecualikan atau menghalangi keterlacakan pada blockchain, meningkatkan tingkat kecurigaan dan dengan demikian memerlukan tindakan anti pencucian

uang yang spesifik. Pada saat yang sama, perlawanan terhadap pencucian uang dan pendanaan terorisme menyoroti dimensi hukum pengawasan internasional.

Tanpa koordinasi langkah-langkah dan standar lintas batas, kemampuan masing-masing negara untuk menilai dan membendung risiko tanpa terlalu mengganggu aliran keuangan legal menjadi terbatas. Oleh karena itu, Satuan Tugas Aksi Keuangan (Financial Action Task Force), sebuah badan antar pemerintah, terus-menerus memantau aktivitas global pencucian uang dan pendanaan teroris, termasuk aspek ekonomi dan teknisnya, dan mengembangkan indikator dan rekomendasi berdasarkan hal ini, khususnya untuk mata uang virtual. termasuk stablecoin.

Perlindungan Investor dan Konsumen dalam Penerbitan Mata Uang Virtual

Di masa lalu, penerbitan unit virtual oleh masing-masing pelaku dalam beberapa kasus telah menyebabkan kerugian besar bagi investor. Hal yang disebut Initial Coin Offerings (Penawaran Koin Perdana) ini memberi perusahaan penerbit fungsi setara untuk bentuk peningkatan modal yang diatur dan jauh lebih ketat. sehingga menjamin tingkat perlindungan investor dan konsumen yang lebih tinggi. Perbedaan dalam tingkat peraturan juga disebabkan oleh fakta bahwa, meskipun unit virtual mungkin memiliki arti yang sama dengan saham, tergantung pada desain tokennya, unit virtual tersebut mungkin tidak termasuk dalam kategori undang-undang sekuritas. Usulan Komisi untuk Oleh karena itu, Peraturan tentang Pasar Aset Kripto memberikan persyaratan yang lebih rinci untuk penerbitan aset kripto. Secara khusus, penerbit aset kriptografi diharuskan menyiapkan buku putih aset kripto dengan penjelasan rinci tentang proyek, struktur hukum dan risikonya dan memberitahukan buku putih ini kepada pihak yang berwenang. Baik penerbit maupun badan pengelolanya di masa depan harus bertanggung jawab atas kerugian yang disebabkan oleh informasi yang tidak lengkap atau menyesatkan dalam buku putih tersebut.

Persyaratan Peraturan Khusus untuk "Token yang Direferensikan Nilai"

Proposal Peraturan Pasar dalam Aset Kripto juga menyediakan kategori baru "token yang direferensikan nilai". Ini adalah token kripto yang dihubungkan dengan keamanan untuk meningkatkan stabilitas nilai. Keamanan ini dapat terdiri dari mata uang negara, barang, nilai kriptografi lainnya atau kombinasi keduanya. Aturan baru yang akan diperkenalkan untuk token yang direferensikan nilai di satu sisi tidak hanya berfungsi sebagai perlindungan konsumen dan investor, tetapi juga stabilitas pasar. pasar keuangan. Penerbit token yang direferensikan nilai memerlukan izin untuk melakukan penawaran umum token atau izin untuk berdagang di platform perdagangan, yang juga memerlukan, antara lain, penerbitan buku putih nilai aset kripto. Buku putih aset kripto akan berisi, antara lain, penjelasan rinci tentang cadangan aset, pengaturan penyimpanan, modalitas investasi aset cadangan dan posisi hukum pemegang token. Seperti halnya buku putih untuk aset kripto, keduanya penerbit dan badan pengelolanya bertanggung jawab atas kerugian akibat informasi yang tidak lengkap, tidak benar, atau menyesatkan dalam buku putih. Selain itu, penerbit juga wajib berkomunikasi secara adil, jelas, dan tidak menyesatkan, termasuk dalam komunikasi pemasaran.

Selain persyaratan perlindungan investor ini, persyaratan lebih lanjut bagi penerbit token yang direferensikan nilai mendekati situasi peraturan lembaga kredit. Persyaratan ini mencakup persyaratan yang berkaitan dengan struktur perusahaan internal, strategi dan pengalaman kepatuhan internal, dan keandalan. anggota badan pengelola, tetapi juga persyaratan yang berkaitan dengan modal ekuitas. Usulan Peraturan Pasar Aset Kripto juga memberikan aturan rinci tentang penyimpanan dan pengelolaan aset cadangan, termasuk akses penerbit ke aset cadangan untuk memenuhi permintaan penebusan. Terakhir, opsi penebusan bagi pemegang token akan dipastikan dengan mewajibkan penerbit untuk memberikan hak penebusan yang jelas dan dapat dilaksanakan terhadap penerbit atau sehubungan dengan aset cadangan, atau untuk memastikan bahwa jumlah yang cukup penyedia pihak ketiga menawarkan penebusan pada kondisi pasar.

Kewajiban khusus juga dipertimbangkan untuk apa yang disebut token dengan referensi nilai signifikan, yang dimaksudkan untuk lebih meningkatkan perlindungan terhadap non-pembayaran mengingat efek jaringan khusus dari ekosistem digital dan juga untuk memastikan penebusan selama operasi. Klasifikasi token yang direferensikan nilai sebagai signifikan didasarkan pada enam faktor. Mirip dengan lembaga kredit, faktor-faktornya terkait dengan volume dan saling ketergantungan dengan sistem keuangan. Namun, karena adanya pengalihan efek jaringan dari ekosistem digital, ukuran basis pelanggan perusahaan di balik token yang direferensikan nilai menjadi lebih kecil. juga diperhitungkan. Sebagai konsekuensinya, bagi penerbit token dengan referensi nilai yang signifikan, persyaratan yang dipertimbangkan adalah kebijakan remunerasi yang ramah risiko, memastikan kemungkinan penebusan melalui penyedia pihak ketiga, memantau manajemen likuiditas dan tingkat modal ekuitas.

Kesimpulan

Perlakuan hati-hati terhadap mata uang digital sebagian besar ditandai dengan klasifikasi dan adaptasi masalah digital ke dalam kategori yang sudah ada. Namun, mata uang digital memiliki karakteristik teknis dan ekonomi yang membedakannya secara struktural dari mata uang negara, terutama dalam kaitannya dengan peredaran lintas batas negara. Perbedaan-perbedaan ini tetap ada meskipun mata uang negara didigitalkan dalam bentuk uang kitab suci. Karakteristik ini memunculkan kebutuhan kehati-hatian yang spesifik, khususnya untuk perlindungan investor dan konsumen serta pencegahan pencucian uang dan pendanaan teroris. Stablecoin juga, jika mencapai volume tertentu, dapat mempengaruhi stabilitas pasar keuangan atau efektivitas langkah-langkah kebijakan moneter oleh bank sentral. Proposal untuk mengatur aset kripto, termasuk mata uang virtual, bertujuan untuk mengizinkan penerbitan dan perdagangan aset kripto di Uni Eropa hanya dalam kondisi tertentu. Kategori-kategori yang baru diperkenalkan untuk berbagai bentuk aset kripto membawa mata uang virtual lebih dekat ke rezim regulasi kehati-hatian yang sudah ada. Dalam melakukan hal ini, mereka mengadopsi peraturan tertentu yang mempertimbangkan karakteristik spesifik mata uang digital.

BAB 10
HUKUM PIDANA DIGITALITAS GLOBAL

Seiring dengan pertumbuhan aktivitas digital dalam beberapa dekade terakhir, perilaku berbahaya semakin meningkat di ruang siber yang mengancam perdagangan, bisnis, komunikasi swasta, dan lembaga publik. Pemerintah segera menyadari bahwa fenomena global ini tidak dapat diatasi dengan undang-undang dalam negeri. sendirian dan beralih ke organisasi internasional untuk melindungi masyarakat dari ancaman di ruang siber. Pada tahun 1990-an, Dewan Eropa menjadi salah satu lembaga multilateral pertama dan terkemuka yang menanggapi masalah yang berkembang ini dengan seruan untuk mengkriminalisasi aktivitas digital tertentu yang berbahaya. Hal ini berujung pada diadopsinya Konvensi Dewan Eropa tentang Kejahatan Dunia Maya pada tahun 2001. Sejak tahun 1990an, PBB juga telah menangani kejahatan dunia maya dengan beberapa langkah kebijakan yang berfokus terutama pada peningkatan kapasitas dan berbagi pengetahuan teknis di antara negara-negara berkembang di bidang penuntutan pidana.

Kontribusi ini merupakan kritik terhadap peraturan hukum pidana digitalitas global saat ini. Pertama, mendefinisikan hukum pidana digitalitas global sebagai “kejahatan dunia maya” dan mengkaji sejarah serta kelemahan istilah “kejahatan dunia maya”. Berikut ini adalah analisis mengenai tantangan global tertentu yang timbul dari kejahatan dunia maya. Pada dua bagian berikutnya, analisis ini membedakan antara pendekatan legislatif dan kebijakan terhadap kejahatan dunia maya, sebelum mengkaji peraturan dan kebijakan spesifik yang diterapkan dalam beberapa dekade terakhir. Diakhiri dengan pembahasan mengenai karakteristik hukum pidana digitalitas global dan kelemahan hukum kejahatan dunia maya saat ini.

Berikut ini saya berpendapat bahwa kebebasan individu terancam oleh larangan kejahatan dunia maya (hukum pidana substantif). Perkembangan teknis dan peraturan kejahatan dunia maya juga meningkatkan kemungkinan pengawasan terhadap otoritas penegak hukum mulai dari pelacakan satelit hingga penambangan data. Selain itu, penghormatan terhadap hak prosedural tersangka, hak privasi dan nilai-nilai supremasi hukum memainkan peran kecil dalam undang-undang kejahatan dunia maya (hukum pidana prosedural). Selain itu, dimensi global kejahatan dunia maya memicu konflik yurisdiksi yang harus diatasi, misalnya, ketika menentukan di mana kejahatan tersebut dilakukan. Namun, tantangan-tantangan ini menimbulkan permasalahan prinsip yang berbeda yang banyak diperdebatkan di kalangan kritikus hukum kejahatan dunia maya.

10.1 MENDEFINISIKAN HUKUM PIDANA DIGITALITAS GLOBAL

Hukum Pidana Digitalitas Global mengacu pada kerangka hukum yang mengatur tindak pidana yang melibatkan penggunaan teknologi informasi dan komunikasi (TIK) di tingkat global. Perkembangan teknologi digital telah membawa tantangan baru dalam ranah

hukum pidana, dan hukum pidana digitalitas global dirancang untuk mengatasi kejahatan yang terjadi secara lintas batas di dunia maya.

Berikut adalah beberapa elemen yang mencirikan Hukum Pidana Digitalitas Global:

1. **Kejahatan Siber Global:** Hukum pidana digitalitas global mencakup berbagai jenis kejahatan siber yang terjadi di dunia maya, termasuk serangan siber, pencurian data, pencucian uang digital, ransomware, dan kejahatan siber lainnya yang dapat menyebar secara internasional.
2. **Kerjasama Internasional:** Karena kejahatan digital sering kali tidak terbatas oleh batas-batas negara, hukum pidana digitalitas global membutuhkan kerjasama internasional yang erat. Inisiatif dan lembaga seperti Europol, Interpol, dan berbagai perjanjian bilateral atau multilateral diperlukan untuk memerangi kejahatan siber secara efektif.
3. **Perlindungan Data Internasional:** Pengaturan dan perlindungan data yang berlaku di tingkat global sangat penting dalam konteks hukum pidana digital. Peraturan ini bertujuan untuk melindungi privasi individu dan mencegah penyalahgunaan data pribadi di dunia maya.
4. **Hukuman untuk Kejahatan Digital:** Hukum pidana digitalitas global mencakup sanksi dan hukuman untuk pelaku kejahatan digital. Ini dapat mencakup denda, hukuman penjara, atau sanksi lainnya sesuai dengan tingkat seriusnya kejahatan.
5. **Keamanan Siber dan Pertahanan:** Aspek hukum pidana digitalitas global juga mencakup langkah-langkah untuk meningkatkan keamanan siber dan pertahanan negara-negara terhadap ancaman keamanan siber.
6. **Ketentuan Pengadilan Digital:** Pengadilan digital atau mekanisme alternatif untuk menyelesaikan sengketa digital mungkin termasuk dalam kerangka hukum ini, memungkinkan penyelesaian sengketa secara efisien dan adil di dunia maya.
7. **Perjanjian dan Konvensi Internasional:** Adanya perjanjian dan konvensi internasional yang diadopsi untuk menanggapi tantangan kejahatan siber. Contohnya adalah Konvensi Budapest tentang Kejahatan Siber, yang merupakan perjanjian pertama yang mengatasi kejahatan siber secara umum.

Hukum pidana digitalitas global terus berkembang sejalan dengan perkembangan teknologi dan jenis kejahatan baru yang muncul. Pemerintah, lembaga internasional, dan sektor swasta harus terlibat dalam upaya bersama untuk mengatasi tantangan ini secara efektif dan melindungi masyarakat global dari ancaman keamanan siber.

Dari Kejahatan Komputer ke Kejahatan Dunia Maya

Saat ini “kejahatan dunia maya” adalah istilah akademis dan legislatif yang umum digunakan dalam membahas pengaturan aktivitas digital melalui hukum pidana. Namun, terdapat kesulitan dalam mendefinisikan istilah tersebut karena sejarahnya, ruang lingkup “ruang siber”, sifat aktivitas digital yang bersifat lintas batas, dan kurangnya penelitian yang didorong oleh teori.

Para ahli berbeda pendapat dalam menentukan nama peraturan pidana aktivitas digital, sehingga banyak usulan alternatif yang beredar untuk “kejahatan dunia maya” istilah yang baru muncul. Sebelumnya, istilah *“kejahatan komputer”* telah digunakan secara luas. Donn B. Parker mungkin pertama kali mendefinisikannya pada tahun 1976 sebagai kejahatan di mana komputer adalah (1) objek kejahatan, (2) lingkungan tempat kejahatan terjadi, (3)

instrumen untuk melakukan kejahatan, atau (4) simbol kejahatan (misalnya berpura-pura menggunakan program komputer untuk memungkinkan terjadinya kejahatan). Meskipun kejahatan dunia maya kini sedang marak, definisi terkini masih sangat bergantung pada kriteria Parker untuk isinya. Sebagian besar definisi kontemporer berpendapat bahwa kejahatan dunia maya mencakup penggunaan perangkat digital seperti komputer sebagai bagian integral dalam melakukan kejahatan atau menjadikan sistem komputer sebagai objek kejahatan.

Kejahatan komputer dan istilah serupa tidak lagi digunakan karena keterbatasannya dalam menjelaskan semakin banyaknya jenis peraturan pidana aktivitas digital. Kejahatan komputer tidak mencakup berbagai aktivitas yang menggunakan perangkat digital baru seperti ponsel pintar dan bukan komputer. Istilah *"kejahatan digital"* dan *"kejahatan teknologi informasi dan komunikasi"* lebih tepat. Namun, mereka berpendapat bahwa melakukan kejahatan memerlukan keterampilan digital atau teknologi dari pihak pelaku. Menyebutnya sebagai *"kejahatan internet"* mengabaikan pelanggaran yang hanya mengandalkan komputer atau sekadar memanipulasi sistem komputer tanpa menggunakan internet. Istilah kejahatan teknologi dan kejahatan teknologi informasi dan komunikasi menunjukkan bahwa fenomena ini terbatas pada bidang teknologi. Namun, banyak juga pelanggaran siber yang terjadi di dunia analog (misalnya penipuan, pencemaran nama baik). Kata kejahatan virtual diusulkan untuk hanya merujuk pada kejahatan yang dilakukan dalam latar video game, dan oleh karena itu hanya mencakup sebagian kecil dari spektrum pelanggaran dunia maya.

Istilah kejahatan dunia maya juga dapat dikritik karena beberapa alasan, namun akan digunakan dalam bab ini karena prevalensinya. Namun demikian, titik buta dan ketergantungan jalurnya memerlukan kajian kritis. Istilah ini dapat dikatakan gagal karena evolusi non-akademiknya, ketidakjelasannya, sifat perilaku digital yang bersifat lintas batas, dan dominasi penelitian praktis. Istilah kejahatan dunia maya tidak berasal dari dunia akademis. Seperti yang ditunjukkan oleh teori dekonstruksi postmodern, definisi dan narasi sangat mempengaruhi cara suatu fenomena dianalisis. Dalam bidang akademis, awalnya istilah "sibernetika" digunakan untuk merujuk pada studi tentang mesin dan sistem umpan balik. Peneliti AS mungkin sudah tidak lagi menggunakan istilah tersebut ketika para ilmuwan Soviet juga mulai menyebut teknologi informasi baru sebagai *"sibernetika"*.

Ruang Siber pertama kali digunakan oleh novelis dan penulis esai fiksi ilmiah William Gibson pada tahun 1982, yang mendapatkan ketenaran utamanya sebagai pencipta dari subgenre literatur cyberpunk yang berhubungan dengan dampak perkembangan teknologi terhadap manusia. Sejak tahun 1990-an, tren yang ada adalah apa yang disebut *"cyberhype"*, seperti yang dikatakan McKenzie Wark, yang mengacu pada kemungkinan-kemungkinan baru yang berasal dari penyebaran informasi teknologi dengan menambahkan awalan *"cyber"* yang memiliki konotasi positif (cyberspace, cybershopping, cybersex, cybersurfing).

Selama dua dekade terakhir, kata tersebut tidak lagi digunakan untuk penerapan teknologi baru; sebaliknya, istilah ini sekarang merujuk pada perilaku berbahaya atau terlarang (pelecehan dunia maya, rasisme dunia maya, terorisme dunia maya, perang dunia

maya, dll.). Namun, istilah *"siber"* tidak menjelaskan fenomena yang terkait dengannya; hal ini justru menyiratkan bahwa ada tantangan teknis khusus yang memerlukan solusi teknis. Tantangan-tantangan ini tidak diperlakukan sebagai konflik sosial dan permasalahan yang lazim terjadi di dunia "offline" jauh sebelum tantangan tersebut menjadi tantangan "online" (pelecehan, rasisme, terorisme, perang, dll.). Fokus pada teknologi baru menciptakan peluang kriminal baru mengaburkan kepentingan ekonomi dan negara yang mungkin memotivasi seruan untuk mengkriminalisasi aktivitas, seperti seruan untuk menghukum pembajakan digital untuk melindungi konten berhak cipta.

"Ruang siber", sebagai tempat terjadinya kejahatan dunia maya, akhir-akhir ini telah memperluas batasannya secara radikal. Bisa dibilang, dunia maya bukanlah "ruang" yang dapat didefinisikan secara ilmiah, melainkan sebuah deskripsi fiksi (William Gibson) dari dunia digital. Saat ini komputer dan perangkat lain yang terhubung ke internet ada di mana-mana, sehingga sulit untuk membedakan antara perilaku di "dunia maya" di satu sisi dan di dunia "offline" di sisi lain. Pelanggar kemungkinan besar akan menggunakan teknologi informasi meskipun hanya berupa telepon genggam atau mobil yang dilengkapi sistem navigasi. Seperti yang dinyatakan oleh David Wall: "Yang paling membingungkan adalah kecenderungan untuk menganggap hampir semua pelanggaran yang melibatkan komputer sebagai kejahatan dunia maya". Teknologi baru seperti Internet of Things berkontribusi pada sifat samar-samar dari ranah "ruang siber". Oleh karena itu, sejak awal diskusi, banyak komentator telah mengkategorikan kejahatan dunia maya hanya sebagai kejahatan biasa yang dilakukan dengan menggunakan atau menargetkan sistem komputer.

Sifat kejahatan dunia maya yang bersifat lintas batas mempersulit pencarian definisi. Kejahatan sering kali didefinisikan berdasarkan konsep budaya tentang konflik dan kerugian sosial. Misalnya, apa yang dianggap sebagai prostitusi terlarang mungkin berbeda antar budaya. Jika terdapat dimensi lintas batas, tindakan tersebut mungkin hanya dianggap merugikan dari sudut pandang salah satu negara yang terlibat. Definisi "kejahatan dunia maya" juga dapat dibentuk oleh persyaratan hukum yang berbeda dari satu negara ke negara lain. Terutama ketika menyangkut pelanggaran konten, batasan konstitusional dalam mengkriminalisasi jenis ujaran tertentu sangat berbeda. Misalnya, KUHP Jerman melarang penolakan Holocaust, sedangkan di AS hal ini dilindungi oleh hak konstitusional atas kebebasan berpendapat.

Sejumlah buku dan artikel akademis tentang "kejahatan dunia maya" berfokus pada aspek teknis dan praktisnya, misalnya, menjelaskan aspek teknis malware, serangan DoS, dll. atau merinci jenis bukti yang digunakan oleh otoritas penegak hukum. Presentasi-presentasi ini, alih-alih menggunakan analisis sistematis atau kritis, hanya bersifat deskriptif dan seringkali tidak dapat divalidasi secara ilmiah. Seperti yang ditunjukkan oleh kriminologi kritis, sering kali karya-karya tersebut menganut gagasan bahwa teknologi baru menciptakan peluang baru untuk melakukan tindakan kriminal hanya dengan mengandalkan laporan subjektif. meningkatnya dampak buruk yang ditimbulkan oleh perusahaan hak cipta, perusahaan keamanan siber, media, dan pemerintah. Sebagian besar penulis survei tersebut tidak memperlakukan kejahatan dunia maya sebagai sebuah konstruksi sosial; oleh karena

itu, mereka tidak dapat mempertanyakan asumsi normatif atau kepentingan ekonomi yang membuat aktivitas digital tertentu dianggap berbahaya, seperti peretasan atau pembajakan digital. Analisis ini mungkin mengabaikan fakta bahwa meningkatnya volume kerusakan yang didokumentasikan mungkin sekadar mencerminkan betapa meluasnya kerusakan yang terjadi. penggunaan teknologi informasi telah menjadi bagian dari bisnis, pemerintahan, dan kehidupan sehari-hari.

Pelanggaran Kejahatan Dunia Maya

Sebagian besar definisi kejahatan dunia maya membedakan antara kejahatan yang dimungkinkan oleh dunia maya dan kejahatan yang ketergantungan terhadap dunia maya. Kejahatan yang dimungkinkan oleh dunia maya adalah kejahatan konvensional yang dilakukan dengan menggunakan teknologi informasi sistem komputer sebagai instrumennya, misalnya sebagai dalam penipuan siber, penguntitan siber. Kejahatan ketergantungan dunia maya menargetkan perangkat atau infrastruktur teknologi informasi sistem komputer sebagai objeknya, seperti dalam peretasan komputer, malware. Sistem komputer umumnya didefinisikan sebagai perangkat yang memproses data secara otomatis berdasarkan suatu program. Karena hal ini mencakup mesin tik elektronik, beberapa penulis menyarankan untuk mendefinisikan kejahatan dunia maya secara khusus sehubungan dengan target atau niatnya, misalnya, sebagai "aktivitas yang dimediasi komputer yang baik ilegal atau dianggap terlarang oleh pihak-pihak tertentu dan dapat dilakukan melalui jaringan elektronik global".

Namun, definisi sempit tersebut akan mengecualikan kejahatan yang terjadi di luar internet atau jaringan lain yang biasanya tercantum dalam perjanjian transnasional seperti Konvensi Kejahatan Dunia Maya, misalnya, penggunaan perangkat fisik (misalnya flash drive USB) untuk menginfeksi komputer dengan malware. Bahkan definisi yang lebih luas mungkin memerlukan perluasan mengingat keberadaan teknologi informasi yang ada di mana-mana saat ini. Dalam beberapa tahun terakhir, teknologi informasi semakin menyatukan domain fisik, digital, dan biologis seperti yang dicontohkan oleh Internet of Things, rumah pintar, komputasi awan, mengemudi semi-otomatis, dll. Semakin banyak perangkat yang terhubung ke internet (ponsel, mobil, printer). Karena keberadaannya yang terus berkembang, para penjahat semakin banyak menggunakan teknologi informasi dengan berbagai cara. Oleh karena itu, sebagian besar akademisi dan pembuat undang-undang sepakat bahwa tidak ada definisi yang mencakup semua hal mengenai "kejahatan dunia maya", namun definisi yang ada akan berguna untuk menjelaskan tindakan-tindakan tertentu yang merupakan kejahatan dunia maya. Penyerahan ini merupakan indikasi lain bahwa "kejahatan dunia maya" bukanlah istilah yang cocok untuk digunakan dalam penelitian akademis, seperti disebutkan sebelumnya.

Umumnya, apa yang disebut *"keranjang tindakan"* didasarkan pada tiga kelompok pelanggaran berbeda yang tercakup dalam Konvensi Kejahatan Dunia Maya yang disusun dalam tiga kategori berbeda; Pertama, pelanggaran akses, atau tindakan yang melanggar kerahasiaan, integritas dan ketersediaan data dan sistem komputer, khususnya peretasan komputer. Kedua, pelanggaran penggunaan, atau pelanggaran konvensional yang dilakukan dengan menggunakan perangkat teknologi informasi untuk keuntungan atau kerugian

pribadi atau finansial, misalnya pemalsuan komputer, penipuan dunia maya. Terakhir, pelanggaran konten yang adalah kejahatan terkait konten yang dilakukan melalui internet atau jaringan lain untuk distribusi, akuisisi, konsumsi, dan sejenisnya, misalnya pornografi anak berbasis komputer, pelanggaran hak cipta terkait komputer dan perkataan kebencian.

10.2 DIMENSI GLOBAL KEJAHATAN DUNIA MAYA

Tantangan Global

Dimensi kejahatan dunia maya yang bersifat lintas batas negara menimbulkan tantangan terbesarnya, pertama, karena negara-negara memperlakukan hukum pidana mereka sebagai ekspresi kedaulatan. Hal ini memberikan mereka senjata ampuh untuk melakukan kontrol sosial yang melindungi para korban, namun juga membatasi kebebasan individu sehingga harus dibenarkan. Hukum pidana juga sering kali dibentuk dan dihubungkan dengan konsepsi budaya nasional, mengenai perilaku menyimpang. Ruang lingkup pelarangan pidana dan pengamanan prosedural sangat bergantung pada persyaratan konstitusi nasional yang berbeda-beda. Dengan kata lain, hukum pidana pada dasarnya adalah hukum nasional, dan hukum ini terutama ditegakkan oleh otoritas nasional.

Kedua, aktivitas dunia maya pada dasarnya merupakan fenomena lintas batas negara. Sebagian besar proses transfer data, mulai dari menulis email hingga mengakses situs web, terjadi di lebih dari satu negara karena setiap tindakan yang dilakukan oleh pengguna internet melibatkan penggunaan server yang biasanya berlokasi di luar negeri. Infrastruktur penting seperti pasokan air dan aktivitas sehari-hari seperti mengendarai mobil semakin banyak dijalankan oleh teknologi informasi dan sering kali diintegrasikan ke dalam jaringan komputer, menjadikannya target kejahatan dunia maya yang juga dapat dengan mudah dilakukan dari luar negeri.

Internet juga telah memfasilitasi peningkatan perdagangan lintas batas, jasa, komunikasi, dan lain-lain. Akibatnya, kejahatan yang dulunya hanya terjadi di satu negara kini sering kali melibatkan lebih dari satu negara jika dilakukan menggunakan internet (misalnya penipuan komputer dalam konteks perdagangan atau bisnis atau fitnah di jejaring sosial). Serangan terhadap sistem komputer dapat dengan mudah diatur dan dilakukan dari luar negeri melalui internet.

Kejahatan semacam ini memerlukan investigasi dan keterlibatan aparat penegak hukum di berbagai negara; namun, melakukan investigasi di negara lain dan menegakkan hukum di luar negeri bertentangan dengan kedaulatan negara. Pendekatan klasik untuk menghindari hambatan ini dalam kasus-kasus seperti ini adalah dengan saling memberikan bantuan hukum timbal balik kepada negara-negara tersebut. Namun, bantuan hukum timbal balik, khususnya ekstradisi, biasanya memerlukan kriminalitas ganda, yang prasyaratnya mungkin tidak terpenuhi. Kriminalitas ganda berarti bahwa tindakan tersebut memenuhi syarat sebagai kejahatan di kedua negara. Berdasarkan prinsip ini, seorang tersangka dapat diekstradisi dari suatu negara untuk diadili karena melakukan kejahatan di negara lain hanya jika kejahatan serupa tercatat di negara yang mengekstradisinya. Jika negara A tidak memiliki undang-undang yang melarang pembuatan malware, misalnya, prinsip kriminalitas

ganda dapat mencegah ekstradisi tersangka dari negara A untuk menghadapi tuduhan pembuatan malware di negara B.

Dalam kasus salah satu virus komputer paling merusak dalam sejarah, worm komputer "ILOVEYOU", yang menginfeksi lebih dari sepuluh juta komputer di seluruh dunia pada tahun 2000, pihak berwenang dengan cepat melacaknya hingga penciptanya di Filipina Namun, sebagai penduduk sah di sana, dia tidak dapat dituntut karena pada saat itu dia menciptakan malware, itu tidak dianggap sebagai kejahatan di Filipina. Selain itu, memberikan bantuan hukum timbal balik melalui jalur formal mungkin memakan waktu terlalu lama untuk memungkinkan keberhasilan investigasi dan penegakan hukum. Misalnya, data lalu lintas yang mungkin merupakan bukti relevan mengenai suatu kejahatan akan segera dihapus, dan prosedur formal untuk mendapatkan bukti dari negara lain dapat memakan waktu berminggu-minggu, bahkan berbulan-bulan. Yang terakhir, situasi ini dapat menciptakan tempat berlindung yang aman. Artinya wilayah di mana kejahatan dunia maya tertentu tidak dapat dituntut meskipun kejahatan tersebut mempunyai dampak yang merugikan di negara lain.

Pendekatan untuk Mengatasi Kejahatan Dunia Maya Global

Dua pendekatan utama untuk menangani kejahatan dunia maya sebagai fenomena global adalah undang-undang dan langkah-langkah kebijakan. Perundang-undangan dapat bersifat nasional, transnasional dan internasional. Perundang-undangan transnasional dan internasional bertujuan untuk menyelaraskan hukum pidana substantif dalam negeri, karena kerja sama antarnegara sering kali memerlukan kriminalitas ganda. Tujuan utama kedua adalah menetapkan aturan prosedural untuk kerja sama antar negara guna memperkuat penyelidikan lintas batas dan penegakan hukum. Pendekatan kebijakan berfokus pada peningkatan kapasitas dalam legislasi atau penegakan hukum, dukungan untuk kerja sama dalam penyelidikan, serta langkah-langkah teknis dan pendidikan. Tujuannya adalah untuk meningkatkan keterampilan dan pengetahuan para aktor sosial yang memerangi kejahatan dunia maya dan calon korban kejahatan dunia maya serta membina struktur kerja sama antarnegara.

10.3 PENDEKATAN LEGISLATIF

Sekilas, orang mungkin berpikir karena jangkauannya yang global, kejahatan dunia maya harus diatur oleh hukum pidana internasional. Namun, kejahatan dunia maya sebagian besar diatur oleh apa yang oleh banyak penulis disebut sebagai hukum pidana transnasional.

Membedakan Hukum Pidana Internasional dan Transnasional

Terdapat konsensus luas di antara para komentator yang menyatakan bahwa membedakan antara hukum pidana internasional dan hukum pidana transnasional adalah hal yang penting. Argumennya adalah bahwa masing-masing hukum tersebut mempunyai rezim kontrol yang berbeda, terutama yang berkaitan dengan yurisdiksi, dan masing-masing mendasari kebutuhan pembenaran yang berbeda. Konsep yang tidak demikian membedakan antara hukum internasional dan transnasional mengaburkan karakter rezim-rezim tersebut yang sangat berbeda.

Hukum transnasional pada awalnya dibingkai oleh Philipp Jessup sebagai *"semua hukum yang mengatur tindakan atau peristiwa yang melampaui batas negara"*. Dengan demikian, hukum pidana transnasional adalah hukum yang menangani kejahatan yang melampaui batas negara. Hukum pidana transnasional ditetapkan melalui perjanjian bilateral atau multilateral yang mewajibkan setiap negara yang menjadi pihak dalam perjanjian tersebut untuk mengkriminalisasi perilaku tertentu (rezim penindasan), dan menerapkan hukum pidana yang sesuai kepada individu dalam memenuhi kewajiban perjanjiannya. Rezim penindasan, bukannya melakukan self-executing, memerlukan tindakan legislatif dari masing-masing negara perjanjian. Perjanjian biasanya hanya memuat seperangkat standar definisi, unsur kejahatan, bentuk perilaku, tanggung jawab pelaku dan sejenisnya. Konvensi-konvensi tersebut juga menetapkan aturan minimum sanksi yang diperlukan untuk menghasilkan tingkat kesesuaian antara definisi kejahatan nasional yang diperlukan untuk penegakan hukum antarnegara, terutama untuk kriminalitas ganda sebagai prasyarat ekstradisi. Misalnya, Konvensi PBB tahun 1988 Menentang Peredaran Gelap Narkotika dan Narkotika. Psikotropika mewajibkan negara pihak untuk mengkriminalisasi penggunaan dan distribusi zat-zat tertentu yang terdaftar seperti heroin. Negara-negara pihak memenuhi persyaratan dengan memasukkan pelanggaran narkotika yang disyaratkan ke dalam hukum pidana domestik mereka dan dengan menuntut pelanggaran di dalam negeri.

Sebaliknya, empat kejahatan inti internasional yang ditetapkan oleh Statuta Roma KUHP Internasional tahun 1998 genosida, kejahatan perang, kejahatan terhadap kemanusiaan, dan kejahatan agresi dapat diterapkan secara langsung terhadap individu. Pengadilan Kriminal Internasional dapat mengadili dan menghukum individu atas tindakan mereka yang melanggar hukum. kejahatan internasional yang dilakukan (jika negara sendiri tidak mampu atau tidak mau melakukannya). Negara pihak tidak harus menyesuaikan hukum pidana domestiknya dengan kejahatan internasional inti yang diatur dalam Kode Etik. Karena landasan hukum transnasional dan internasional berbeda, maka hukum pidana transnasional lebih sulit untuk dibenarkan. Kejahatan internasional hanyalah pelanggaran serius yang bersumber pada nilai-nilai yang dianut secara internasional, seperti martabat manusia. Kriminalisasi didasarkan pada gagasan bahwa tindakan menyebabkan kerugian serius dengan melanggar hak asasi manusia atau prinsip-prinsip lain yang dianut secara global harus dikenakan sanksi. Sebaliknya, hukum pidana transnasional hanya secara sporadis memasukkan kejahatan mala in se. Sebaliknya, hal ini cenderung berfokus pada pelanggaran peraturan sehubungan dengan pengendalian pasar barang dan jasa tertentu (misalnya perdagangan narkoba, materi hak cipta, perdagangan gelap produk tembakau). Pelanggaran yang diakibatkannya tidak berasal dari dampak buruk yang hakiki dari kegiatan tersebut namun perlunya kerja sama dalam mengatasi hambatan yang ditimbulkan oleh kedaulatan terhadap penerapan hukum pidana di luar batas negara secara efektif. Misalnya, hampir tidak mungkin untuk mengendalikan perdagangan obat-obatan terlarang jika negara-negara tetangga tidak melarang produksi dan perdagangan obat-obatan terlarang. distribusi obat-obatan tersebut. Namun, berbeda dengan kasus genosida atau kejahatan perang, tidak

jelas hak siapa yang dilanggar atau kerugian apa yang ditimbulkan jika tidak mematuhi peraturan pasar (misalnya dengan menjual produk tembakau yang tidak dikenakan pajak atau menggunakan obat-obatan terlarang). Ringkasnya, inti dari kasus ini adalah kejahatan internasional dapat dengan mudah dibenarkan karena melindungi hak-hak dan tuntutan dasar, sedangkan hukum pidana transnasional tidak dapat dianggap tidak dapat diterima dan seringkali memerlukan pembenaran lebih lanjut.

Tindakan PBB

Perserikatan Bangsa-Bangsa belum mengembangkan undang-undang kejahatan siber, seperti halnya yang telah dilakukan untuk perdagangan narkoba atau pelanggaran teroris. Kantor PBB untuk Narkoba dan Kejahatan sejauh ini hanya melakukan beberapa penelitian mengenai tantangan kejahatan siber. PBB juga telah menunjuk kelompok ahli , seperti pertemuan kelompok pakar terbuka mengenai kejahatan dunia maya untuk mengkaji tanggapan hukum dan teknis terhadap kejahatan dunia maya. Konvensi PBB tentang kejahatan dunia maya telah diperdebatkan sejak tahun 2010. Namun, fokus PBB telah bergeser dari undang-undang ke tindakan kebijakan karena menyatakan bahwa merupakan pihak dalam Konvensi Kejahatan Dunia Maya Dewan Eropa dengan keras menolak perundingan perjanjian internasional lainnya mengenai kejahatan dunia maya, mengingat bahwa Konvensi tersebut sudah terbuka bagi negara-negara non-Anggota. Langkah-langkah PBB saat ini mencakup pembentukan gudang kejahatan dunia maya dengan basis data nasional undang-undang kejahatan dunia maya, yurisdiksi dan alat-alat untuk pengembangan kapasitas. Hal ini dirancang khusus untuk membantu negara-negara berkembang menerapkan undang-undang kejahatan dunia maya dan untuk berbagi pengetahuan teknis sehubungan dengan penegakan hukum.

Pelanggaran kejahatan dunia maya juga tidak dimasukkan ke dalam Statuta Roma bersama dengan empat kejahatan inti internasional yang tercantum di dalamnya. Meskipun kejahatan inti internasional pada prinsipnya dapat dilakukan dengan sistem komputer sebagai instrumen kejahatan yang penting atau dengan secara khusus menargetkan sistem komputer sebagai objeknya, hingga saat ini kejahatan-kejahatan tersebut hanya melibatkan tindakan yang dapat dikategorikan sebagai kejahatan dunia maya. Para peneliti akademis telah menganjurkan pembentukan Pengadilan Kriminal Internasional untuk Ruang Siber.65 Yurisdiksinya akan dibatasi pada kejahatan siber yang menjadi perhatian paling serius bagi komunitas internasional, seperti kejahatan siber yang melanggar perjanjian global mengenai kejahatan siber atau melancarkan serangan siber terhadap infrastruktur penting dalam negeri. Namun, hingga saat ini konsep tersebut hanya ada di atas kertas. Hal ini dapat dijelaskan dengan adanya anggapan yang cenderung memasukkan berbagai macam pelanggaran yang akan memberikan yurisdiksi luas kepada pengadilan internasional, sehingga sangat membatasi kedaulatan negara terkait aktivitas digital.

Konvensi Dewan Eropa tentang Kejahatan Dunia Maya

Undang-undang yang menangani kejahatan dunia maya sebagian besar adalah hukum transnasional. Di negara-negara Barat, sebagian besar hukum pidana nasional yang menangani kejahatan dunia maya diselaraskan, atau bahkan didorong, oleh Konvensi Dewan

Eropa tentang Kejahatan Dunia Maya dan, di Uni Eropa, melalui Keputusan dan Arahan Kerangka Kerja yang terkait.

Konvensi mengenai Kejahatan Dunia Maya (Cybercrime) adalah perjanjian multilateral mengenai kejahatan dunia maya sebuah rezim hukum yang oleh banyak komentator dikategorikan sebagai hukum pidana transnasional, bukan hukum pidana internasional. Meskipun faktanya perjanjian ini kurang berhasil dibandingkan dengan konvensi transnasional lainnya seperti Konvensi PBB Melawan Transnasional Kejahatan Terorganisir, Konvensi Kejahatan Dunia Maya masih menjadi instrumen hukum paling berpengaruh untuk mengatur kejahatan dunia maya secara global.68 Pada bulan Februari 2021, negara telah menandatanganinya, dan 65 negara telah meratifikasinya. Para penandatangannya mencakup sebagian besar anggota Dewan Eropa, terutama Jerman, Perancis, Italia, dan Inggris.

Negara-negara yang bukan anggota Dewan Eropa dapat diterima menjadi anggota Konvensi dengan persetujuan bulat dari para penandatangan. Kategori ini mencakup AS, Kanada, Jepang, Australia serta beberapa negara bagian Afrika (misalnya Afrika Selatan, Ghana, Senegal) dan Amerika Latin (Argentina, Chili, Peru). Sejumlah pihak yang skeptis meragukan seberapa besar pengaruh Konvensi ini terhadap undang-undang kejahatan dunia maya global karena Konvensi ini belum ditandatangani oleh Rusia dan Tiongkok tidak termasuk sekitar 50% aktivitas internet global. Namun, dalam tiga tahun terakhir, ada tambahan sepuluh negara-negara menandatangani Konvensi. Brasil baru-baru ini memulai proses aksesi untuk bergabung dalam Konvensi. Selain itu, Konvensi Kejahatan Dunia Maya memberikan pengaruh yang besar terhadap regulasi kejahatan dunia maya oleh negara-negara non-Anggota, misalnya di Mesir, Nigeria, dan Pakistan.

Konvensi ini mempelopori pendekatan netral-teknologi sehubungan dengan pelanggaran dunia maya yang memungkinkan negara tersebut beradaptasi dengan perkembangan teknologi baru, sebuah pendekatan yang telah menjadi standar dalam undang-undang kejahatan dunia maya. Singkatnya, Konvensi ini berfungsi sebagai model undang-undang kejahatan dunia maya di sebagian besar negara Barat tetapi juga di Asia, Afrika, dan Amerika Selatan. Konvensi ini mewajibkan negara-negara pihak untuk mengkriminalisasi serangkaian tindakan yang dianggap sebagai kejahatan dunia maya serta kerja sama antar negara dalam penegakan hukum dan telah menyebabkan harmonisasi rezim pengendalian kejahatan dunia maya nasional di negara-negara yang menganut Konvensi tersebut.

Tidak semua peraturan nasional mengenai kejahatan dunia maya menerapkan Konvensi Kejahatan Dunia Maya, meskipun hal ini jarang terjadi di negara-negara pihak atau negara-negara yang terkena dampak. Sebagian besar peraturan domestik mengenai kejahatan dunia maya di negara-negara Barat sejalan dengan atau setidaknya dipengaruhi oleh Konvensi ini karena Konvensi ini memuat cakupan yang luas mengenai tindakan-tindakan yang harus dikriminalisasi. Selain itu, beberapa aktivitas siber tidak memiliki dimensi lintas batas (misalnya aktivitas siber penipuan yang menargetkan orang-orang di dalam suatu negara). Namun, aktivitas semacam ini biasanya juga termasuk dalam hukum

pidana nasional, berdasarkan Konvensi Kejahatan Dunia Maya. Seperti halnya hukum transnasional pada umumnya, ketentuan pidana yang disyaratkan biasanya tidak mensyaratkan unsur perilaku lintas batas negara, namun mencakup perilaku, terlepas dari apakah hal tersebut mempunyai dimensi transnasional atau tidak. Hal ini mungkin mencerminkan tujuan dari rezim penindasan: Mereka harus melarang tindakan tertentu. melakukan tindakan tidak hanya dalam situasi lintas batas negara namun juga di dalam negara dengan asumsi bahwa tindakan tersebut pada akhirnya akan menghasilkan dampak lintas batas. Hal ini menjamin penegakan hukum antar negara bagian, terutama melalui kriminalitas ganda, yang biasanya diperlukan untuk ekstradisi, dan mencegah adanya tempat berlindung yang aman.

Konvensi Kejahatan Dunia Maya menetapkan persyaratan untuk kriminalisasi aktivitas dunia maya hukum pidana substantif serta untuk menuntut kejahatan dunia maya hukum pidana prosedural dan konflik yurisdiksi. Putusan mengenai dua hal terakhir tidak akan disajikan karena kontribusi ini berfokus pada larangan pidana.

Sebagai konsekuensi dari permasalahan definisi yang disebutkan di atas (lihat Bagian 1), Konvensi Kejahatan Dunia Maya tidak mendefinisikan kejahatan dunia maya seperti itu. Sebaliknya, undang-undang ini membatasi dirinya hanya pada mewajibkan hukuman untuk tiga jenis pelanggaran "perilaku siber" tertentu, yaitu (1) pelanggaran akses, (2) penggunaan, dan (3) pelanggaran konten. Konvensi ini memperkenalkan pendekatan netral teknologi yang memungkinkan negara tersebut beradaptasi terhadap teknologi baru. Bagian terminologi Konvensi hanya mendefinisikan *"sistem komputer", "data komputer", "penyedia layanan" dan "data lalu lintas"* (Pasal 1). Suatu sistem komputer berarti setiap perangkat atau sekelompok perangkat yang saling berhubungan atau terkait, satu atau lebih perangkat tersebut secara otomatis memproses data berdasarkan suatu program (ibid.). Sistem komputer dapat menjadi sistem yang berdiri sendiri.

Judul pertama tentang pelanggaran bertujuan untuk melindungi integritas sistem komputer. Hal ini memerlukan kriminalisasi atas tindakan "yang bertentangan dengan kerahasiaan, integritas dan ketersediaan data dan sistem komputer" (yang disebut pelanggaran CIA). Hal ini termasuk akses ilegal (terutama "peretasan komputer") (Pasal 2), yang didefinisikan sebagai akses yang disengaja dan tidak sah. ke seluruh atau sebagian sistem komputer. Pelanggaran-pelanggaran ini biasanya memicu terjadinya kejahatan lebih lanjut seperti memodifikasi atau memperoleh data yang disimpan. Oleh karena itu, Konvensi ini menawarkan kepada negara-negara pihak kemungkinan untuk membatasi tanggung jawab pidana dengan memasukkan unsur-unsur kejahatan yang bersifat restriktif, seperti pelanggaran langkah-langkah keamanan (misalnya, mengabaikan otentikasi kata sandi) , niat tidak jujur atau pelanggaran yang dilakukan terhadap sistem komputer melalui jaringan.

Pasal 3 berfokus pada perlindungan integritas dan kerahasiaan data. Undang-undang ini menyerukan kriminalisasi intersepsi ilegal yang disengaja atas transmisi data non-publik (rahasia) dari atau di dalam sistem komputer, misalnya, mencuri data selama transfer melalui jaringan nirkabel (WLAN). Sekali lagi, para pihak dapat menambahkan unsur-unsur kejahatan yang membatasi, seperti niat tidak jujur. Spionase data tanpa akses ilegal

sebelumnya tidak dikategorikan sebagai tindakan yang dikriminalisasi (misalnya menyalin file sambil melakukan pemeliharaan pada komputer). Beberapa negara telah memperluas perlindungan dengan menghukum spionase data yang hanya melibatkan informasi spesifik atau segala jenis data komputer yang disimpan.

Pasal 4 membahas pelanggaran interferensi data, sehingga melindungi integritas data komputer, termasuk perusakan, penghapusan, dan sebagainya pada data komputer. Para Pihak pada Konvensi ini dapat mensyaratkan bahwa campur tangan tersebut mengakibatkan kerugian yang serius. Pasal 5 bertujuan untuk melindungi integritas sistem komputer dengan memberikan sanksi terhadap gangguan sistem, yang berarti gangguan serius dan tidak sah yang disengaja terhadap fungsi sistem komputer (misalnya serangan penolakan layanan yang membuat situs web untuk sementara tidak dapat diakses oleh lalu lintas yang sah; serangan terhadap fungsi sistem komputer infrastruktur penting seperti pasokan air yang dijalankan oleh sistem komputer). Hal ini tidak termasuk manipulasi sistem komputer selain interferensi (misalnya penambahan data). Berbeda dengan artikel sebelumnya, artikel ini tidak secara eksplisit memberikan elemen pembatasan opsional. Namun, campur tangan tersebut harus bersifat "serius", dan menyerahkan tanggung jawab kepada negara pihak untuk menentukan kriteria keseriusan yang dapat mereka gunakan untuk membatasi pelanggaran tersebut. Misalnya, peraturan ini dapat menetapkan dampak merugikan yang signifikan terhadap kemampuan menggunakan sistem atau berkomunikasi dengan sistem lain (sehingga spamming tidak termasuk dalam tanggung jawab pidana).

Pasal 6 ditujukan pada penggunaan "alat peretas". Undang-undang ini secara eksklusif menghukum tindakan-tindakan yang berpotensi membahayakan yang biasanya terjadi sebelum pelanggaran-pelanggaran yang telah terjadi. Undang-undang ini menyerukan kriminalisasi terhadap tindakan-tindakan yang secara sengaja memproduksi, menjual atau dengan cara lain menyediakan perangkat yang dirancang atau diadaptasi terutama untuk tujuan melakukan pelanggaran-pelanggaran yang telah ditetapkan atau untuk membobol kata sandi. , kode akses dan sejenisnya, dengan maksud untuk digunakan dalam melakukan pelanggaran yang telah ditetapkan (Pasal 6(1)(a)). Pasal 6(1)(b) mengharuskan adanya hukuman atas kepemilikan yang disengaja atas alat-alat tersebut dengan maksud untuk menggunakannya dalam melakukan pelanggaran yang sudah ditetapkan. Pihak-pihak dalam Konvensi dapat mewajibkan sejumlah barang tersebut untuk dimiliki sebelum tanggung jawab pidana dapat dipicu. Selain itu, negara pihak hanya diperbolehkan untuk mengkriminalisasi penjualan, distribusi, atau penyediaan barang-barang yang dimaksud, khususnya tidak termasuk kepemilikan (Pasal 6(2)). Pelanggaran-pelanggaran ini kontroversial karena tidak dapat ditentukan dengan jelas kapan pelaku mempunyai niat yang cukup untuk dimintai pertanggungjawaban. Spesialis keamanan, misalnya, mungkin berisiko menghadapi tanggung jawab pidana ketika mereka membeli atau menggunakan alat tersebut secara profesional (alat penggunaan ganda).

Jenis pelanggaran yang kedua mengharuskan kriminalisasi kejahatan "offline" tertentu yang menggunakan sistem komputer untuk keuntungan pribadi atau finansial. Tujuannya adalah untuk melindungi properti, aset keuangan, dan keaslian dokumen. Pasal 7

mewajibkan negara untuk mengkriminalisasi pemalsuan yang dibantu komputer dengan tujuan menciptakan data tidak autentik untuk dianggap atau ditindaklanjuti demi tujuan hukum seolah-olah data tersebut asli. Suatu pihak mungkin memerlukan niat untuk menipu atau niat tidak jujur serupa. Pasal 8 mewajibkan para pihak untuk memberikan sanksi terhadap penipuan yang berhubungan dengan komputer.

Judul ketiga tentang delik berkaitan dengan isi. Pasal 9 menerapkan hukuman atas tindakan yang melibatkan pornografi anak, termasuk produksi, penjualan dan pengadaan yang disengaja dengan menggunakan sistem komputer (yaitu membelinya) serta kepemilikan belaka. Para pihak mempunyai kelonggaran untuk tidak mengkriminalisasi dua pelanggaran terakhir. Secara keseluruhan, Seni. Pasal 9 terutama mencakup tindakan yang menjadi sumber pelecehan terhadap anak (dalam rangka memproduksi pornografi anak) namun tidak mengeksploitasi anak secara seksual. Karena sebagian besar negara telah memberikan sanksi terhadap kekerasan terhadap anak-anak serta cara-cara distribusi tradisional, Art. 9 terutama berupaya untuk menyelaraskan berbagai peraturan mengenai pornografi anak, terutama yang berkaitan dengan usia. Hal ini juga mencakup kegiatan-kegiatan awal seperti pembuatan gambar fiksi, yang tidak melanggar hak-hak anak namun mungkin digunakan untuk memancing anak-anak agar berpartisipasi dalam tindakan pornografi.

Pasal 10 berfungsi untuk melindungi hak kekayaan intelektual, karena pelanggaran yang melibatkan distribusi digital atas materi berhak cipta telah meningkat secara eksponensial. Konvensi ini menyerukan pemberian sanksi terhadap pelanggaran hak cipta dan hak terkait yang disengaja terkait komputer sebagaimana didefinisikan dalam hukum nasional sesuai dengan kewajiban internasional. Karena sebagian besar negara telah mengkriminalisasi pelanggaran hak cipta, Art. Pasal 10 pada dasarnya memberikan prinsip-prinsip dasar. Pasal ini hanya menyerukan kriminalisasi terhadap pelanggaran dalam skala komersial (Pasal 10(1)). Para pihak mempunyai hak untuk tidak mengkriminalisasi suatu tindakan, dengan syarat tersedia upaya hukum lain yang efektif (Pasal 10(3)).

Karena pihak-pihak yang merundingkan Konvensi ini tidak dapat sepakat untuk mengkriminalisasi "perkataan kebencian" yang berhubungan dengan komputer, ketentuan-ketentuan terkait dipisahkan dalam Protokol Pertama Konvensi. Protokol ini mewajibkan para pihak untuk mengkriminalisasi penggunaan sistem komputer untuk menyebarkan pesan-pesan rasis. dan materi xenofobia, karena melontarkan ancaman atau penghinaan yang rasis dan xenofobia, dan untuk menyangkal, terlalu meremehkan, menyetujui atau membenarkan genosida atau kejahatan terhadap kemanusiaan (misalnya penyangkalan Holocaust). Hanya 45 negara yang menandatangani Protokol Tambahan, dan hingga kini baru 32 negara yang meratifikasinya. Banyak negara pihak, seperti Amerika Serikat, menganggap persyaratan Protokol ini tidak sesuai dengan kebebasan berpendapat yang dijamin konstitusi. Kurangnya harmonisasi peraturan mengenai perkataan kebencian menyebabkan kesulitan dalam penuntutan jika hal tersebut terjadi dalam konteks antarnegara, dan hal ini sering terjadi.

Konvensi ini menyerukan kriminalisasi bahkan ketika mencoba melakukan pelanggaran-pelanggaran yang disebutkan di atas dan karena membantu atau bersekongkol dalam pelanggaran-pelanggaran tersebut (Pasal 11) serta tanggung jawab pidana terhadap badan hukum, termasuk penyedia layanan internet (Pasal 12). Konvensi juga merekomendasikan penerapan sanksi yang efektif, proporsional dan menjerat, termasuk perampasan kebebasan (Pasal 13), namun tidak menetapkan sanksi minimum.

Keputusan dan Arahan Kerangka Kerja Uni Eropa Mengatasi Kejahatan Dunia Maya

Di Uni Eropa, kejahatan yang tercakup dalam Konvensi Kejahatan Dunia Maya dimasukkan dalam berbagai Keputusan dan Arahan Kerangka Kerja UE, khususnya dalam Petunjuk mengenai serangan terhadap sistem informasi (2013). Dengan adanya Perjanjian Lisbon (2009), hampir semua kriteria yang menandai perbedaan material antara hukum pidana dan bidang kebijakan lainnya di Uni Eropa dihilangkan yang paling sering dilihat sebagai pengembangan jenis hukum pidana transnasional baru yang sering disebut dengan hukum pidana transnasional. hukum pidana supranasional. Namun peraturan pidana UE masih belum mengikat secara langsung di hampir semua bidang dan harus diterapkan dalam hukum pidana domestik seperti halnya hukum transnasional. Meskipun demikian, proses legislatif dan keberlakuan persyaratan UE untuk hukum pidana domestik telah berubah secara signifikan karena penggantian Keputusan Kerangka Kerja dengan Petunjuk (Pasal 83(2) TFEU). Secara khusus, hal ini menghasilkan langkah-langkah untuk mengendalikan dan mendorong penerapan serta pemberian sanksi terhadap ketidakpatuhan (proses pelanggaran atas keterlambatan atau kesalahan transposisi Petunjuk, Pasal 258 TFEU). Hal ini telah meningkatkan harmonisasi aturan-aturan konstitutif dalam definisi dan hukuman kejahatan secara signifikan, sehingga menghasilkan sejumlah besar amandemen terhadap hukum pidana nasional di Uni Eropa.

Evolusi hukum pidana UE didorong oleh penerapan aturan saling pengakuan (Pasal 82 TFEU), yang menciptakan sistem hukum pidana Eropa dalam menegakkan keputusan dan putusan. Salah satu tonggak dalam perkembangan ini adalah penggantian ekstradisi prosedur yang ditetapkan oleh Surat Perintah Penangkapan Eropa (European Arrest Warrant/EAW) yang tidak mensyaratkan kriminalitas ganda di kedua negara yang terlibat dalam pelaksanaannya. Berbeda dengan Konvensi Kejahatan Dunia Maya, Petunjuk mengenai serangan terhadap sistem informasi hanya mewajibkan Negara-negara Anggota UE untuk mengkriminalisasi apa yang disebut sebagai pelanggaran CIA (lihat Bagian 3.3). Ini adalah pelanggaran akses yang diatur dalam Judul 1 Konvensi Kejahatan Dunia Maya, meskipun dengan beberapa pengecualian. Petunjuk tersebut menyerukan kriminalisasi peretasan komputer, intersepsi ilegal atas transmisi data komputer non-publik dari atau di dalam sistem komputer, pelanggaran interferensi (Pasal 3–6) serta produksi, penjualan atau distribusi yang disengaja. alat yang relevan (Pasal 7). Negara-negara Anggota dapat membatasi cakupan pelanggaran akses pada kasus-kasus yang tidak ringan. Intervensi sistem yang ilegal diperluas hingga mencakup interupsi sistem, dan pelanggaran karena membuat data tidak dapat diakses dapat dikualifikasikan sebagai tindak pidana (Pasal 4). Selain itu, Petunjuk tersebut menyerukan agar pelanggaran campur tangan menjadi lebih parah jika

identitas asli pelaku dirahasiakan, jika melibatkan kejahatan terorganisir, atau jika alat yang dirancang untuk menyerang sejumlah besar sistem informasi atau sistem penting digunakan (Pasal 9).

Petunjuk ini tidak mencakup versi kejahatan tradisional yang berhubungan dengan komputer atau kejahatan yang berhubungan dengan konten. Namun, hal ini diatur secara terpisah dalam peraturan UE lainnya, seperti Petunjuk untuk memerangi pelecehan seksual dan eksploitasi seksual terhadap anak-anak dan pornografi anak (2011).

Arahan Komunitas Ekonomi Negara-negara Afrika Barat dalam Memerangi Kejahatan Dunia Maya

Beberapa organisasi antar pemerintah regional di Afrika telah menangani kejahatan siber dengan arahan mereka sendiri. Diantaranya adalah Petunjuk Memerangi Kejahatan Dunia Maya (Cybercrime) dalam ECOWAS yang diadopsi pada tahun 2011 oleh 15 negara di Afrika Barat setelah menjadi jelas bahwa beberapa negara tersebut telah menjadi sumber utama penipuan email dan penipuan biaya di muka di seluruh dunia. Petunjuk ini dapat dikategorikan sebagai kejahatan dunia maya transnasional hukum yang mewajibkan Negara-negara Anggota untuk menyelaraskan undang-undang kejahatan dunia maya mereka dengan mengkriminalisasi kejahatan-kejahatan tertentu dan untuk bekerja sama dalam penyelidikan. Dalam konteks hukum pidana substantif, Petunjuk ini memiliki cakupan yang lebih luas daripada Konvensi Kejahatan Dunia Maya. Sebab, mencakup semua kejahatan yang pendeteksiannya memerlukan bukti elektronik. Lebih jauh lagi, undang-undang ini menyerukan kriminalisasi terhadap pelanggaran yang secara ilegal tetap menggunakan sistem komputer, dengan sengaja menggunakan data palsu atau memanipulasi data secara tidak sah meskipun hanya karena kelalaian.

Persyaratan Petunjuk ini akan diadopsi pada bulan Januari 2014. Namun, hingga bulan Maret 2019, setidaknya sepertiga dari anggota belum menerapkan undang-undang kejahatan dunia maya dan tindakan lain yang diperlukan. Hambatannya mencakup perbedaan prioritas di negara-negara miskin, kurangnya kapasitas untuk membuat undang-undang mengenai kejahatan dunia maya, dan tidak adanya cara dan sarana untuk mendorong kerja sama yang efektif. Hal ini mungkin akan membantu jika Petunjuk tersebut memasukkan proses pelanggaran seperti yang dilakukan Uni Eropa. Namun, mekanisme kontrol seperti itu tidak akan membantu jika negara-negara juga melakukan hal yang sama. tidak mampu melaksanakan undang-undang tersebut karena kurangnya kapasitas dan sumber daya pemerintah dan legislatif. Akan lebih baik jika fokus pada peningkatan kapasitas dan penyediaan dukungan finansial untuk meningkatkan investigasi antarnegara dan penegakan hukum, dengan kata lain, pada pendekatan kebijakan.

10.4 PENDEKATAN KEBIJAKAN

Seperti disebutkan sebelumnya, fokus PBB telah bergeser dari pendekatan legislatif ke pendekatan kebijakan, meskipun masih ada tahap tentatif untuk mengembangkan konvensi internasional mengenai kejahatan dunia maya. Beberapa program pengukuran kebijakan regional juga sedang berjalan.

Langkah-Langkah Kebijakan PBB untuk Mengatasi Kejahatan Dunia Maya

Pada tahun 2011, PBB membentuk sebuah kelompok ahli yang bertugas untuk mengkaji hukum yang ada saat ini dan tanggapan lainnya terhadap kejahatan dunia maya dan mengembangkan hal-hal baru. Kelompok ahli tersebut mempresentasikan Draf Studi Komprehensif tentang Kejahatan Dunia Maya pada tahun 2013, yang masih menjadi dasar bagi Program kebijakan PBB lainnya saat ini. Program Global PBB mengenai Kejahatan Dunia Maya mendukung peningkatan kapasitas, pencegahan dan pendidikan, kerja sama internasional, dan studi mengenai fenomena kejahatan dunia maya di negara-negara berkembang. Alat-alat yang digunakan mencakup pembangunan basis data mengenai undang-undang kejahatan dunia maya dan pengetahuan teknis yang relevan untuk investigasi dan penegakan hukum. Program ini berupaya meningkatkan efisiensi investigasi dan penuntutan, untuk mendukung respons nasional terhadap kejahatan dunia maya melalui undang-undang dan penegakan hukum. Hal ini juga bertujuan untuk meningkatkan pengetahuan masyarakat mengenai tantangan kejahatan dunia maya dengan memperkuat pertukaran antara pemerintah dan informasi
perusahaan teknologi.

Strategi Kebijakan Regional untuk Menangani Kejahatan Dunia Maya

Sejumlah strategi kebijakan regional yang saling melengkapi telah diterapkan untuk memperkuat kapasitas negara dalam merespons kejahatan dunia maya. Proyek gabungan *"Capacity Building On Cybercrime And E-Evidence"* (GLACY) yang dilaksanakan oleh UE dan Dewan Eropa yang berlangsung dari tahun 2013 hingga 2016 merupakan contoh yang baik. Proyek ini mendorong tujuh negara prioritas (Mauritius, Maroko, Filipina, dan Filipina). Pines, Senegal, Afrika Selatan, Sri Lanka dan Tonga) untuk mengadopsi atau menyelaraskan undang-undang kejahatan dunia maya mereka agar sejalan dengan standar yang ditetapkan dalam Konvensi Kejahatan Dunia Maya. Semuanya telah menandatangani Konvensi sejak saat itu. Pelatihan bagi para hakim dan jaksa serta aparat penegak hukum diperkuat dengan memperkenalkan modul-modul mengenai kejahatan siber ke dalam kurikulum akademi pelatihan peradilan dan dengan memberikan materi dan alat pelatihan kepada otoritas penegak hukum kejahatan siber (misalnya mengenai forensik data, prosedur operasi standar). Negara-negara prioritas juga meningkatkan kemampuan mereka dalam kerja sama internasional, misalnya dengan menghubungkan otoritas penegakan hukum kejahatan dunia maya dengan EUROPOL dan INTERPOL.

OECD, Forum Kerjasama Ekonomi Asia-Pasifik (APEC), Persemakmuran, Liga Arab dan Dewan Kerjasama Teluk (UAE) dan Organisasi Negara-negara Amerika (OAS) semuanya mempunyai inisiatif kejahatan dunia maya. Organisasi-organisasi ini terutama mengatasi tantangan kejahatan dunia maya sesuai dengan kebijakan PBB dengan membentuk kelompok ahli, melakukan studi analitis dan membuat rekomendasi (tidak mengikat).118 Rencana khusus untuk mendorong peningkatan kapasitas atau kerja sama internasional serta untuk menyelaraskan undang-undang kejahatan dunia maya Namun, jumlahnya masih sedikit dan jarang.

10.5 CIRI DAN KELEMAHAN HUKUM PIDANA DIGITALITAS GLOBAL

Karakteristik Hukum Pidana Digitalitas Global Saat Ini

Hukum pidana digitalitas global diatur secara berbeda di berbagai wilayah di dunia. Namun, sebagian besar peraturan kejahatan dunia maya memiliki kesamaan karakteristik tertentu, yang akan disoroti dalam bagian ini. Karena dimensinya yang bersifat lintas batas, hukum pidana digitalitas global sebagian besar merupakan hukum pidana transnasional. Hukum pidana transnasional terdiri dari konvensi bilateral atau multilateral yang mewajibkan negara pihak untuk memasukkan pelanggaran tertentu ke dalam hukum pidana domestiknya (rezim penindasan). Persyaratan tersebut umumnya mencakup unsur pidana tertentu, persyaratan mens rea, dan actus reus, serta standar minimal sanksi. Untuk meningkatkan kerja sama dalam investigasi lintas batas dan penegakan hukum, hukum pidana transnasional bertujuan untuk menciptakan kriminalitas ganda, yang biasanya merupakan prasyarat untuk kolaborasi antar negara, misalnya untuk memberikan bantuan hukum timbal balik. Kriminalitas ganda dicapai melalui harmonisasi hukum pidana domestik sejalan dengan persyaratan rezim penindasan.

Ciri Hukum Pidana Digitalitas Global:

1. **Kerjasama Internasional:** Hukum pidana digitalitas global menekankan pentingnya kerjasama internasional dalam menghadapi kejahatan siber. Ini melibatkan pertukaran informasi, data, dan koordinasi antara berbagai negara untuk menanggapi kejahatan lintas batas.
2. **Adaptabilitas terhadap Teknologi:** Ciri ini mencerminkan kemampuan hukum pidana digitalitas global untuk terus beradaptasi dengan perkembangan teknologi. Hukum ini perlu dapat mengakomodasi perubahan dalam metode kejahatan siber, seperti malware baru atau taktik penipuan.
3. **Perlindungan Data dan Privasi:** Hukum pidana digitalitas global mencakup ketentuan yang melindungi data pribadi dan privasi individu. Ini mencerminkan kebutuhan untuk mengakui dan melindungi hak-hak individu di dunia maya.
4. **Hukuman yang Sesuai:** Hukum ini mencakup sanksi dan hukuman yang sesuai dengan tingkat seriusnya kejahatan siber. Hal ini untuk memberikan efek jera dan menunjukkan seriusnya komunitas global dalam menangani pelanggaran keamanan siber.
5. **Ketentuan Pengadilan Digital:** Pengadilan digital atau mekanisme penyelesaian sengketa dalam kerangka hukum pidana digitalitas global dapat membantu menyelesaikan kasus secara cepat dan efisien di dunia maya.

Kelemahan Hukum Pidana Digitalitas Global:

1. **Perbedaan Regulasi Nasional:** Meskipun ada upaya untuk mengkoordinasikan hukum pidana digital secara global, perbedaan dalam regulasi nasional dapat menjadi kendala. Setiap negara memiliki sistem hukum, kebijakan, dan pendekatan yang berbeda terhadap kejahatan siber.
2. **Ketidakmampuan Mengikuti Perkembangan Teknologi:** Kecepatan perkembangan teknologi sering kali lebih cepat daripada kemampuan pembuatan dan penyesuaian hukum. Ini dapat membuat hukum pidana digitalitas global kurang efektif dalam menanggapi ancaman terbaru dan metode kejahatan siber.

3. **Kesulitan dalam Penegakan Hukum:** Penegakan hukum kejahatan siber dapat sulit karena pelaku kejahatan sering dapat menyembunyikan identitas mereka secara online dan memanfaatkan infrastruktur teknologi untuk melibatkan diri dalam kegiatan ilegal.
4. **Keterbatasan Kerjasama Internasional:** Meskipun kerjasama internasional penting, ada kendala dalam praktiknya. Beberapa negara mungkin tidak memiliki peraturan hukum yang memadai atau mungkin tidak bersedia berkerjasama dalam penyelidikan dan penuntutan.
5. **Kurangnya Standar Global yang Konsisten:** Kurangnya standar global yang konsisten dalam hal hukum pidana digital dapat menciptakan celah dan ambiguitas dalam penerapan hukum, terutama ketika menangani kejahatan lintas batas.
6. **Keterbatasan Daya Deterrent:** Meskipun hukuman dapat dijatuhkan, daya deterrent terkadang kurang efektif, terutama jika pelaku kejahatan percaya bahwa mereka dapat terhindar dari penangkapan atau jika sanksi yang dijatuhkan tidak memadai.

Pemecahan kelemahan-kelemahan ini memerlukan kerja sama yang erat antara pemerintah, lembaga internasional, sektor swasta, dan masyarakat sipil untuk meningkatkan keefektifan hukum pidana digitalitas global.

Hukum pidana di Eropa yang menerapkan persyaratan konvensi pemberantasan transnasional sering kali melarang tindakan lintas batas dan hanya melarang tindakan domestik karena kejahatan transnasional jarang memasukkan faktor transnasional dalam unsur tindakannya. Hal ini karena rezim penindasan juga bertujuan untuk melarang tindakan tertentu di dalam suatu negara dengan asumsi bahwa hal tersebut menimbulkan dampak lintas batas negara dalam jangka panjang (misalnya produksi obat-obatan di suatu negara cenderung mengarah pada distribusi obat-obatan di negara lain). Selain itu, rezim penindasan juga bertujuan untuk melarang tindakan tertentu di dalam suatu negara dengan asumsi bahwa tindakan tersebut menimbulkan dampak lintas batas negara dalam jangka panjang (misalnya, produksi obat-obatan di suatu negara cenderung mengarah pada distribusi obat-obatan di negara lain). Selain itu, rezim penindasan juga bertujuan untuk melarang tindakan tertentu di dalam suatu negara dengan asumsi bahwa hal tersebut menimbulkan dampak lintas batas negara dalam jangka panjang (misalnya, produksi obat-obatan di suatu negara cenderung mengarah pada distribusi obat-obatan di negara lain). Selain itu, rezim penindasan secara global atau global setidaknya kriminalisasi regional membantu mencegah terbentuknya tempat berlindung yang aman di mana tindakan tertentu berada di luar jangkauan penuntutan. Oleh karena itu, rezim penindasan transnasional pada umumnya dan regulasi kejahatan dunia maya pada khususnya mengarah pada pengendalian spektrum luas terhadap semua jenis perilaku terlepas dari dimensi lintas batasnya.

Kontrol yang luas terhadap semua jenis perilaku yang melekat dalam hukum pidana transnasional bahkan lebih luas lagi bagi rezim pemberantasan kejahatan siber karena dua alasan: Pertama, rezim pemberantasan kejahatan siber tidak hanya mengatur ketergantungan siber sistem komputer sebagai objeknya, namun juga kejahatan *"cyber-enabled"* sistem komputer sebagai instrumennya. Kategori terakhir ini cenderung

memperluas jangkauan tindakan yang terkena sanksi secara signifikan, karena penggunaan teknologi informasi telah meningkat pesat selama dekade terakhir. Jika setiap orang menggunakan perbankan online, semua perilaku penipuan yang melibatkan transaksi bank akan dikategorikan sebagai kejahatan dunia maya dan dikendalikan oleh rezim penindasan kejahatan dunia maya. Kedua, berbeda dari bidang hukum pidana lainnya, kejahatan dunia maya dikategorikan berdasarkan alat yang digunakan atau objek yang menjadi sasaran yaitu sistem komputer. Sebaliknya, banyak penulis dan pembuat undang-undang mengkategorikan pelanggaran berdasarkan kepentingan hukum yang mereka lindungi, misalnya pelanggaran terhadap kebebasan pribadi (paksaan, penculikan, dll.) di satu sisi dan pelanggaran terhadap integritas fisik (penyerangan, dll.) di sisi lain. Pengkategorian ini mengakibatkan terbatasnya ruang lingkup larangan pidana dalam menafsirkan undang-undang. Misalnya, meludahi seseorang tidak dilarang dalam pelanggaran terhadap integritas fisik seperti penyerangan karena tidak menimbulkan kerugian fisik. Kemungkinan penafsiran restriktif ini hilang jika hukum pidana menggunakan kategori seperti *"cybercrime"* yang dibedakan berdasarkan instrumennya. digunakan atau objek yang dituju.

Karena tujuan utama hukum pidana transnasional adalah untuk mendorong kerja sama antarnegara dalam penyelidikan dan penegakan hukum, persyaratan hukum pidana substantif dan persyaratan hukum acara seringkali sangat terjerat dalam peraturan kejahatan dunia maya. Peraturan hukum pidana digitalitas global seperti Konvensi Kejahatan Dunia Maya biasanya tidak hanya mencakup persyaratan hukum pidana substantif. Mereka juga menetapkan standar hukum acara pidana, khususnya yang berkaitan dengan pengumpulan dan penyimpanan bukti elektronik, serta konflik yurisdiksi. Mengingat bahwa tujuan peraturan kejahatan dunia maya bukanlah untuk mencegah atau memberikan sanksi terhadap kerugian, melainkan untuk meningkatkan penegakan hukum antar negara bagian, peraturan tersebut sering kali memerlukan tindakan hukuman yang memajukan perilaku merugikan atau membahayakan tersebut agar negara dapat melakukan investigasi pada tahap awal. Misalnya, Konvensi Kejahatan Dunia Maya tidak hanya mensyaratkan kriminalisasi terhadap akses ilegal terhadap suatu sistem komputer, namun juga kepemilikan yang disengaja atas alat-alat yang dapat digunakan untuk mengakses sistem komputer secara ilegal. Sebagai konsekuensinya, terdapat banyak hambatan dalam upaya untuk melakukan kejahatan siber. memulai investigasi jauh lebih rendah. Menurut prinsip hukum pidana, bukti awal yang cukup bahwa seseorang melakukan kejahatan harus ada sebelum aparat penegak hukum diizinkan untuk melakukan penyelidikan. Mengkriminalisasi kepemilikan alat peretas meniadakan kebutuhan akan bukti bahwa mereka benar-benar mengakses sistem komputer untuk memulai penyelidikan. Bukti bahwa tersangka hanya memiliki alat hacking di komputer saja sudah cukup.

Hampir semua peraturan kejahatan dunia maya yang ada tidak hanya mencakup pelanggaran akses dan penggunaan tetapi juga pelanggaran konten yaitu perkataan kebencian online seperti misalnya Protokol Tambahan pada Konvensi Kejahatan Dunia Maya tahun 2003. Pelanggaran konten lebih sulit untuk dibenarkan dibandingkan dua kategori pelanggaran pertama, karena pelanggaran tersebut mempengaruhi hak konstitusional atas

kebebasan berpendapat dari pembicara. Rezim pemberantasan kejahatan dunia maya jarang memasukkan hak-hak prosedural tersangka meskipun pada kenyataannya rezim tersebut biasanya menetapkan pedoman untuk investigasi, penegakan hukum, dan konflik yurisdiksi yang mempengaruhi hak-hak tersebut. Alasan tidak diberikannya hak-hak tersangka mungkin karena rezim penindasan sangat fokus pada peningkatan efisiensi penuntutan pidana dalam situasi lintas batas. Namun efisiensi tersebut mungkin terhambat oleh hak-hak tersangka yang kuat dan dapat ditegakkan.

Singkatnya, hukum pidana digitalitas global memiliki beberapa karakteristik yang membedakannya dari bidang hukum pidana lainnya. Hukum pidana digitalitas global adalah hukum transnasional. Konvensi ini menyerukan negara-negara untuk menetapkan kejahatan tertentu dalam hukum pidana nasional mereka untuk meningkatkan kerja sama antarnegara. Secara khas, peraturan ini melarang berbagai perilaku di luar perilaku lintas negara, di luar perlindungan kepentingan hukum tertentu, di luar kejahatan yang bergantung pada dunia maya, dan khususnya di luar tindakan yang secara langsung menyebabkan kerugian. Hal ini juga ditandai dengan adanya keterikatan yang kuat antara hukum pidana substantif dan prosedural, namun biasanya tidak memberikan perlindungan bagi tersangka.

Kelemahan Hukum Pidana Digitalitas Global Saat Ini

Meskipun banyak perhatian akademis telah diberikan pada terkikisnya hak-hak tersangka (di masa depan) dalam peraturan kejahatan dunia maya, kebebasan individu yang dibatasi oleh larangan kejahatan dunia maya (hukum pidana substantif) relatif diabaikan. Oleh karena itu, kontribusi kali ini berkonsentrasi pada aspek kelemahan hukum pidana digitalitas global saat ini.

Karena sebagian besar hukum pidana digitalitas global pada dasarnya adalah hukum transnasional, kedua konsep tersebut memiliki sejumlah kelemahan yang sama. Tujuan utama dan nilai utama dari hukum transnasional adalah untuk mengambil langkah-langkah yang lebih efektif untuk menekan kejahatan transnasional. Pendekatan seperti ini tidak berfokus pada kepentingan hukum yang harus dilindungi oleh hukum pidana atau pada kebebasan individu yang dibatasi oleh hukum pidana. larangan. Tujuannya justru pragmatis: untuk menjalankan sistem pengendalian yang berfungsi dengan baik terhadap perilaku menyimpang. Dengan tujuan ini, mendekriminalisasi bidang kejahatan transnasional tertentu, seperti penggunaan ganja untuk rekreasi atau beberapa bentuk peretasan, menjadi hampir mustahil. Hal ini sangat meresahkan, karena hukum pidana transnasional pada umumnya mencakup kejahatan mala larangan, yang berarti pelanggaran peraturan yang kesalahannya berasal dari pelanggaran peraturan berdasarkan kebijakan negara tertentu. Hukum pidana transnasional cenderung mengkriminalisasi aktivitas-aktivitas yang disebutkan semata-mata demi kepentingan pengendalian kejahatan yang efektif. Misalnya, Konvensi Kejahatan Dunia Maya mewajibkan kriminalisasi terhadap pelanggaran hak cipta, meskipun hak cipta mungkin sudah dilindungi dengan upaya hukum perdata (kerusakan, putusan sela ganti rugi, dll.).

Selain itu, hukum pidana transnasional seringkali memperluas cakupan pertanggungjawaban pidana. Konvensi ini secara rutin menyerukan untuk mengkriminalisasi

tidak hanya pelanggaran-pelanggaran kecil seperti percobaan percobaan, namun juga tindakan persiapan dan permulaan yang tidak segera dilakukan dan belum tentu menimbulkan kerugian (misalnya pelanggaran kepemilikan barang-barang yang dianggap berbahaya seperti obat-obatan terlarang, senjata atau alat peretasan). Misalnya, Konvensi Kejahatan Dunia Maya serta Petunjuk mengenai serangan terhadap sistem informasi menyerukan kriminalisasi atas kepemilikan alat yang dapat digunakan ketika melakukan pelanggaran dunia maya lainnya. Tindak pidana preventif seperti ini membatasi kebebasan hingga tingkat yang lebih besar dibandingkan dengan tindak pidana tradisional yang memberikan sanksi atas kerugian yang ditimbulkan atau membahayakan. Tindak pidana preventif menurunkan ambang batas penuntutan secara signifikan. Bahkan pelanggaran yang masih kecil pun biasanya memerlukan niat untuk menimbulkan kerugian yang terbatas dan langkah-langkah substantif untuk mencapai tujuan tersebut. Pelanggaran pidana preventif sering kali tidak memerlukan langkah lebih lanjut untuk merugikan seseorang dan seringkali bahkan tidak ada niat untuk melakukannya. Misalnya, Konvensi Kejahatan Dunia Maya menyerukan kriminalisasi peretasan komputer namun tidak mensyaratkan unsur-unsur kejahatan lebih lanjut, seperti pelanggaran langkah-langkah keamanan atau niat untuk mencuri data. Hal ini mengarah pada kriminalisasi peretasan untuk hiburan atau sebagai bentuk protes di beberapa Negara Anggota dan sangat membatasi hak-hak peretas yang seringkali tidak memiliki niat jahat tetapi "meretas" hanya untuk bersenang-senang atau untuk meningkatkan kesadaran akan defisit dalam pengukuran keamanan, perlindungan data dan sejenisnya.

Hukum transnasional membatasi kedaulatan dan pemerintahan mandiri yang demokratis. Negara menganggap hukum pidana sebagai ekspresi kedaulatannya. Tindakan kriminalisasi sangat membatasi kebebasan di bidang-bidang tertentu. Hukum pidana merupakan sarana kontrol sosial yang seringkali sangat terkait dengan preferensi budaya dan keyakinan. Oleh karena itu, hukum pidana merupakan salah satu bidang hukum yang khususnya menuntut perdebatan dan pengambilan keputusan yang demokratis. Namun demikian, perkembangan hukum pidana transnasional masih belum transparan dan didominasi oleh para ahli teknis hukum di tingkat internasional. Masyarakat seringkali hanya memiliki sedikit pengetahuan dan pendapat dalam pengembangan norma atau mekanisme, sebuah fakta yang sering diabaikan oleh badan legislatif dalam negeri yang mengubah kewajiban perjanjian internasional menjadi hukum domestik. Sejarah Konvensi Kejahatan Dunia Maya patut dicontoh karena kurangnya partisipasi demokratis dalam penyusunannya. Konvensi ini dirancang mulai tahun 1997 oleh kelompok ahli Dewan Eropa yang beranggotakan jaksa, hakim dan peneliti hukum pidana dengan keahlian di bidang kejahatan dunia maya. namun tidak menyertakan perwakilan yang dipilih secara demokratis. Peluncuran pertama rancangan perjanjian tersebut dilakukan dalam versinya yang ke-19 tidak lama sebelum rancangan tersebut diselesaikan oleh Komite Menteri dan dibuka untuk ditandatangani. Hal ini menyisakan sedikit waktu yang berharga untuk debat publik yang dapat mempengaruhi isinya. Konvensi ini mewajibkan negara-negara pihak yang meratifikasinya untuk memasukkan kejahatan-kejahatan yang disyaratkan termasuk

pelanggaran-pelanggaran preventif ke dalam hukum domestik mereka tanpa adanya kemungkinan perdebatan terbuka mengenai ruang lingkup kejahatan-kejahatan tersebut.

Defisit demokrasi menjadi sangat meresahkan ketika kebijakan-kebijakan tersebut dialihkan dari negara-negara maju ke negara-negara berkembang. Seringkali negara-negara berkembang tidak berpartisipasi secara aktif dalam penyusunan konvensi transnasional, seperti yang terjadi pada Konvensi Kejahatan Dunia Maya. Dalam kebanyakan kasus, mereka hanya dapat memilih untuk menandatangani perjanjian yang telah ditetapkan (sebagai negara prioritas dalam program GLACY). Sebagai konsekuensinya, baik situasi khusus maupun struktur hukumnya tidak dipertimbangkan. Misalnya saja, dalam kaitannya dengan kejahatan dunia maya, negara-negara berkembang sering kali menjadi eksportir dibandingkan importir kejahatan, yang berujung pada pelarangan yang membatasi kebebasan lebih banyak orang di negara berkembang dibandingkan di negara maju. Misalnya, Petunjuk ECOWAS tentang Memerangi Kejahatan Dunia Maya (Cybercrime Directive on Fighting Cybercrime) dimulai karena beberapa Negara Anggota telah menjadi sumber utama penipuan email dan penipuan biaya di muka di seluruh dunia. Dalam kasus ini pelakunya sebagian besar adalah penduduk negara-negara Afrika Barat sedangkan korbannya adalah penduduk negara-negara Eropa atau Amerika Serikat.

Dengan kecenderungannya yang melampaui batas seperti yang digambarkan, hukum pidana transnasional mengancam akan sangat membatasi kebebasan individu. Oleh karena itu, hal ini menimbulkan pertanyaan mengenai pembenaran, namun hal ini hanya memainkan peran kecil dalam proses negosiasi perjanjian. Rezim penindasan tidak memberikan banyak perhatian pada kebebasan yang terkena dampak karena tujuan utama mereka adalah pengendalian kejahatan yang efektif. Bahkan sehubungan dengan individu yang terkena dampak penegakan hukum, mereka biasanya bergantung pada kewajiban hak asasi manusia yang ada, yang berarti bahwa perlindungan individu bergantung pada tingkat perlindungan hak asasi manusia yang terjadi di negara-negara yang terlibat (misalnya, ketentuan hak yang dapat ditegakkan). Masalahnya pembenaran diperkuat karena permasalahan teoritik pembatasan hukum pidana preventif. Jika prinsip pembatasnya adalah menyeimbangkan keamanan dengan kebebasan, undang-undang tersebut dapat dengan mudah dibenarkan dengan menyatakan bahwa keamanan bagi banyak orang melebihi kebebasan individu bagi segelintir orang.

Ancaman terhadap kebebasan individu merupakan keberatan penting terhadap undang-undang kejahatan dunia maya. Pelanggaran terkait konten merupakan bagian penting dari pelanggaran kejahatan dunia maya. Oleh karena itu, potensi ancaman terhadap kebebasan berekspresi dan penggunaan kejahatan dunia maya sebagai sarana sensor dan kontrol negara telah menjadi sumber kekhawatiran. Lebih dari separuh negara pihak Konvensi termasuk pemain besar seperti Amerika Serikat belum menandatangani atau meratifikasi Protokol Tambahan mengenai kriminalisasi tindakan yang bersifat rasis atau xenofobia yang dilakukan melalui sistem komputer karena mereka menganggap persyaratannya bertentangan dengan persyaratan yang ada. hak konstitusional mereka atas kebebasan berpendapat. Pasal 15(1) Konvensi Kejahatan Dunia Maya merefleksikan hal ini

dan meminta penerapannya agar memenuhi standar hak asasi manusia dan proporsionalitas. Namun, membatasi standar perlindungan dalam undang-undang domestik dan perjanjian internasional berarti bahwa pembatasan ini hanya akan berdampak pada efektif di negara-negara yang memiliki standar serupa dalam kode hukumnya.

Kelemahan lain dari undang-undang kejahatan dunia maya saat ini adalah fokus pada cara dan objek kejahatan (sistem komputer). Dari sudut pandang ini, kepentingan hukum yang harus dilindungi serta kebebasan individu yang terkena dampaknya tidak begitu mendapat perhatian. Diskusi berpusat pada pertanyaan-pertanyaan seperti bagaimana teknologi baru dan cara-cara baru dalam penggunaan yang berbahaya diintegrasikan ke dalam sistem kendali. Konvensi Kejahatan Dunia Maya, misalnya, sering dikritik karena tidak bisa mengimbangi pesatnya perkembangan teknologi informasi (misalnya perkembangan jaringan sosial dan munculnya masalah komunikasi di jaringan sosial seperti cyberbullying). Kritik ini mengarah pada untuk menyerukan agar semakin banyak tindakan kriminalisasi. Seringkali terabaikan bahwa larangan-larangan baru membatasi kebebasan individu dan bahwa masalah-masalah seperti cyberbullying adalah masalah-masalah sosial yang sebaiknya ditangani melalui respon sosial.

Kesimpulan

Lawrence Lessig menyatakan pada awal tahun 1996 “bahwa ada keputusan yang harus dibuat mengenai arsitektur dunia maya nantinya, dan pertanyaannya adalah bagaimana keputusan tersebut akan dibuat. Atau lebih baik lagi, dimana keputusannya akan diambil”. Jawaban yang diberikan oleh pemerintah terlalu cepat tanpa adanya debat publik dan partisipasi demokratis karena adanya ancaman mendesak di “dunia maya” dan meningkatnya biaya penuntutan pidana. Kebebasan individu dikesampingkan. Hanya jika sudah jelas kebebasan mana yang dibatasi oleh larangan pidana maka akan ada standar untuk mengidentifikasi kriminalisasi berlebihan yang banyak terdapat dalam undang-undang kejahatan dunia maya yang hanya mencakup pelanggaran kepemilikan, pelanggaran akses tanpa maksud untuk menimbulkan kerugian, pelanggaran konten, dan sebagainya. Kini saatnya memikirkan alternatif terhadap larangan pidana sebagai respons terhadap aktivitas siber yang berbahaya. Masalah sosial harus diatasi dengan strategi pencegahan sosial termasuk peningkatan kesadaran dan promosi mekanisme pencegahan sederhana yang akan mencegah sebagian besar kasus kejahatan dunia maya.

DAFTAR PUSTAKA

A. S. Verghese, “Competition Policy in Globalized, Digitalized Economy,” World Economic Forum 91-93 route de la Capitale CH1223, 2019

Aditya Nugraha, Rifha. (2018). Pelindungan Data Pribadi dan Privasi Penumpang Maskapai Penerbangan Pada Era Big Data, Jurnal Mimbar Hukum, Vol. 30 No. 2.

Agustina, M. (2020). Persaingan Usaha Tidak Sehat Antar Online Shop DalamKondisi Covid-19 Terhadap Kebijakan Yang Dikeluarkan Oleh Presiden. ResJudicata, 3(1), 15-25.

Anjarningtyas, MC. 2022. TANGGUNG JAWAB ENDORSER ATAS KERUGIAN KONSUMEN AKIBAT PENGGUNAAN PRODUK ENDORSEMENT. Jurnal Ilmiah Ilmu Hukum, 28(4), 3690-3695.

Ansori, Aan. (2016). Digitalisasi Ekonomi Syariah, Jurnal Ekonomi Keuangan dan Bisnis Islam, Vol. 7 No. 1.

Aprita, Serlika&Adhitya, Rio. 2020. Hukum PerdaganganInternasional. Depok :Rajawali Pers,

Arief, E. (2020). Politik Hukum PerjanjianInternasional Masyarakat Ekonomi Asean Di Era Globalisasi. Jurnal JURISTIC, 1(02), 237-249.

Burhan, FA. 2022. “ Kominfo: Hacker Incar Sistem E-Commerce dan Instansi Pemerintah”. https://katadata.co.id/desysetyowati/digital/61f290348fbcc/kominfo-hacker-incar-sistem-e-commerce-dan-instansi-pemerintah. Diakses tanggal 24 Maret 2022.

Chen, Y. (2020). Improving market performance in the digital economy. ChinaEconomic Review, 62, 101482.

CNN Indonesia. 2021. “Konsumen Belanja Online RI Melonjak 88 Persen pada 2021”. https://www.cnnindonesia.com/ekonomi/20211229141536-92-740093/konsumen-belanja-online-ri-melonjak-88-persen-pada-2021. Diakses tanggal 25 Maret 2022.

D. Hendarsyah, “E-Commerce Di Era Industri 4.0 Dan Society 5.0,” vol. 8, pp. 171–184, 2019.

Dewi, Sinta. (2016). Konsep Pelindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing di Indonesia, Jurnal Yustisia, Vol.5 No. 1.

Dewi, Sinta. (2018). Pelindungan Privasi dan Data Pribadi Dalam Era Ekonomi Digital di Indonesia, Jurnal Vej, Volume 4 No. 1.

Efendi, S. (2020). The Role of Human Capital in the Education Sector in Efforts toCreate Reliable Organizational Human Resources. International Journal of Science and Society, 2(1), 405-413.

Efendi, S., Sugiono, E., Guritno, E., Sufyati, & Hendryadi. (2020). Building innovationand competitiveness for low technology manufacturing SMEs through imitatingcapability and learning: The case of Indonesia. Cogent Social Sciences, 6(1), 1803515.

European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law, Belgium, 2014.

Greeneaf, Graham, Asian Data Privacy Laws - Trade and Human Rights Perspectives, Oxford University Press, New York, 2014.

Hendarsyah, D. 2019. E-COMMERCEDI ERA INDUSTRI 4.0 DAN SOCIETY 5.0. Jurnal Ilmiah Ekonomi Kita, 8(2), 176-177.

Indonesia, Undang-Undang No. 10 Tahun 1998 tentang Perbankan. Undang-Undang Nomor 10, LN No. 182 Tahun 1998. TLN. No. 3790.

Indonesia, Undang-Undang No. 14 Tahun 2008 tentang Keterbukaan Informasi Publik, Undang-Undang Nomor 14, LN No. 61 Tahun 2008. TLN. No. 4846.

Indonesia, Undang-Undang No. 19 Tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 19, LN No. 251 Tahun 2016. TLN. No. 5952.

Indonesia, Undang-Undang No. 24 Tahun 2013 tentang Perubahan Atas Undang – Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan. Undang-Undang Nomor 24, LN No. 232 Tahun 2013. TLN. No.5475.

Indonesia, Undang-Undang No. 36 Tahun 2009 tentang Kesehatan. Undang-Undang Nomor 36, LN No. 144 Tahun 2009. TLN. No. 5063.

Indonesia, Undang-Undang No. 44 Tahun 2009 tentang Rumah Sakit. Undang-Undang Nomor 44, LN No. 153 Tahun 2009. TLN. No. 5072.

Indonesia, Undang-Undang No. 8 Tahun 1999 tentang Pelindungan Konsumen. Undang – Undang Nomor 8, LN No. 42 Tahun 1999. TLN. No. 3821.

Indriyani, Masitoh. dkk. (2017). Pelindungan Privasi dan Data Pribadi Konsumen Daring Pada Online Marketplace System, Justitia Jurnal Hukum, Vol.1, No. 2.

Mazli, A. 2021. Urgensi Pembaharuan Undang-Undang Perlindungan Konsumen Indonesia Di Era E-Commerce. Jurnal LEX Reinassance, 6(2), 298-312.

Musyafah, AA. et, al. 2018. PERLINDUNGAN KONSUMEN JASA PENGIRIMAN BARANG DALAM HAL TERJADIKETERLAMBATAN PENGIRIMAN BARANG. Jurnal Law Reform, 14(2), 153-157.

Nata, KDR. et, al. 2022. PERLINDUNGAN HUKUM ATAS KEBOCORAN DATA PRIBADI KONSUMEN PADA PERDAGANGAN ELEKTRONIK LOKAPASAR (MARKETPLACE). Jurnal Preferensi Hukum, 3(1), 143-148.

Novita, YD. 2021. Urgensi Pembaharuan Regulasi Perlindungan Konsumen di Era Bisnis Digital. Jurnal Pembangunan Hukum Indonesia, 3(1), 46-58.

Nugrahaningsih, W. 2017. Implementasi Undang -Undang Nomor 8 tahun 1999 tentang Perlindungan Konsumen Terhadap Bisnis Online. Jurnal Serambi Hukum, 11(1), 30-32.

P. Akman, “An Agenda for Competition Law and Policy in the Digital Economy,” Journal of European Competition Law & Practice, vol. 10, 2019.

Pujianto, Agung.dkk. (2018). Pemanfaatan Big Data dan Pelindungan Privasi Konsumen di Era Ekonomi Digital, Majalah Ilmiah Bijak, Vol. 15 No. 2.

Putri, AD. 2022. “Perlindungan Hukum atas Kebocoran Data Pribadi Konsumen pada E-Commerce”. https://heylawedu.id/blog/perlindungan-hukum-atas-kebocoran-data-pribadi-konsumen-pada-e-commerce. Diakses tanggal 24 Maret 2022.

Republik Indonesia. 1999. Undang-undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Jakarta: Badan Pemeriksa Keuangan.

Republik Indonesia. 2008. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Jakarta: Badan Pemeriksa Keuangan.

Republik Indonesia. 2016. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Jakarta: Badan Pemeriksa Keuangan.

Rustam, Muhammad. (2017). Internet dan Penggunaannya (Survei di Kalangan Masyarakat Kabupaten Talakar Provinsi Sulawesi Selatan), Jurnal Studi Komunikasi dan Media, Vol. 21 No. 1.

Santoso, R., Munawi, H. A., & Nevita, A. P. (2020). Analisa Perilaku Konsumen: Strategi Memenangkan Persaingan Bisnis di Era Ekonomi Digital. Jurnal G- Tech, 4(1), 286-293.

Sautunnida, Lia. (2018). Urgensi Undang-Undang Pelindungan Data Pribadi di Indonesia Studi Perbandingan Hukum Inggris dan Malaysia, Kanun Jurnal Ilmu Hukum, Vol. 20 No. 2.

Sawitri, D. 2019. Revolusi Industri 4.0 : Big Data Menjawab Tantangan Revolusi Industri 4.0. Jurnal Ilmiah Maksitek, 4(3), 1-3.

Simanullang, HN. 2017. Perlindungan Hukum terhadap Konsumen dalam Transaksi ECommerce. Melayunesia Law, 1(1), 122.

T. Wu and S. Thompson, “Tim Wu and Stuart A. Thompson, 2021, The Roots of Big Tech Run Disturbingly Deep, Washingtonpost, USA.,” Washington Post, USA, 2021.

Thomas M. Lenard, Daniel B. Britton, et.al., The Digital Economy Fact Book, The Progress & Freedom Foundation Washington, D.C., 2006.

Tobing, CI. dan Fitriana, D. 2022. URGENSI PERLINDUNGAN DATA PRIBADI DALAM TRANSAKSI ONLINE (E-COMMERCE). Jurnal Pengabdian Kepada Masyarakat, 2(1), 76-78.

Tumbel, TGM. 2020. Perlindungan Konsumen Jual Beli Online Dalam Era Digital. Lex Et Societatis, VIII(3), 93-98.

Wu, F. ‘How Neoliberal is China’s Reform? The Origins of Change during Transition’, Eurasian Geography and Economics, 51 (5),(2010), pp.619-631.

Wu, J. and Zhang, Y. 'Xi proposes a 'new Silk Road' with Central Asia', China Daily, 2013 Yahuda, M. The International Politics of the Asia-Pacific. 3rd edn. New York: Routledge, 2011.

Hukum di Era Globalisasi Digital

Dr. Agus Wibowo, M.Kom, M.Si, MM

BIO DATA PENULIS

Penulis memiliki berbagai disiplin ilmu yang diperoleh dari Universitas Diponegoro (UNDIP) Semarang. dan dari Universitas Kristen Satya Wacana (UKSW) Salatiga. Disiplin ilmu itu antara lain teknik elektro, komputer, manajemen dan ilmu sosiologi. Penulis memiliki pengalaman kerja pada industri elektronik dan sertifikasi keahlian dalam bidang Jaringan Internet, Telekomunikasi, Artificial Intelligence, Internet Of Things (IoT), Augmented Reality (AR), Technopreneurship, Internet Marketing dan bidang pengolahan dan analisa data (komputer statistik).

Penulis adalah pendiri dari Universitas Sains dan Teknologi Komputer (Universitas STEKOM) dan juga seorang dosen yang memiliki Jabatan Fungsional Akademik Lektor Kepala (Associate Professor) yang telah menghasilkan puluhan Buku Ajar ber ISBN, HAKI dari beberapa karya cipta dan Hak Paten pada produk IPTEK. Penulis juga terlibat dalam berbagai organisasi profesi dan industri yang terkait dengan dunia usaha dan industri, khususnya dalam pengembangan sumber daya manusia yang unggul untuk memenuhi kebutuhan dunia kerja secara nyata.

YAYASAN PRIMA AGUS TEKNIK

PENERBIT :
YAYASAN PRIMA AGUS TEKNIK
JL. Majapahit No. 605 Semarang
Telp. (024) 6723456. Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

ISBN 978-623-8120-72-7 (PDF)
9 786238 120727

Dr. Agus Wibowo, M.Kom, M.Si, MM

Hukum di Era Globalisasi Digital

YAYASAN PRIMA AGUS TEKNIK

PENERBIT :
YAYASAN PRIMA AGUS TEKNIK
JL. Majapahit No. 605 Semarang
Telp. (024) 6723456. Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id