IPMHI Law Journal, Vol. 1 No. 2, Edisi Juli-Desember 2021
P-ISSN: 2797-8508, E-ISSN: 2807-8330
DOI : https://doi.org/10.15294/ipmhi.v1i2.53270

OPTIMALISASI PENANGGULANGAN KEBOCORAN DATA MELALUI *REGULATORY BLOCKCHAIN* GUNA MEWUJUDKAN KEAMANAN SIBER DI INDONESIA

Inaz Indra Nugroho*, Reza Pratiwi, Salsabila Rahma Az Zahro
Universitas Diponegoro
*Correspondent Email : inazindranugroho@students.undip.ac.id

Naskah diterima: 29/10/2021, Revisi: 15/11/2021, Disetujui: 31/12/2021

Abstrak

Pada era disrupsi saat ini, inovasi teknologi dan informasi terus mengalami perkembangan, salah satu contohnya adalah e-commerce. Namun pada pelaksanaannya, masih dijumpai beberapa kelemahan, salah satunya dalam sistem keamanan siber yang mengatur perlindungan data pribadi milik pengguna e-commerce yang mengakibatkan kebocoran data pribadi. Selain itu, belum adanya peraturan khusus terkait perlindungan data pribadi menyebabkan banyaknya permasalahan terkait kebocoran data pribadi. Hal ini bertentangan dengan Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD NRI Tahun 1945) yang menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi. Penulisan ini memiliki tujuan untuk membantu mewujudkan penegakan keamanan siber di Indonesia. Karya tulis ilmiah ini menggunakan metode penulisan yuridis empiris. Metode pengumpulan data yang digunakan yaitu studi lapangan dengan melakukan wawancara dan studi kepustakaan, seperti peraturan perundang-undangan, buku dan jurnal. Ketika data sudah terkumpul, kemudian dianalisis mengunakan metode kualitatif. Berdasarkan hasil analisa yang telah dikumpulkan, bahwa sistem keamanan siber di Indonesia masih membutuhkan inovasi terhadap perlindungan data pribadi, yaitu berupa sistem keamanan blockchain. Penggunaan sistem blockchain memerlukan sebuah payung hukum agar keberadannya dapat mengurangi permasalahan kebocoran data pribadi. Berkaitan dengan hal itu, diperlukan kebijakan terkait sistem keamanan siber yang memiliki orientasi pada era disrupsi terhadap perlindungan data pribadi, yaitu Regulatory Blockchain. Dalam pelaksanaannya membutuhkan peran stakeholder, seperti Kementerian Komunikasi dan Informatika, serta Badan Siber dan Sandi Negara untuk merealisasikan Pasal 28G ayat (1) UUD NRI Tahun 1945.

Kata Kunci : ***Blockchain; Data Pribadi; E-Commerce; Era Disrupsi; Kejahatan Siber***

How to cite:

Nugroho, I., Pratiwi, R., & Az Zahro, S. (2021). Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber di Indonesia. *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal*, 1(2)

Diterbitkan oleh:
Ikatan Penulis Mahasiswa Hukum Indonesia
IPMHI Law Journal

PENDAHULUAN

1. Latar Belakang

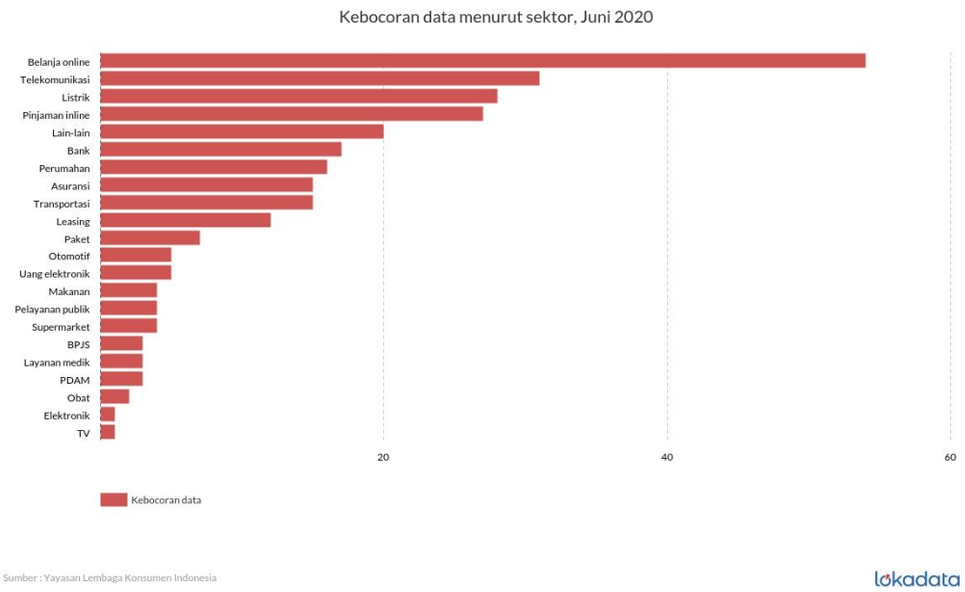
Globalisasi mengharuskan dunia terus melangkah ke arah modernisasi, sehingga mendorong munculnya berbagai inovasi dibidang teknologi dan informasi. Era revolusi industri 4.0 menjadi akibat dari adanya globalisasi tersebut. Menurut Kamus Besar Bahasa Indonesia (KBBI), revolusi adalah sebuah perubahan dalam suatu bidang yang sangat mendasar, sedangkan industri adalah peralatan dan sarana yang digunakan untuk mengolah dan memproses suatu barang.[1] Maka dapat diartikan bahwa revolusi industri merupakan sebuah perubahan yang mendasar terkait sarana dan peralatan dalam mengolah atau memproses suatu barang.

Jika dikaitkan dengan konteks ini, revolusi industri merupakan sebuah perubahan yang mendasar dalam bidang teknologi untuk dapat mengolah dan memproses segala kebutuhan manusia dengan mudah dan praktis. Misalnya, proses mengolah suatu barang yang semula dikerjakan oleh manusia kini telah digantikan oleh tenaga mesin.[2] Sedangkan revolusi industri 4.0 itu sendiri adalah era dimana semua aktivitas masyarakat akan berpindah ke dunia digital karena adanya perubahan dalam bidang teknologi. Pada umumnya, era revolusi industri akan menjadi awal mula dari era disrupsi, yaitu era yang menimbulkan perubahan dalam kehidupan masyarakat secara besar-besaran, dalam hal ini disebabkan oleh perkembangan inovasi dibidang teknologi.

Era disrupsi telah berhasil membuat kehidupan masyarakat bergantung pada teknologi. Maka demi mengimbangi kebutuhan masyarakat yang mengalami perkembangan dan perubahan tersebut, teknologi pun akan terus mengalami perubahan dan perkembangan atau akan memunculkan sebuah inovasi baru agar terus dapat membantu masyarakat dalam memenuhi kebutuhan mereka. E-*commerce* menjadi salah satu bukti dari adanya perkembangan dan inovasi teknologi di era disrupsi ini. E-commerce telah mampu mengubah tatanan kehidupan masyarakat terutama dalam hal memenuhi kebutuhan sehari-harinya dengan segala kemudahan dan kepraktisan yang berhasil ditawarkan.

Namun, saat ini ramai terdengar bahwa telah terjadi kasus kebocoran data pribadi milik pengguna e-commerce. Hal ini dapat dibuktikan melalui grafik berikut.

[1] Kamus Besar Bahasa Indonesia, (https://kbbi.kemdikbud.go.id/, diakses pada 5 Agustus 2021).
[2] Hendra Suwardana, "Revolusi Industri 4.0 Berbasis Revolusi Mental", Jati Unik, Vol. 2 No.1,2018, 110-111.



Gambar 1. Kebocoran Data Menurut Sektor di Indonesia, Juni 2020.
***Sumber: Lokadata[3]**

Berdasarkan pada grafik di atas, kasus kebocoran data paling banyak dialami oleh para pengguna situs belanja online atau *e-commerce*. Banyaknya kasus kebocoran data milik pengguna *e-commerce* tentu membuat masyarakat menjadi khawatir akan keamanan data pribadi milik mereka. Masyarakat takut jika data pribadi mereka akan disalahgunakan untuk melakukan sebuah kejahatan atau tindakan melanggar hukum lainnya oleh pihak yang tidak bertanggung jawab. Terlebih lagi, sampai saat ini pihak yang mengalami kebocoran data pribadi masih belum mendapatkan perlindungan dan kepastian hukum yang jelas. Kasus kebocoran data ini tidak mencerminkan nilai yang terkandung di dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD NRI 1945), khususnya Pasal 28G ayat (1) yang menjabarkan bahwa perlindungan diri pribadi merupakan hak setiap orang. Akan tetapi dalam kasus tersebut, para pihak terkait belum dapat memberikan perlindungan terhadap diri pribadi dari masing-masing pengguna *e-commerce*.

Kebijakan mengenai perlindungan data pribadi milik konsumen atau dalam konteks ini ialah pengguna *e-commerce* yang bersifat mengikat dan lebih kuat belum terdapat di Indonesia. Peraturan mengenai perlindungan data pribadi yang berlaku sekarang yaitu ketentuan yang terdapat di dalam Pasal 26 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (Permen Kominfo Nomor 20 Tahun 2016), serta Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik (PP Nomor 80 Tahun 2019). Namun, regulasi tersebut belum dapat menangani kasus kebocoran data dengan baik. Terbukti, sampai sekarang kasus kebocoran data masih terus mengalami peningkatan sebagaimana yang tergambar dalam tabel berikut.

[3] Ayyi Achmad Hidayah – Shila Ezerli, "Kasus Kebocoran Data Semakin Banyak, Belanja Daring Paling Rentan" Lokadata, (https://lokadata.id/artikel/kasus-kebocoran-data-semakin-banyak-belanjadaring-paling-rentan, diakses pada 7 Agustus 2021).

Tabel 1. Jumlah Kasus Kebocoran Data di Indonesia

Tahun	Jumlah Kasus
2020	± 104.090.000
2021	± 386.500.000

***Sumber: Olahan Sendiri**

Salah satu penyebab dari meningkatnya kasus kebocoran data tersebut adalah dikarenakan regulasi khusus mengenai perlindungan data pribadi belum ada hingga saat ini. Rancangan Undang-Undang (RUU) tentang Perlindungan Data Pribadi yang dimasukan pada Program Legislasi Nasional (Prolegnas) hampir disahkan menjadi undang-undang yang baru, tetapi RUU tersebut harus ditarik kembali dari daftar peraturan undang-undang yang akan disahkan dalam Prolegnas pada tahun 2020, dikarenakan banyaknya pihak pengusaha yang merasa bahwa isi dari RUU tersebut terlalu merugikan mereka.[4] Sistem keamanan data di Indonesia yang masih terlalu lemah menjadi penyebab naiknya tingkat permasalahan mengenai pencurian data pribadi. Alasan lain yang dapat menyebabkan naiknya angka kasus kebocoran data pribadi milik masyarakat adalah karena sistem keamanan data yang ada di Indonesia masih terlalu lemah. Maka dari itu, peretas (*hacker*) dapat dengan mudah masuk dan mencuri data pribadi milik masyarakat, terkhususnya para pengguna *e-commerce*.

Jika dilihat dari sisi regulasi yang masih lemah, maka untuk tetap menjamin keamanan data pribadi milik para pengguna *e-commerce*, diperlukan sebuah *upgrading* pada sistem keamanan yang digunakan oleh pihak *e-commerce* itu sendiri. Sistem keamanan yang dapat melindungi data pribadi milik pengguna *e-commerce* tersebut adalah sistem keamanan baru yang dinamakan *Regulatory Blockchain*. *Regulatory Blockchain* merupakan suatu kebijakan yang nantinya dikeluarkan oleh Kementerian Komunikasi dan Informatika (Kominfo) untuk mewajibkan seluruh pemilik *e-commerce* menerapkan sistem keamanan *blockchain* pada pengaturan keamanan data mereka. Kewenangan Kominfo dalam membuat peraturan terkait *regulatory blockchain* sesuai dengan amanah yang terkandung di dalam PP Nomor 80 Tahun 2019.

Blockchain merupakan jenis sistem keamanan yang menggunakan teknik *peer to peer* dalam memindahkan sebuah data, sehingga penggunaan dan pengawasannya tidak hanya bergantung pada satu server. Sistem keamanan yang digunakan oleh *blockchain* berupa sistem *sharing security*. *Sharing security* yang dimiliki oleh *blockchain* dapat memperkuat tingkat keamanan dalam penyimpanan data.Hal ini dikarenakan, para peretas (*hacker*) harus menembus sistem keamanan yang berlapis terlebih dahulu agar dapat mencuri data pribadi milik pengguna *e-*

[4] Asosiasi Penyelenggara Telekomunikasi Seluruh Indonesia (ATSI), "Rapat Dengar Pendapat Umum DPR RI-ATSI RUU Perlindungan Data Pribadi", (https://www.atsi.or.id/atsi-menghadiri-rdpu- dengan-komisi-i-dpr-ri/, diakses pada 7 Agustus 2021).

commerce.[5] Dengan demikian, penggunaan sistem keamanan *blockchain* dapat mengurangi angka peretasan atau kebocoran data pribadi yang ada di Indonesia.

Blockchain pertama kali diperkenalkan di tahun 2008 melalui sebuah artikel yang berjudul *"Bitcoin: A Peer to Peer Electronic Cash"* yang dikarang oleh seorang kewarganegaraan Jepang yang bernama **Satoshi Nakamoto**.[6] Keinginan untuk melakukan transaksi online dengan cepat dan mudah tanpa harus melibatkan pihak ketiga melahirkan suatu sistem bernama *blockchain*, sehingga segala sesuatu yang menjadi akibat dari adanya pihak ketiga seperti pembayaran biaya transfer dan biaya kirim akan dihapuskan. Model transaksi yang digunakan adalah sistem atau model kepercayaan di antara dua pihak terkait transaksi dalam *e-commerce*. Meskipun sistem dalam bertransaksi ini sebelumnya sudah ada, namun sistem yang sudah ada tersebut masih dapat menyebabkan transaksi berjalan tidak dengan cepat dan mudah jika setiap institusi finansial memiliki perbedaan dalam memproses transaksinya. Maka dari itu, Nakamoto beranggapan bahwa dibutuhkannya sistem pembayaran elektronik yang memiliki basis pembuktian kriptografi yang dapat memungkinkan para pihak agar dapat bertransaksi secara daring dengan aman dan praktis tanpa melalui pihak ketiga.[7]

Di negara Amerika Serikat, *blockchain* digunakan oleh sebuah perusahaan yang memproduksi perangkat lunak komputer dengan nama *International Business Machine Corporation* (IBM) yang bergerak pada sektor industri dan sektor bisnis. Selain itu, perusahaan ini juga membuat *platform* perdagangan nilai tukar yang dinamakan *hyperledger fabric*. Proyek ini didukung oleh tujuah bank dunia diantaranya adalah Unicredit, KBC dan HSBC.[8]

Sedangkan di Indonesia sendiri, kegunaan *blockchain* disamakan dengan buku besar akuntansi elektronik yang disimpan secara publik dan berisi daftar berbagai transaksi antar pihak yang telah teregistrasi.[9] Berdasarkan spesifikasi tingkat keamanan yang dimiliki, *blockchain* mampu menyimpan informasi terkait aktivitas berbagai transaksi keuangan secara online dengan baik. Sistem *sharing security* yang dimiliki oleh *blockchain* mampu menjaga data keuangan yang ada dengan aman, sehingga lembaga keuangan seperti Otoritas Jasa Keuangan dan Bank Indonesia tertarik untuk memanfaatkannya sebagai pencatat sekaligus penyimpan aktivitas transaksi keuangan yang dilakukan secara online. Dampak positif yang ditimbulkan karena keberadaan *blockchain* dalam bidang keuangan ini tidak hanya dirasakan oleh lembaga keuangan saja, tetapi juga bisa dirasakan oleh masyarakat secara luas.

---

[5] Universitas Islam Indonesia, "Blockchain Tingkatkan Keamanan Data Dari Peretasan", (https://www.uii.ac.id/blockchain-tingkatkan-keamanan-data-dari-peretasan/, diakses pada 5 Agustus 2021).

[6] Harris C., "The History of Bitcoin" Crypto Currency News, (https://cryptocurrencynews.com/the-history-of-bitcoin/, diakses pada 6 Agustus 2021).

[7] Nakamoto S., "Bitcoin: A Peer-to-Peer Electronic Cash System", (https://bitcoin.org/bitcoin.pdf, diakses pada 6 Agustus 2021).

[8] International Business Machines Corporation (IBM), "Welcome to IBM Blockchain", (https://www.ibm.com/blockchain, diakses pada 7 Agustus 2021).

[9] Ery Punta Hendraswara, "Blockchain From a Society's Perspective" Indonesia Blockchain Society, (https://files.acci.or.id/files/presentation/ibs-blockchain-from-a-society-perspective.pdf, diakses pada 7 Agustus2021).

Meskipun di Indonesia penggunaan *blockchain* lebih berfokus pada pemanfaatan di bidang keuangan. Akan tetapi, jika dilihat dari berbagai spesifikasi dan keunggulan yang dimiliki oleh *blockchain*, maka dapat dimanfaatkan juga dalam dunia *e-commerce* khususnya untuk menyimpan dan meningkatkan keamanan data pribadi para pengguna *e-commerce*. Selain itu, dengan banyaknya kasus kebocoran data pribadi milik pengguna *e-commerce*, semakin menguatkan fakta terkait lemahnya sistem keamanan yang dimiliki oleh *e-commerce* saat ini. Oleh karena itu, diperlukan optimalisasi dalam penggunaan *blockchain* di Indonesia dengan menerapkan sistem keamanan *regulatory blockchain* bagi semua pihak *e-commerce* yang ada di Indonesia.

2. Perumusan Masalah

1. Bagaimana penanganan kasus kebocoran data pribadi pengguna *e-commerce* di Indonesia saat ini?
2. Bagaimana konsep pengaturan regulatory blockchain yang akan digunakan dalam mengatasi kasus kebocoran data pribadi milik pengguna e-commerce di era disrupsi?

METODE

Penulisan karya tulis ilmiah ini menggunakan jenis penelitian yuridis empiris, yaitu penelitian hukum mengenai penerapan ketentuan hukum normatif secara nyata pada masyarakat dalam peristiwa hukum tertentu.[10] Hal ini dilakukan dengan meneliti peraturan hukum yang berkaitan dengan kasus yang dibahas, kemudian digabungkan dengan data dan kenyataan yang hidup ditengah-tengah masyarakat. Data dalam penelitian ini diperoleh dari hasil wawancara dengan mengajukan pertanyaan kepada responden secara daring.

HASIL PENELITIAN DAN PEMBAHASAN

1. PENANGANAN KASUS KEBOCORAN DATA PENGGUNA *E-COMMERCE* DI INDONESIA SAAT INI

Seiring perkembangan zaman, teknologi menimbulkan dampak yang besar bagi kehidupan manusia. Kehadirannya membawa perubahan dalam bentuk perilaku dan pola hidup masyarakat, serta menyebabkan perubahan ekonomi, budaya, sosial dan penegakan hukum. Perkembangan ini telah memasuki revolusi industri 4.0 yang ditandai dengan meningkatnya pemakaian teknologi informasi. Dengan adanya perkembangan tersebut, aktivitas masyarakat tidak akan terlepas dari teknologi. Salah satu bentuk dari perkembangan teknologi di bidang ekonomi adalah sistem perdagangan secara elektronik yang disebut dengan *e-commerce*. Sistem tersebut memberikan kemudahan bagi penjual untuk dapat mengetahui target pasar yang membutuhkan produk atau jasa mereka, serta memberikan kemudahan bagi pembeli yang mencari produk atau barang yang dibeli secara *online*. Kemudahan yang dirasakan oleh pembeli dan penjual dapat memberi mereka keuntungan. Namun dari kemudahan dan keuntungan yang mereka peroleh, timbul permasalahan mengenai kebocoran data pribadi para pengguna *e-commerce*.

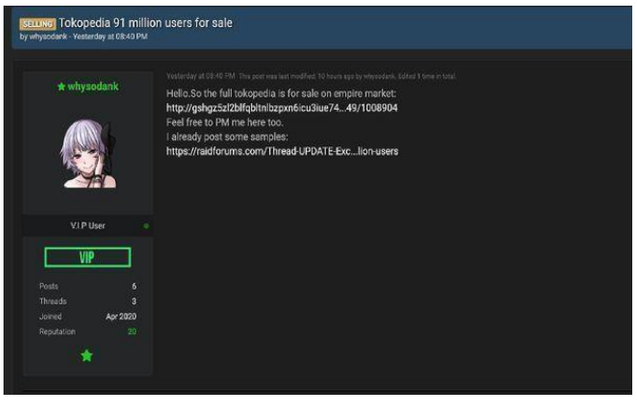
[10] Abdulkadir Muhammad, Hukum dan Penelitian Hukum (Bandung: Citra Aditya Bakti, 2004), 134.

Berdasarkan data *United Nations Conference on Trade and Development* (UNCTAD) tahun 2015, menyebutkan terdapat 2.100 kasus yang menimbulkan permasalahan terkait data pribadi milik pengguna *e-commerce* dengan jumlah mencapai 822 juta data pribadi terekam dalam kegiatan *e-commerce*, serta dikumpulkan di *marketplace*. Kemudian, terdapat 152 juta data pribadi, seperti nama, enkripsi *password*, identitas konsumen, nomor kartu kredit dan debit, serta berbagai informasi yang berkaitan dengan data pembelian konsumen. Pihak yang melakukan pelanggaran data pribadi dengan tujuan untuk kepentingan bisnis sekitar 53% pelaku usaha. Data pribadi yang diambil adalah *password*, nama akun, dan aktivitas pengguna di *e-mail*.[11] Permasalahan tersebut dijelaskan dalam Pasal 4 huruf a Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen yang menjelaskan, *"hak konsumen adalah hak atas kenyamanan, keamanan dan keselamatan dalam mengkonsumsi barang dan/atau jasa".* Jika dikaitkan dari permasalahan kebocoran data dan penjelasan hak konsumen tersebut, dapat diartikan bahwa pengguna *e- commerce* menjadi korban dari penyalahgunaan data pribadi yang menganggu kenyamanan ketika melakukan aktivitas *e-commerce*, serta berakibat pada keamanan dan keselamatan para pengguna *e-commerce* yang tidak sepenuhnya terjamin.

Di Indonesia, kasus kebocoran data pribadi pernah dialami oleh perusahaan Tokopedia. Pada bulan mei 2020, bermula dari adanya postingan akun mengenai kumpulan data pribadi dari pengguna Tokopedia pada forum internet bernama *RaidForums*. Forum ini merupakan tempat diskusi untuk melakukan kegiatan pencurian data di ruang siber. Kemudian, sebuah akun twitter @underthebreach mengklaim bahwa terdapat sekitar 15 juta data pribadi akun pengguna Tokopedia yang dicuri. Data pribadi yang dicuri mencakup email, ID, nama lengkap, jenis kelamin, nomor *handphone*, tanggal lahir dan password. Hal ini direspon oleh **Nuraini Razak** selaku *Vice President of Corporate Communications* Tokopedia yang mengkonfirmasi adanya kegiatan pencurian data pribadi pengguna dan mereka akan memastikan bahwa informasi data yang penting akan tetap terlindungi. Selain itu, kembali ditemukan sebuah akun *Whysodank* yang menjual beberapa data pribadi pengguna Tokopedia sejumlah 91 juta akun di forum *darkweb* bernama *EmpireMarket*. Maka dari itu, pihak Tokopedia akan memeriksa dan mengklaim data pembayaran pengguna seperti kartu kredit dan debit masih terjaga keamanannya. Pihak Tokopedia juga menyatakan akan menjaga keamanan data pribadi yang menjadi prioritas utama mereka.[12]

[11] UNCTAD, Report no. TD/B/C.II/EM.5/2: Trade and Development Board; Investment, Enterprise, and Development Commission Expert Meeting on Cyber laws and Regulations for Enhancing E-Commerce (Geneva: United Nations, 2015), 10-11.

[12] Adhl Wicaksono, "Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan Dijual" , CNN Indonesia, (https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91- juta-akun-tokopedia-bocor-dan-dijual, diakses pada 06 Agustus 2021).



Gambar 2. Penjualan Data
Data Pribadi Pengguna Tokopedia oleh Whysodank
***Sumber: CNN Indonesia**

Setelah kejadian kebocoran data menimpa perusahaan Tokopedia pada tahun 2020 lalu, Komunitas Konsumen Indonesia (KKI) yang diwakili oleh **David Tobing** menggugat Menteri Komunikasi dan Informatika (Menkominfo) sebagai pihak Tergugat 1 dan pihak Tokopedia sebagai Tergugat 2. Menkominfo sebagai pihak yang berwenang dalam perlindungan data pribadi, maka Menkominfo dalam gugatannya sebagai tergugat 1. Gugatan ini terdaftar secara *e-court* di Pengadilan Negeri Jakarta Pusat dengan Nomor Register 235/PDT.G/2020/PN.JKT/PST dan telah melakukan sidang pada bulan Juni tahun 2020. Kemudian, KKI menerima pengaduan dari masyarakat mengenai penguasaan dan pencurian data pribadi pengguna Tokopedia. Pengaduan ini disampaikan karena khawatir akan terjadi tindakan yang melawan hukum dan menimbulkan kerugian bagi para pengguna Tokopedia di kemudian hari.

Gambar 3. Surat Pernyataan dari Tokopedia
***Sumber: Gmail Pengguna Tokopedia**

Selain itu, KKI juga menyampaikan sebuah tuntutan yaitu permintaan kepada Menkominfo untuk mencabut Tanda Daftar Penyelenggaraan Sistem Elektronik Tokopedia, dan harus membayar denda administrasi sejumlah Rp 100 miliar yang akan diserahkan pada kas negara dalam jangka waktu paling lambat 30 hari putusan sejak putusan perkara. Penanganan lain dari

Tokopedia yaitu penyampaian permintaan maaf dan pertanggungjawaban yang dimuat dalam media cetak di Indonesia, serta atas permintaan dari KKI memerintahkan kepada Tokopedia untuk memberitahu kepada pengguna Tokopedia mengenai pencurian data pribadi pengguna.[13]

Kejadian yang menimpa Tokopedia bukan pertama kali di Indonesia, kasus kebocoran data juga terjadi di perusahaan Bukalapak. Data pribadi pengguna Bukalapak dijual sekitar 13 juta akun oleh *Asian Boy* dan 12 juta akun oleh *Tryhard User* di forum *hacker Raid Forums*. Dalam menangani kasus kebocoran data, pihak Bukalapak belum dapat memberikan perlindungan hukum terhadap konsumen yang mengalami kebocoran data. Langkah yang diambil Bukalapak hanya berupa penggantian sistem keamanan data pribadi pengguna sebagai bentuk pencegahan atas terulangnya permasalahan tersebut. **Rachmat Kaimuddin**, selaku *Chief Executive Officer* (CEO) menjelaskan perusahaan Bukalapak memiliki sistem keamanan yang berlapis dalam menyimpan, menerima dan mengolah data pengguna. Ketika menerima, sistem akan menggunakan metode https agar data yang masuk tidak akan dicuri. Kemudian, ketika disimpan menggunakan metode keamanan mutakhir dan berlapis. Ketika mengolah dan menggunakan data, perusahaan Bukalapak menggunakan pengawasan ketat, agar jejak pengakses akan terekam dengan baik.[14]

Kejadian yang menimpa Tokopedia dan Bukalapak merupakan sebuah contoh *e-commerce* di Indonesia yang melanggar hak privasi masyarakat karena adanya kasus kebocoran data pribadi pengguna. Hal ini tidak sesuai dengan amanat yang terkandung dalam Pasal 28G ayat (1) UUD NRI Tahun 1945. Selain itu, adanya kasus kebocoran data tersebut menggambarkan bahwa masih lemahnya sistem keamanan siber *e- commerce* di Indonesia, serta dapat juga disebabkan karena belum adanya suatu kebijakan khusus terkait perlindungan data pribadi. Keberadaan kebijakan khusus yang mengatur perlindungan data pribadi, sangat penting peranannya guna memberikan perlindungan hukum terhadap hak pribadi masyarakat. Peraturan yang saat ini berlaku mengenai perlindungan data pribadi antara lain Pasal 26 ayat 1 UU ITE, Permen Kominfo Nomor 20 Tahun 2016, PP Nomor 80 Tahun 2019 tentang Perdagangan melalui Sistem Elektronik. Namun, peraturan tersebut belum mampu menangani kasus kebocoran data yang saat ini masih terjadi. Maka dari itu, dibutuhkan sebuah regulasi terkait penggunaan sistem keamanan elektronik yang baru yaitu *regulatory blockchain* agar dapat menjamin keamanan data pribadi.Terlebih lagi belum ada *e-commerce* di Indonesia yang menggunakan sistem keamanan blockchain, sehingga *regulatory blockchain* perlu ditetapkan saat ini.

2. KONSEP PENGATURAN REGULATORY BLOCKCHAIN DALAM MENGATASI KASUS KEBOCORAN DATA PRIBADI MILIK PENGGUNA E-COMMERCE

[13] Ramiz Afif Naufal, Skripsi: "Tanggung Jawab PT Tokopedia dalam Kasus Kebocoran Data PribadiPengguna" (Yogyakarta: Universitas Islam Indonesia, 2020), 95-96.
[14] Adhl Wicaksono, "13 Juta Data Bocor Bukalapak Dijual di Forum Hacker", CNN Indonesia, (https://www.cnnindonesia.com/teknologi/20200506065657-185-500477/13-juta-data-bocor-bukalapak-dijual-di-forum-hacker, diakses pada 07 Agustus 2021).

Di era disrupsi ini, kemajuan teknologi tidak dapat terpisahkan dalam kehidupan masyarakat. Namun, kemajuan teknologi dibarengi juga dengan peningkatan kejahatan siber. Salah satunya adalah kejahatan siber terkait kebocoran data pribadi pengguna *e-commerce*. Hal ini terjadi karena tidak adanya regulasi terkait perlindungan data pribadi. Selain itu sistem keamanan yang digunakan oleh *e-commerce* di Indonesia saat ini masih lemah. Permasalahan ini memerlukan solusi berupa sistem yang mampu merekam dan menyimpan data pribadi dengan aman, sistem tersebut menggunakan sistem *blockchain*. *Blockchain* menggunakan teknik *peer to peer* dan *sharing security* dalam penyimpanan datanya. *Peer to peer* menyediakan lebih dari satu server dalam memindahkan data-data, sedangkan *sharing security* memberikan keamanan berlapis dalam penyimpanan data. Teknik penyimpanan data tersebutdapat memperkuat sistem keamanan dan melindungi data pribadi pengguna *e-commerce*.

Regulatory blockchain merupakan suatu kebijakan yang mengharuskan seluruh pemilik *e-commerce* menerapkan sistem *blockchain* pada pengaturan keamanan data mereka. Lembaga yang berwenang mengeluarkan kebijakan terkait *regulatory blockchain* adalah Kominfo, sehingga kebijakan tersebut akan dikeluarkan dalam bentuk Peraturan Menteri Kominfo. Hal ini dikarenakan sesuai dengan tugas pokok dan fungsi dari Kominfo untuk menjamin keamanan data pribadi masyarakat di ruang siber sebagaimana yang telah dijelaskan dalam Permen Kominfo Nomor 20 Tahun 2016.

Dalam pelaksanaannya, Kominfo akan dibantu oleh Badan Siber dan Sandi Negara (BSSN) selaku penguji dan pengawas sistem keamanan *e-commerce*. Penetapan BSSN selaku penguji dan pengawas sistem keamanan siber *e-commerce* merupakan bagian dari penyelenggaraan keamanan siber sesuai dengan Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber Sandi Negara. Maka dari itu, BSSN memenuhi kualifikasi sebagai lembaga yang mampu untuk menguji sistem *blockchain e-commerce*.

Regulatory blockchain terdiri dari dua prosedur, yaitu prosedur yang diperuntukan bagi *e-commerce* yang sudah didaftarkan dan prosedur yang diperuntukan bagi *e-commerce* yang baru akandidaftarkan.

1. Prosedur yang diperuntukan bagi *e-commerce* yang sudah didaftarkan Prosedur ini dilakukan apabila *e-commerce* yang bersangkutan sudah mendaftarkan diri ke Kominfo dan sudah beroperasi sah secara hukum. Prosedur ini memiliki beberapa tahapan sebagai berikut:
    a. *E-commerce* berkewajiban mengganti sistem keamanan yang digunakan sebelumnya ke sistem *blockchain*;
    b. Selanjutnya, BSSN melakukan pengawasan terhadap penyelenggaraan sistem *blockchain* yang telah diterapkan *e-commerce* tersebut;
    c. Dalam penyelenggaraan sistem *blockchain* tersebut, BSSN berhak melakukan pengujian secara berkala (setiap satu tahun sekali) guna memastikan sistem keamanan *blockchain* masih mampu menyimpan data pribadi secara aman;
    d. Pengujian ini akan menghasilkan status kelayakan yang berupa status “berhasil” dan status “belum berhasil”. Apabila belum berhasil, maka *e-commerce* wajib merevisi sistem

keamanannya untuk diajukan kembali dalam kurun waktu maksimal 60 hari.

Berikut merupakan bagan dari prosedur *regulatory blockchain* yang diperuntukan bagi*e-commerce* yang sudah didaftarkan:

Gambar 4. Bagan dari Prosedur *Regulatory Blockchain* yang Diperuntukan bagi *E-commerce* yang Sudah Didaftarkan.
***Sumber : Olahan sendiri**

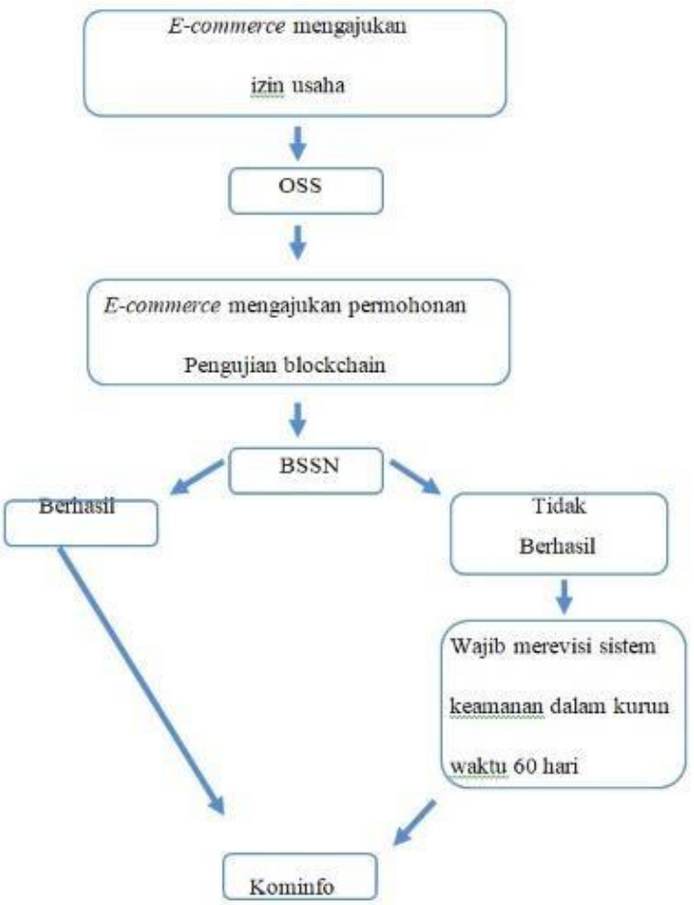
2. Prosedur yang diperuntukan bagi *e-commerce* yang baru akan didaftarkan.

   E-commerce yang dimaksud dalam prosedur ini adalah *e-commerce* yang baru dibentuk dan akan menjalankan proses pengajuan izin usaha. Izin usaha *e-commerce* didapatkan dari Kominfo sesuai dengan PP Nomor 80 Tahun 2019.

   Prosedur ini meliputi beberapa tahapan sebagai berikut:

   a. *E-commerce* mengajukan izin usaha kepada lembaga *Online Single Submission* (OSS). Setelah mendapatkan izin dari lembaga OSS, *e- commerce* melanjutkan tahapan selanjutnya;
   b. *E-commerce* mengajukan permohonan untuk pengujian sistem keamanan *blockchain* ke BSSN;
   c. BSSN melakukan pengujian terhadap sistem *blockhain e-commerce* yang mengajukan permohonan;
   d. Pengujian ini akan menghasilkan status kelayakan yang berupa status "berhasil" dan status "belum berhasil". Apabila belumberhasil, maka *e-commerce* wajib merevisi sistem keamanannya untuk diajukan kembali dalam kurun waktu maksimal 60 hari;
   e. Status "berhasil" yang didapatkan dari BSSN akan digunakan sebagai syarat dalam pengajuan izin penyelenggaraan sistem elektronik ke Kominfo.

Berikut merupakan bagan dari Prosedur yang diperuntukan bagi *e-commerce* yang baru akan didaftarkan:



Gambar 5. Bagan dari Prosedur *Regulatory Blockchain* yang Diperuntukan bagi *E-commerce* yang Baru Akan Didaftarkan.
***Sumber: Olahan sendiri**

Adapun indikator pengujian yang digunakan BSSN dalam penetapan status kelayakan adalah sebagai berikut :

1) Tata kelola sistem perlindungan data pribadi;
2) Sumber daya manusia di bidang informasi dan teknologi (IT) yang memadai;
3) Manajemen risiko dalam menangani kasus kebocoran data;
4) Aspek lainnya yang diperlukan.

Prosedur di atas diharapkan dapat menjadi alternatif penyelesaian bagi pemerintah dan pihak terkait dalam menanggulangi kasus kebocoran data pribadi, khususnya milik pengguna *e-commerce*. Dengan adanya *regulatory blockchain*, maka akan dapat mengisi kekosongan regulasi tentang perlindungan data pribadi di Indonesia. Selain itu, prosedur ini juga memberikan jaminan keamanan data pribadi bagi pengguna *e-commerce*. Oleh karena itu, diperlukan peraturan tertulis yang mengatur terkait *regulatory blockchain* yang dikeluarkan oleh Kominfo.

SIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan penjabaran materi sebelumnya, maka dapat ditarik kesimpulan sebagai berikut:

1) Kasus kebocoran data pribadi pengguna *e-commerce* terus mengalami peningkatan di setiap tahunnya. Misalnya saja, kasus kebocoran data pribadi yang dirasakan oleh para pengguna Tokopedia dan Bukalapak. Melihat seringnya kasus kebocoran data pribadi yang terjadi, maka hal ini tentu harus dijadikan sebagai salah satu fokus utama pemerintah Indonesia dalam rangka melindungi hak pribadi masyarakatnya. Kebocoran data pribadi tersebut disebabkan karena lemahnya sistem keamanan data yang digunakan oleh pihak *e-commerce,* sehingga para peretas dapat dengan mudah masuk dan mencuri data pribadi milik pengguna *e-commerce* tersebut. Selain itu, kasus kebocoran data pribadi juga dapat disebabkan oleh kurangnya regulasi khusus terkait perlindungan data pribadi yang bersifat lebih mengikat dan lebih kuat. Oleh karena itu, diperlukan sebuah kebijakan yang mewajibkan seluruh *e-commerce* menggunakan sistem keamanan data yang baru, yaitu *blockchain*, serta diperlukan juga penetapan regulasi khusus terkait perlindungandata pribadi, guna menekan angka kasus kebocoran data pribadi pengguna *e-commerce* di Indonesia.
2) Solusi yang dapat digunakan dalam menyelesaikan permasalahan terkait kebocoran data pribadi pengguna *e-commerce* yaitu dengan menggunakan sistem keamanan *blockchain*. *Blockchain* menggunakan teknik *peer to peer* dan *sharing security* dalam penyimpanan datanya, sehingga data pribadi tidak akan mudah diretas atau dicuri. Penggunaan sistem keamanan *blockchain* memerlukan sebuah regulasi yang mewajibkan semua *e-commerce* yang disebut *regulatory blockchain*. Regulasi tersebut dikeluarkan dan ditetapkan oleh Kominfo, selaku lembaga yang berwenang untuk menangani kasus terkait kebocoran data pribadi. Kewenangan ini juga sebagai salah satu bentuk pelaksanaan dari PP Nomor 80 Tahun 2019. Regulatory blockchain mengatur dua jenis prosedur pengujian blockchain, yaitu prosedur yang diperuntukkan bagi e-commerce yang sudah didaftarkan dan prosedur yang diperuntukkan bagi e-commerce yang baru akan didaftarkan.

B. Saran

Dalam rangka menguatkan regulasi terkait perlindungan data pribadi di Indonesia, maka diperlukan pengesahan dan pemberlakuan terkait undang-undang perlindungan data pribadi.Selain itu, diperlukan pula regulasi terkait penggunaan sistem keamanan blockchain bagi e-commerce, yang dinamakan dengan regulatory blockchain.Dengan adanya regulatory blockchain, diharapkan dapat mengurangi angka kasus kebocoran data.

DAFTAR PUSTAKA

Buku:

Qin, Zheng. 2009. *Introduction to E-commerce*. Beijing: Tsinghua University Press.

Kenneth, L., dan J. Laudon. 2007. *Management Information System* Jakarta: Salemba Empat.

Priatna, T. 2019. *Disrupsi Pengembangan Sumber Daya Manusia Dunia Pendidikan Di Era Revolusi Industri 4.0* Bandung: Pusat Penelitian dan Penerbitan UIN Sunan Gunung Djati Bandung.

Muhammad, A. 2004. *Hukum dan Penelitian Hukum*. Bandung: Citra Aditya Bakti. Fajar, M., dan Yulianto Achmad. 2010. *Dualisme Penelitian Hukum Empiris danNormatif*. Yogyakarta: Pustaka Pelajar.

Fajar, dkk. 2009. *Dualisme Penelitian Hukum Normatif dan Empiris*. Yogyakarta: Pustaka Pelajar.

Amirudin. 2006. *Pengantar Metode Penelitian Hukum*. Jakarta: Raja Grafindo Prasada.

UNCTAD. 2015. *Report no. TD/B/C.II/EM.5/2: Trade and Development Board; Investment, Enterprise, and Development Commission Expert Meeting on Cyber laws and Regulations for Enhancing E-Commerce* . United Nations. Geneva.

Jurnal:

Marita, L.S. 2015. *Cyber Crime dan Penerapan Cyber Law Dalam Pemberantasan Cyber Law Di Indonesia*, Cakrawala 15(2): 2.

Suwardana, H. 2018. *Revolusi Industri 4.0 Berbasis Revolusi Mental*, Jati Unik 2(1): 110-111.

Rahardja, U., A. Qurotul, Y. Muhamad, E. Aulia. 2020. *Penerapan Teknologi Blockchain sebagai Media Pengaman Proses Transaksi E-Commerce*, CESS (Journal of Computer Engineering System and Science) 5(1): 29.

Rosadi, S.D. 2018. *Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital di Indonesia*, VeJ Fakultas Hukum Universitas Padjajaran 4(1): 95.

Tesis/Disertasi/Skripsi:

Naufal, R.A. 2020. Tanggung Jawab PT Tokopedia dalam Kasus Kebocoran Data Pribadi Pengguna. *Skripsi*. Universitas Islam Indonesia. Yogyakarta.

Website Resmi:

Asosiasi Penyelenggara Telekomunikasi Seluruh Indonesia (ATSI). 2020. Rapat Dengar Pendapat Umum DPR RI-ATSI RUU Perlindungan Data Pribadi. https://www.atsi.or.id/atsi-menghadiri-rdpu-dengan-komisi-i-dpr-ri/.7 Agustus 2021.

Kamus Besar Bahasa Indonesia. https://kbbi.kemdikbud.go.id/. 5 Agustus 2021.

Hidayah, A.A., E. Shila. 2020. Kasus Kebocoran Data Semakin Banyak, Belanja Daring Paling Rentan. Lokadata. https://lokadata.id/artikel/kasus-kebocoran- data-semakin-banyak-belanja-daring-paling-rentan. 7 Agustus 2021.

Universitas Islam Indonesia. 2021. Blockchain Tingkatkan Keamanan Data Dari Peretasan. https://www.uii.ac.id/blockchain-tingkatkan-keamanan-data-dari- peretasan/. 5 Agustus 2021.

Harris, C. 2018. The History of Bitcoin. Crypto Currency News. (https://cryptocurrencynews.com/the-history-of-bitcoin/. 6 Agustus 2021.

Satoshi, N. 2002. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf. 7 Agustus 2021.

International Business Machines Corporation (IBM). Welcome to IBM Blockchain. https://www.ibm.com/blockchain. 7 Agustus 2021.

Hendraswara, E.P. Blockchain From a Society's Perspective. Indonesia Blockchain Society. https://files.acci.or.id/files/presentation/ibs-blockchain-from-a- society-perspective.pdf. 7 Agustus 2021.

Universitas Brawijaya. Pengenalan Peer-to-peer (P2P). http://blog.ub.ac.id/novianihasianna/files/2012/10/PENGENALAN- PEER.pdf. 13 Agustus 2021.

Wicaksono, A. 2020. Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan Dijual. CNN Indonesia, (https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual. 06 Agustus 2021.

Wicaksono, A. 2020. 13 Juta Data Bocor Bukalapak Dijual di Forum Hacker, CNN Indonesia. https://www.cnnindonesia.com/teknologi/20200506065657-185-500477/13-juta-data-bocor-bukalapak-dijual-di-forum-hacker. 07 Agustus 2021.

Prosiding:

Pallingi, S. C. Eric. Limbongan. 2022. *Pengaruh Internet Terhadap Industri Ecommerce dan Regulasi Perlindungan Data Pribadi Pelanggan di Indonesia.* Prosiding Seminar Nasional Riset dan Teknologi (SEMNAS RISTEK) Jakarta. Universitas Indraprasta PGRI: 226.