Barelang Journal of Legal Studies
Volume 2 Issue 1 (March 2024), pp. 73-87
ISSN (Online): 3026-3182
Published by Universitas Internasional Batam, Indonesia

Komersialisasi Data dalam Politik Hukum Keamanan Siber

Justitia Ferryanto[1*], David Tan[1], Ampuan Situmeang[1], Risno Mina[2], Khilmatin Maulidah[3]
*Corresponding Author: 2252044.justitia@uib.edu

Received: 21-12-2023
Revised: 24-1-2024
Accepted: 22-2-2024

Citation:
Ferryanto, J., Tan, D., Situmeang, A., Mina, R., & Maulidah, K. (2023). Komersialisasi Data dalam Politik Hukum Keamanan Siber. *Barelang Journal of Legal Studies*, 2(1), 73-87.

ABSTRAK

Komersialisasi data merupakan isu yang relevan dalam upaya peningkatan taraf keamanan siber di era revolusi industri 4.0, yang harus diakomodasi secara hukum untuk memastikan pemanfaatan teknologi informasi yang baik dan tidak merugikan pemilik data. Penelitian ini bertujuan untuk mendalami posisi isu komersialisasi hukum Indonesia di tengah upaya pemerintah dalam mengembangkan kerangka hukum keamanan siber. Dengan metode penelitian hukum normatif, penelitian ini menganalisis hukum positif yang berlaku di Indonesia, dengan perspektif teori hukum responsif dan teori hukum murni. Analisis penelitian ini menemukan bahwa politik hukum keamanan siber di Indonesia masih belum dapat mengakomodasi isu komersialisasi data, dan tidak memiliki arah yang jelas. Analisis juga menemukan bahwa pemerintah kerap tidak konsisten dalam memperbaiki permasalahan normatif di setiap kerangka hukum keamanan siber yang disahkan.

Keta Kunci: Keamanan Siber; Komersialisasi Data; Politik Hukum
DOI: https://doi.org/10.37253/barjoules.v2i1.10182

PENDAHULUAN

Di era revolusi industri 4.0, data merupakan aset berharga bagi banyak pihak (Vassakis et al., 2018). Kemajuan teknologi informasi memungkinkan pengumpulan, penyimpanan, dan

[1] Faculty of Law, Universitas Internasional Batam, Indonesia
[2] Faculty of Law, Universitas Muhammadiyah Luwuk, Indonesia
[3] Sekolah Tinggi Ilmu Hukum IBLAM, Indonesia

analisis data dalam skala yang besar, sekaligus memberikan peluang besar bagi inovasi dan pertumbuhan ekonomi. Di sisi lain, komersialisasi data juga membawa tantangan baru dalam hal keamanan dan privasi (Durovic & Lech, 2021) Di tengah dinamika ini, Indonesia, sebagai negara dengan potensi besar di era revolusi industri 4.0, harus menghadapi tantangan untuk menyeimbangkan potensi pemanfaatan data dan memastikan keamanan siber bagi pengguna berbagai teknologi informasi yang terdapat di ruang-ruang digital di Indonesia. Perkembangan yang dibawa oleh revolusi industri 4.0 inilah yang menjadikan keamanan siber sebagai agenda penting dalam politik hukum Indonesia belakangan ini (Simorangkir, 2021) Pemerintah Indonesia telah menginisiasikan beberapa langkah untuk memperkuat kerangka hukum dan kebijakan terkait keamanan siber, dengan mengembangkan kerangka hukum yang sudah ada dan memperkenalkan pengaturan baru. Sebagai salah satu faktor yang mempengaruhi keamanan siber, sayangnya komersialisasi data dapat dikatakan sebagai konsep yang belum lama berkembang, sehingga masih membutuhkan analisis hukum yang lebih mendalam. Selain itu, komersialisasi data juga pada hakikatnya bersifat interdisipliner, dengan mencakup aspek hukum, teknologi, dan bisnis, sehingga analisis mengenai fenomena ini tersebar di berbagai departemen akademik dan tidak hanya terpusat pada ranah hukum saja.

Secara konseptual, keamanan siber semakin mendapat perhatian seiring dengan berkembangnya berbagai teknologi yang mendorong ketergantungan pada teknologi *cloud*, dalam proses berkomunikasi dan berbagi data melalui jaringan digital (Wylde et al., 2022) Budaya berbagi data yang terus berkembang ini kemudian menimbulkan kesadaran akan nilai data, yang pada akhirnya mendorong berbagai bentuk komersialisasi data (Cole et al., 2021) Sebuah studi komparatif yang menjabarkan pengaturan mengenai data di Amerika Serikat dan Uni Eropa menemukan bahwa Amerika Serikat dalam membuat pengaturan terkait komersialisasi data lebih berfokus kepada upaya meminimalkan *trade-off* yang dari manfaat sosio-ekonomi dari komersialisasi data, yang memberikan ruang normatif lebih luas bagi Amerika Serikat untuk memperhatikan aspek keamanan siber. Pendekatan ini berbeda dengan yang diterapkan oleh Uni Eropa, yang lebih berfokus kepada hak fundamental seperti privasi dan perlindungan data pada umumnya, yang memberikan perlindungan lebih terhadap pengguna berbagai teknologi informasi (Guay & Birch, 2022) Di Indonesia sendiri isu komersialisasi data belum banyak didalami, meskipun kerap disinggung dalam analisis terkait kerangka hukum perlindungan data pribadi

(Kurnianingrum, 2020) Terdapat kesenjangan penelitian dalam ranah hukum terkait keamanan siber dalam konteks komersialisasi data, khususnya dalam pengembangan hukum di Indonesia.

Melalui metode penelitian hukum normatif dan pendekatan perundang-undangan, penelitian ini menganalisis hukum positif yang berlaku di Indonesia. Penelitian ini menggunakan data sekunder dalam bentuk sumber hukum primer, antara lain UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, UU No. 19 Tahun 2016 tentang Perubahan atas UU No. 11 Tahun 2008, Permenkominfo No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, dan UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi. Pisau analisis yang digunakan untuk mendalami pembahasan penelitian ini adalah teori hukum responsif dan teori hukum murni. Teori hukum responsif menekankan interaksi dinamis antara hukum dan masyarakat, memfasilitasi pemahaman tentang evolusi hukum berdasarkan kebutuhan sosial. Di sisi lain, positivisme hukum menawarkan pendekatan objektif dengan fokus pada hukum yang ada, dengan mendorong analisis yang terstruktur dan pemisahan antara hukum dan moral. Kombinasi kedua teori ini memberikan kerangka analisis komprehensif untuk menganalisis isu komersialisasi data dalam politik hukum keamanan siber di Indonesia, dengan mempertimbangkan aspek teoretis dan praktis hukum.

METODE PENELITIAN

Metode penelitian ini menggunakan pendekatan normatif dengan fokus pada pendekatan perundang-undangan dan pendekatan konseptual (Disemadi, 2022). Pendekatan perundang-undangan dilakukan dengan menganalisis berbagai peraturan yang mengatur komersialisasi data dan keamanan siber, baik di tingkat nasional maupun internasional. Analisis ini mencakup Undang-Undang Perlindungan Data Pribadi, peraturan keamanan siber, serta kebijakan global seperti *General Data Protection Regulation* (GDPR). Pendekatan ini bertujuan untuk memahami sejauh mana regulasi yang ada memberikan perlindungan hukum terhadap komersialisasi data dalam konteks keamanan siber. Pendekatan konseptual digunakan untuk mengkaji relevansi teori hukum dalam membangun politik hukum yang sesuai dengan perkembangan teknologi (Disemadi, 2022). Dalam hal ini, Teori Hukum Responsif dianalisis untuk menilai bagaimana regulasi dapat disesuaikan dengan kebutuhan masyarakat dan perubahan teknologi, sementara

Teori Hukum Murni digunakan untuk menilai aspek normatif regulasi dengan pendekatan yang lebih formal dan sistematis. Pengumpulan data dilakukan melalui studi pustaka, yang mencakup bahan hukum primer seperti undang-undang dan peraturan terkait, serta bahan hukum sekunder berupa literatur akademik, jurnal ilmiah, dan buku yang membahas teori hukum dan keamanan siber. Analisis data dilakukan secara yuridis-kualitatif dengan mengevaluasi peraturan yang ada dan menghubungkannya dengan teori hukum yang relevan. (Tan, 2021)

DISKUSI DAN ANALISIS

Relevansi Komersialisasi Data dalam Konteks Keamanan Siber

Dalam era digital saat ini, data telah menjadi komponen sentral dalam perekonomian global. Setiap interaksi yang dilakukan di dunia maya menghasilkan data yang, jika dikelola dengan benar, dapat memberikan wawasan berharga bagi perusahaan dan individu. Komersialisasi data, yaitu praktik memanfaatkan data untuk tujuan komersial, telah menjadi isu yang penting di tengah era revolusi industri 4.0 yang semakin banyak memanfaatkan data di berbagai bentuk teknologi informasi (González Chávez et al., 2023) Komersialisasi data semakin relevan seiring dengan meningkatnya penggunaan teknik pengumpulan dan analisis data dalam volume yang besar, seperti *Big Data Analytics* (Durovic & Lech, 2021) Maka dari itu, komersialisasi data secara langsung mempengaruhi bagaimana standar keamanan dari suatu sistem elektronik harus diterapkan, dan bagaimana kerangka hukum dapat mengatur mengenai *legal compliance* agar meningkatkan keamanan dan integritas sistem elektronik tersebut dalam mengumpulkan, mengolah, dan memanfaatkan data.

Terdapat potensi risiko keamanan yang terkait dengan pengumpulan dan penyimpanan data dalam jumlah besar. Sebagai contoh, pertimbangan dapat diberikan pada bagaimana infrastruktur teknologi informasi mendukung penyimpanan data yang aman dan bagaimana protokol keamanan diterapkan untuk melindungi data dari berbagai upaya pengaksesan tidak sah. Akses terhadap data secara tidak sah ini juga dapat dilakukan dalam berbagai baca melalui serangan siber, seperti *spoofing*, *tampering*, *denial of service (DoS)*, *eavesdropping*, dan *traffic analysis*, (Hossain et al., 2019) Bentuk serangan-serangan siber seperti ini dapat mengancam integrasi dan

privasi data, karena dapat memungkinkan pihak yang tidak bertanggung jawab untuk memperoleh akses secara tidak sah, serta memberikan mereka kemampuan untuk mengubah, atau menyebarkan data tersebut untuk tujuan lain.

Kemudian, terdapat juga pertimbangan etika dalam komersialisasi data. Meskipun teknologi memungkinkan pengumpulan data dalam skala yang belum pernah terjadi sebelumnya, pertanyaannya adalah sejauh mana data tersebut dapat dan seharusnya digunakan untuk tujuan komersial. Komersialisasi data harus dapat dipertanggungjawabkan tujuannya, serta bagaimana data tersebut akan digunakan oleh pihak ketiga yang memperoleh data tersebut. Artinya, tingkat *legal compliance* yang diterapkan melalui kerangka hukum harus dapat mengikat semua pihak yang memperoleh akses terhadap data tersebut, untuk memastikan terjaganya kepentingan pemilik data, baik itu dari segi privasi atau untuk mencegah pencurian identitas untuk tujuan-tujuan yang dapat membahayakan kehidupan pemilik data tersebut. Secara umum, tujuan pemanfaatan dari komersialisasi data juga tidak boleh berlawanan dengan kepentingan dan ketertiban umum, yang dewasa ini dapat berpengaruh secara luas mengingat besarnya volume data yang dikomersialisasikan (Fini et al., 2018)

Selanjutnya, ada potensi untuk menggunakan data dalam cara yang dapat mempengaruhi opini publik atau perilaku konsumen. Sebagai contoh, bagaimana data digunakan dalam konteks pemasaran digital dan apakah ada potensi untuk manipulasi atau bias dalam penggunaan data tersebut. Pengaturan hukum dalam hal ini berfungsi untuk membatasi semua bentuk pemasaran digital, agar tidak mendorong masyarakat ke dalam perilaku konsumtif yang buruk bagi kepentingan dan ketertiban umum. Artinya, harus ada batasan yang dapat memastikan bahwa teknik pemasaran digital yang menggunakan volume data yang besar dapat memberikan penawaran dan sugesti kepada masyarakat mengenai produk yang relevan, tanpa memanipulasi persepsi masyarakat mengenai hal tertentu. Sebaliknya, segala bentuk manipulasi algoritma yang terdapat dalam berbagai macam teknik pemasaran digital, harus dapat digunakan untuk memberdayakan masyarakat sebagai konsumen dalam membuat keputusan yang lebih baik dan sesuai dengan kebutuhan (Darmody & Zwick, 2020) Hal ini juga dapat digunakan untuk meningkatkan kepercayaan konsumen terhadap data yang digunakan dalam suatu sistem elektronik, sekaligus meningkatkan keterlibatan masyarakat dalam perkembangan suatu pasar (Boldosova, 2019)

Namun, ada juga manfaat yang jelas dari komersialisasi data. Dengan analisis data yang tepat, ada potensi untuk meningkatkan efisiensi, mengoptimalkan strategi pemasaran, dan memberikan layanan yang lebih disesuaikan dengan kebutuhan pengguna, yang pada akhirnya dapat meningkatkan aktivitas ekonomi dan meningkatkan pemanfaatan potensi revolusi industri 4.0. Selain itu, data dapat digunakan untuk mendeteksi ancaman keamanan siber dan mengembangkan strategi mitigasi risiko (Mazumdar & Wang, 2018) Sebaliknya, pembuatan profil invasif dan analisis inferensial data yang tidak bisa diprediksi, yang dapat pada akhirnya membahayakan pemilik data, dapat menjadi ancaman besar dari pemanfaatan komersialisasi data, khususnya melalui metode *data sharing* (Wachter, 2018)

Pengaturan yang berkaitan dengan komersialisasi data pada umumnya berkaitan erat dengan izin *(permission)*, yang dikonseptualisasikan secara lebih umum melalui istilah *consent*, yang memiliki translasi Bahasa Indonesia yang sama. Dalam pandangan teori hukum murni, *permission* merupakan unsur normatif yang aneh, karena perannya sebagai operator normatif yang lemah. *Permission* nyatanya tidak mengikat seperti halnya kewajiban atau larangan, dan memberikan ruang untuk memilih. *Permission* hanya berperan membuka jalur tindakan dan tidak menutupnya. Logika natural positivisme dari izin *(permission)* inilah yang dapat dijadikan dasar untuk terus mengembangkan kerangka hukum yang sesuai, untuk menutupi kekurangan normatif dari izin pemanfaatan data di tengah maraknya praktik komersialisasi data, sehingga dapat memaksimalkan pemanfaatan berbagai bentuk teknologi di era revolusi industri 4.0, tanpa merugikan masyarakat.

Perkembangan Kerangka Hukum Keamanan Siber di Indonesia

Perkembangan berbagai bentuk teknologi di era revolusi industri 4.0 telah membawa berbagai bentuk peluang pertumbuhan ekonomi yang signifikan bagi Indonesia. Dengan potensi yang besar ini, Indonesia terus berkembang seiring meningkatnya penggunaan teknologi informasi yang ada, yang semakin terintegrasi dengan kehidupan sehari-hari masyarakat. Pengaturan mengenai transformasi digital yang terjadi di Indonesia dimulai dari kesadaran mengenai potensi teknologi digital, yang ditandai dengan disahkannya UU No. 21 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU) sebagai *cyber law* perdana di Indonesia.(Rohmy et al., 2021) Sebagai pengaturan ruang digital *(cyber space)* pertama di sistem hukum Indonesia, UU

ITE historisnya merupakan hasil penggabungan RUU Tindak Pidana Teknologi Informasi dan RUU *e-commerce* pada 2003. RUU ini terbagi menjadi dua bagian utama: *e-commerce*, yang mencakup pasar digital, nama domain, dan tanda tangan elektronik; serta kejahatan teknologi informasi, yang mencakup konten ilegal, akses ilegal, ujaran kebencian, fitnah, intersepsi ilegal, dan gangguan data (Hadiyati & Stathany, 2021)

Namun, perlu digarisbawahi bahwa peraturan perundang-undangan yang cakupannya cukup luas ini masih memiliki beberapa kekurangan normatif. Dari sudut pandang keamanan siber, peraturan perundang-undangan ini justru tidak mengatur mengenai keamanan sistem elektronik, meskipun menyebutkan keamanan tanda tangan elektronik dalam Pasal 14 huruf c. Bertolak belakang dengan pengaturan yang cukup bersifat umum dalam konteks sistem informasi elektronik, UU ITE justru tidak menegaskan secara normatif hak-hak apa saja yang dimiliki oleh pemilik data, khususnya mengenai keamanan data pribadinya. Dalam konteks hukum responsif, tuntutan hak dipahami sebagai peluang untuk mengungkap kelainan atau malafungsi yang terdapat dalam masyarakat, dan karenanya dapat dinilai sebagai sumber daya administratif.

Pentingnya pengaturan yang secara eksplisit menyebutkan hak semakin relevan di tengah maraknya praktik komersialisasi data, yang sejatinya menimbulkan urgensi klasifikasi data yang lebih kompleks dari pengakuan atas hak itu sendiri.(Y. Li, 2022) Dampak normatif dari permasalahan ini dapat terlihat dari pengaturan Pasal 40 dan 41 yang mengatur kewajiban pemerintah dalam memastikan terlaksananya pemanfaatan sistem informasi, sekaligus peran masyarakat. Kedua pasal ini tidak secara spesifik mengatur mengenai hak maupun kewajiban pemerintah, serta tidak adanya penjelasan lebih lanjut mengenai masyarakat sebagaimana yang dimaksud dalam Pasal 41.

Tidak hanya itu, UU ITE juga kerap disalahgunakan oleh sebagian orang, termasuk pemerintah, untuk membatasi kebebasan berpendapat. Melalui pengaturan Pasal 27 ayat (3), masyarakat kerap dibungkam dengan ancaman pencemaran nama baik, sehingga menurunkan minat masyarakat untuk berpikir kritis.(Fadilah Raskasih, 2021) Meskipun telah diperbarui melalui UU No. 19 Tahun 2016 tentang Perubahan atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, nyatanya permasalahan ini tidak dapat diselesaikan karena masih terdapat kekaburan normatif. Kemudian, pemerintah justru mencoba memperbaiki permasalahan ini dengan mengeluarkan Surat Keputusan Bersama Menkominfo RI, Jaksa Agung RI, dan Kepala

Polri tentang Pedoman Implementasi atas Pasal Tertentu dalam UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Sebagaimana Telah Diubah dengan UU No. 19 Tahun 2016 tentang Perubahan atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (SKB UU ITE). SKB ini bertujuan untuk memperjelas penerapan Pasal 27 ayat (3) dari UU ITE, untuk menjamin hak konstitusional seperti hak kebebasan berpendapat (Muldani, 2022) Dari perspektif hukum murni, dengan melepaskan konteks politik hukum, terdapat permasalahan normatif karena menunjukkan ketidakjelasan hierarki hukum. Berdasarkan teori hukum murni menjelaskan bahwa konflik hukum dapat dan harus diselesaikan melalui interpretasi, namun penekanan kejelasan hierarki hukum yang jelas merupakan usnur penting untuk mendukung interpretasi tersebut. UU ITE yang seharusnya diterapkan bersama peraturan pelaksana justru diterapkan berdasarkan SKB, yang dibuat hanya itu mengatur penafsiran dari suatu pasal yang dianggap bermasalah.

Selanjutnya, pemerintah mencoba melanjutkan usaha untuk menyusun kerangka hukum *digital governance* melalui Permenkominfo No. 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (Permenkominfo PDP). Pengaturan ini dibentuk untuk melengkapi tujuan awal pemerintah dalam pembentukan UU ITE, dengan penekanan khusus terhadap pelindungan data pribadi. Arah politik hukum yang lebih berfokus kepada perlindungan data pribadi merupakan dampak dari urgensi yang muncul dari maraknya terjadi kebocoran data di berbagai platform digital di Indonesia (Hanifawati, 2021) Namun nyatanya berbagai bentuk pengaturan yang terdapat dalam peraturan ini masih belum menyentuh isu komersialisasi data. Pengaturan yang terdapat dari produk hukum ini nyatanya terlalu terseret politik hukum yang pada saat itu berfokus kepada perlindungan data dari kebocoran yang sedang marak terjadi. Pengaturan yang menyentuh isu komersialisasi data hanya terdapat dalam Pasal 24 yang mengatur mengenai persetujuan dan kesesuaian tujuan dalam pemanfaatan data pribadi oleh penyelenggara sistem elektronik.

Tidak hanya itu, penekanan mengenai pentingnya keamanan siber juga nyatanya masih sangat minim dalam peraturan ini, dengan penyebutan secara tidak langsung mengenai keamanan siber terdapat pada Pasal 33 ayat (2). Di sini pemerintah seolah-oleh berasumsi bahwa keamanan siber sudah merupakan kewajiban natural dari penyelenggara sistem elektronik. Padahal, tidak adanya penekanan yang lebih detail dalam hal ini dapat membahayakan pemilik data pribadi yang

kepentingannya terdapat dalam data yang tersimpan dalam suatu sistem elektronik, karena penyelenggara sistem elektronik tidak harus melalui proses *legal compliance* yang ketat dalam menerapkan taraf keamanan siber yang baik. Pengaturan yang seperti ini secara substantif bertentangan dengan pemahaman teori hukum responsif yang memiliki "cita-cita utama" yang sama dengan hukum otonom, yaitu legalitas.

Selanjutnya pemerintah kembali mengembangkan kerangka perlindungan data melalui UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Melalui pengaturan ini, pemerintah kembali mengembangkan istilah baru, dengan menekankan peran "pengendali data", yang pada produk hukum sebelumnya digabungkan dengan istilah "penyelenggara sistem elektronik." Namun, pemerintah lagi-lagi tidak memberikan penekanan khusus terhadap isu komersialisasi data. Permasalahan paling fatal yang terdapat dalam peraturan perundang-undangan ini adalah tidak terdapatnya pengaturan mengenai pemanfaatan data oleh pihak ketiga. Hal ini justru bertolak belakang dengan pengaturan sebelumnya, yang secara normatif merupakan dasar yang ingin disempurnakan oleh peraturan perundang-undangan ini. Permenkominfo PDP mengatur mengenai pemanfaatan data pribadi oleh pihak ketiga melalui Pasal 28 huruf f, yang memberikan mewajibkan penyelenggara sistem elektronik untuk memberikan opsi persetujuan pemanfaatan data oleh pihak ketiga. UU PDP seharusnya dapat menyempurnakan pengaturan mengenai hal ini, mengingat maraknya praktik "penyembunyian persetujuan" yang kerap dilakukan oleh penyelenggara atau pengendali data dalam *terms of service* di halaman awal penggunaan suatu sistem elektronik (Richards & Hartzog, 2019)

Selain itu, UU PDP juga tidak memberikan klasifikasi data yang lebih detail, meskipun data dijadikan sebagai objek utama pengaturan dari peraturan perundang-undangan ini. Melalui Pasal 4, UU PDP mengatur mengenai jenis data pribadi, namun tidak menyebutkan mengenai data yang berisi perilaku *browsing* dan informasi penggunaan perangkat, yang sebenarnya merupakan jenis data yang sering dikumpulkan dan dimanfaatkan oleh banyak penyelenggara sistem elektronik. Data ini termasuk ke dalam golongan *cookies* dan *cache*, yang merupakan bagian penting dari berbagai bentuk pemanfaatan data untuk memberikan konten maupun iklan yang relevan bagi seorang pengguna, atau yang lebih kenal dengan sebutan *data analytics* (Dekimpe, 2020)

Namun, perkembangan hukum yang dibawa oleh UU PDP sudah semakin mengarah kepada penekanan keamanan siber yang lebih baik, dengan Pasal 16 ayat (2) huruf e secara eksplisit menyebutkan kewajiban pengendali data pribadi dalam melindungi keamanan data pribadi dari pengaksesan tanpa sepengetahuan pengendali data dan/atau pemilik data, yang kembali ditekankan melalui Pasal 35. Sayangnya, pengaturan ini tidak secara sempurna menjelaskan kewajiban sebagaimana dalam pandangan teori hukum murni, karena dari sudut pandang logika positivisme pengaturan ini tidak sepenuhnya memenuhi unsur normatif dari sebuah "kewajiban" sebagaimana pada umumnya. Pengaturan ini tidak dilengkapi dengan bentuk pertanggungjawaban atas kerugian yang diperoleh dari kegagalan dalam menjaga keamanan data. Berdasarkan Pasal 46, pengendali data pribadi hanya diwajibkan untuk memberitahukan pemilik data pribadi mengenai kegagalan tersebut. Tidak hanya itu, tidak juga dijelaskan apa konsekuensi bagi pengendali data pribadi jika tidak memberitahukan hal tersebut.

Kesenjangan dalam Pemahaman Akan Ancaman dari Komersialisasi Data

Pemanfaatan data untuk tujuan komersial memiliki hubungan yang erat dengan keamanan informasi digital. Seiring dengan meningkatnya nilai data sebagai aset, data menjadi sasaran utama bagi pelaku kejahatan di dunia siber. Pelanggaran keamanan data dapat mengakibatkan kerugian finansial yang signifikan, kerusakan pada reputasi perusahaan, dan potensi konsekuensi hukum. Beberapa regulasi perlindungan informasi mewajibkan tindakan keamanan digital tertentu. Sebagai contoh, GDPR mengharuskan organisasi memiliki tingkat perlindungan informasi tertentu. H. Li et al., 2019) Tidak hanya itu, GDPR juga mengatur pentingnya kualitas data, dengan penekanan terhadap kualitas dan kebaruan data, yang dapat membantu proses pengendalian sistem elektronik saat terjadi serangan siber (Grispos et al., 2019) Ancaman dari dunia siber, seperti serangan *ransomware*, dapat mengompromikan integritas data, menjadikan keamanan informasi digital sebagai komponen esensial dalam strategi bisnis yang berorientasi pada data.

Secara konseptual, arah politik hukum yang menekankan pentingnya keamanan siber dapat memanfaatkan pemahaman mendalam segala bentuk ancaman yang terdapat dari praktik komersialisasi data. Dengan mengangkat isu komersialisasi data, pemerintah sebenarnya

berpeluang untuk terus mengembangkan kerangka hukum yang dapat mencukupi keperluan aktivitas di era revolusi industri 4.0. Penekanan akan pentingnya isu komersialisasi data juga sesuai dengan agenda pemerintah yang berencana terus mendorong pertumbuhan ekonomi dengan tema revolusi industri 4.0, dengan terus mendorong segala bentuk pemanfaatan teknologi informasi yang ada (Poerwanto & Shambodo, 2020) Dengan kata lain, pengembangan kerangka hukum yang dapat mengatur mengenai komersialisasi data sebenarnya dapat dilakukan seiring dengan pengembangan kerangka hukum keamanan siber, dengan konsep sistemisasi kerangka hukum yang berkaitan dengan data (Cai & Chen, 2022)

Telah disebutkan sebelumnya bahwa cita-cita utama dari teori hukum responsif adalah legalitas. Namun cita-cita legalitas tidak boleh disamakan dengan upaya mewujudkan legalitas, melalui "legalisasi", yang pada hakikatnya harus melalui penyebaran peraturan dan formalitas prosedural. Pola birokrasi yang mengacu pada proses hukum atau akuntabilitas (melalui *legal compliance*) adalah hal yang cukup asing dalam hukum yang responsif. Cita-cita legalitas perlu dipahami secara lebih umum dan dihilangkan dari formalisme. Dalam sistem yang bertujuan, legalitas adalah pengurangan kekaburan normatif dalam hukum positif dan penyelenggaraannya. Selain itu, perlu digarisbawahi juga bahwa pada hakikatnya hukum responsif bertujuan untuk pemberdayaan dan fasilitasi, dengan akuntabilitas restriktif sebagai fungsi sekunder. Dari sudut pandang ini, dapat dikatakan bahwa politik hukum keamanan siber di Indonesia nyatanya masih belum memfasilitasi berbagai bentuk komersialisasi data sekaligus menjamin perlindungan kepentingan pemilik data tersebut. Meskipun terdapat upaya untuk meningkatkan legalitas dengan pengembangan klasifikasi mendasar dari pengaturan mengenai keamanan dalam pemrosesan data, nyatanya perkembangan tersebut tidak didukung oleh pengaturan yang mendorong akuntabilitas pengendali data melalui *legal compliance.* Langkah pemerintah yang bertujuan menggabungkan berbagai unsur *digital governance* melalui peraturan perundang-undangan seperti UU ITE sebenarnya sudah cukup baik karena memberikan pengaturan yang lebih fleksibel. Seharusnya arah politik hukum seperti ini diteruskan dengan mengembangkan kerangka pengaturan keamanan siber yang sekaligus mencakup unsur perlindungan data dan komersialisasi data.

KESIMPULAN

Hasil analisis menemukan bahwa politik hukum keamanan siber di Indonesia secara keseluruhan masih belum memiliki arah yang jelas, dengan usaha memperbaiki kekurangan normatif yang tidak konsisten. Permasalahan mendasar terdapat pada penafsiran yang berujung kepada ketidakselarasan hierarki peraturan, serta perancangan peraturan perundang-undangan yang tidak mampu menutupi kekurangan normatif dari peraturan sebelumnya yang berposisi lebih rendah secara hierarki. Pengembangan konseptual dari arah politik hukum juga nyatanya masih belum bisa mengakomodasi kepastian hukum mengenai isu komersialisasi data yang praktiknya sudah sangat marak dilakukan di era revolusi industri 4.0. Pemerintah juga masih belum dapat secara konkret menentukan pendekatan yang akan digunakan dalam menerapkan *legal compliance* terkait izin *(permission)* dan pertanggungjawaban dari berbagai bentuk permasalahan yang dapat timbul dari komersialisasi data. Permasalahan-permasalahan ini menunjukkan bahwa isu komersialisasi data belum termasuk ke dalam unsur yang mendapat perhatian khusus dari pemerintah, terlepas dari besarnya relevansi unsur ini dalam era revolusi industri 4.0. Hendaknya pemerintah memeriksa kembali tujuan dan prinsip politik hukum yang akan diteruskan, agar perkembangan kerangka hukum keamanan siber dapat mengakomodasi berbagai isu yang krusial di era revolusi industri 4.0, demi pemanfaatan potensi teknologi informasi yang lebih baik dan bertanggung jawab.

ACKNOWLEDGMENTS

None.

DAFTAR PUSTAKA

Boldosova, V. (2019). Deliberate storytelling in big data analytics adoption. *Information Systems Journal*, *29*(6), 1126–1152. https://doi.org/10.1111/isj.12244

Cai, P., & Chen, L. (2022). Demystifying data law in China: a unified regime of tomorrow. *International Data Privacy Law*, *12*(2), 75–92. https://doi.org/10.1093/idpl/ipac004

Cole, C. L., Sengupta, S., Rossetti, S., Vawdrey, D. K., Halaas, M., Maddox, T. M., Gordon, G., Dave, T., Payne, P. R. O., Williams, A. E., & Estrin, D. (2021). Ten principles for data sharing and commercialization. *Journal of the American Medical Informatics Association*, *28*(3), 646–649. https://doi.org/10.1093/jamia/ocaa260

Darmody, A., & Zwick, D. (2020). Manipulate to empower: Hyper-relevance and the contradictions of marketing in the age of surveillance capitalism. *Big Data & Society*, *7*(1), 1–12. https://doi.org/10.1177/2053951720904112

Dekimpe, M. G. (2020). Retailing and retailing research in the age of big data analytics. *International Journal of Research in Marketing*, *37*(1), 3–14. https://doi.org/https://doi.org/10.1016/j.ijresmar.2019.09.001

Disemadi, H. (2022). Lenses of legal research: A descriptive essay on legal research methodologies. *Journal of Judicial Review*, 24(2). https://doi.org/10.37253/jjr.v24i2.7280

Durovic, M., & Lech, F. (2021). A Consumer Law Perspective on the Commercialization of Data. *European Review of Private Law*, *29*(5), 701–732. https://doi.org/https://doi.org/10.54648/erpl2021038

Fadilah Raskasih. (2021). Batasan Kebebasan Berpendapat Melalui Media Elektronik dalam Perspektif HAM Dikaitkan dengan Tindak Pidana Menurut UU ITE. *JOURNAL EQUITABLE*, *5*(2), 147–167. https://doi.org/10.37859/jeq.v5i2.2462

Fini, R., Rasmussen, E., Siegel, D., & Wiklund, J. (2018). Rethinking the Commercialization of Public Science: From Entrepreneurial Outcomes to Societal Impacts. *Academy of Management Perspectives*, *32*(1), 4–20. https://doi.org/10.5465/amp.2017.0206

González Chávez, C. A., Unamuno, G., Despeisse, M., Johansson, B., Romero, D., & Stahre, J. (2023). Analyzing the risks of digital servitization in the machine tool industry. *Robotics and Computer-Integrated Manufacturing*, *82*, 1–11. https://doi.org/https://doi.org/10.1016/j.rcim.2022.102520

Grispos, G., Glisson, W. B., & Storer, T. (2019). How good is your data? Investigating the quality of data generated during security incident response investigations. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *January*, 7156–7165. https://doi.org/10.24251/hicss.2019.859

Guay, R., & Birch, K. (2022). A comparative analysis of data governance: Socio-technical imaginaries of digital personal data in the USA and EU (2008–2016). *Big Data & Society*, *9*(2), 1–13. https://doi.org/10.1177/20539517221112925

Hadiyati, N., & Stathany, H. (2021). Analisis Undang-Undang ITE Berdasarkan Asas Pembentukan Peraturan Perundang-Undangan di Indonesia. *Mizan: Jurnal Ilmu Hukum*, *10*(2), 146–156. https://doi.org/10.32503/mizan.v10i2.1657

Hanifawati, S. D. (2021). Urgensi Penegakan Hukum Pidana pada Penerima Pinjaman Kegiatan Peer To Peer Lending Fintech Ilegal dan Perlindungan Data Pribadi. *Jurnal Penegakan Hukum Dan Keadilan*, *2*(2), 162–172. https://doi.org/10.18196/jphk.v2i2.12181

Hossain, E., Khan, I., Un-Noor, F., Sikander, S. S., & Sunny, M. S. H. (2019). Application of Big Data and Machine Learning in Smart Grid, and Associated Security Concerns: A Review. *IEEE Access*, *7*, 13960–13988. https://doi.org/10.1109/ACCESS.2019.2894819

Kelsen, H. (2022). Pure Theory of Law. In M. Knight (Ed.), *University of California Pre* (Reprinted). University of California Press.

Kletzer, C. (2018). The Idea of a Pure Theory of Law. In *Hart Publishing*. Hart Publishing.

Kurnianingrum, T. P. (2020). Urgensi Perlindungan Data Pribadi Konsumen di Era Ekonomi Digital. *Kajian*, *25*(3), 197–216.

Li, H., Yu, L., & He, W. (2019). The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management*, *22*(1), 1–6. https://doi.org/10.1080/1097198X.2019.1569186

Li, Y. (2022). Division of Data Ownership Between the Individual and the Enterprise That Collects the Data. *Asian Business Research*, *7*(3), 26–29. https://doi.org/10.20849/abr.v7i3.1121

Mazumdar, S., & Wang, J. (2018). Big Data and Cyber Security: A Visual Analytics Perspective. In S. Parkinson, A. Crampton, & R. Hill (Eds.), *Guide to Vulnerability Analysis for Computer Networks and Systems: An Artificial Intelligence Approach* (pp. 367–381). Springer International Publishing. https://doi.org/10.1007/978-3-319-92624-7_16

Muldani, T. (2022). Implikasi Awal Penerbitan SKB UU ITE Pasal 27 Ayat (3). *MUKASI: Jurnal Ilmu Komunikasi*, *1*(2), 148–163. https://doi.org/10.54259/mukasi.v1i2.857

Nonet, P., & Selznick, P. (2017). Law and society in transition: Toward responsive law. In *Routledge*. https://doi.org/10.4324/9780203787540

Poerwanto, P., & Shambodo, Y. (2020). Revolusi Industri 4.0: Googelisasi Industri Pariwisata dan Industri Kreatif. *Journal of Tourism and Creativity*, *4*(1), 59–72. https://doi.org/10.19184/jtc.v4i1.16956

Richards, N., & Hartzog, W. (2019). The Pathologies of Digital Consent. *Washington University Law Review*, *96*(6), 1461–1503.

Rohmy, A. M., Suratman, T., & Nihayaty, A. I. (2021). UU ITE Dalam Perspektif Perkembangan Teknologi Informasi dan Komunikasi. *Dakwatuna: Jurnal Dakwah Dan Komunikasi Islam*, *7*(2), 309–339. https://doi.org/10.54471/dakwatuna.v7i2.1202

Simorangkir, B. (2021). Memperluas Agenda Studi Keamanan Nasional: Politik, Hukum dan Strategi. *Jurnal Diplomasi Pertahanan*, *6*(3), 45–57. https://doi.org/10.33172/jdp.v6i3.663

Tan, D. (2021). Metode penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan penelitian Hukum. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial*, *8*(5), 1332–1336. https://core.ac.uk/download/pdf/490668614.pdf

Vassakis, K., Petrakis, E., & Kopanakis, I. (2018). Big Data Analytics: Applications, Prospects and Challenges. In G. Skourletopoulos, G. Mastorakis, C. X. Mavromoustakis, C. Dobre, & E. Pallis (Eds.), *Mobile Big Data: A Roadmap from Models to Technologies* (pp. 3–20). Springer International Publishing. https://doi.org/10.1007/978-3-319-67925-9_1

Wachter, S. (2018). Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. *Computer Law & Security Review*, *34*(3), 436–449. https://doi.org/https://doi.org/10.1016/j.clsr.2018.02.002

Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., Khan, I., Hewage, C., & Platts, J. (2022). Cybersecurity, Data Privacy and Blockchain: A Review. *SN Computer Science*, *3*(2), 1–12. https://doi.org/10.1007/s42979-022-01020-4