Juridical Analysis of Illegal Information Access: Case Study on Sales of Data Patients Covid-19

(Analisis Yuridis Akses Informasi Ilegal: Studi Kasus Penjualan Data Pasien Covid-19)

Kessa Hendriyanto
email: kessahendriyanto@gmail.com

Master of Law, Diponegoro University

***Abtract*:** *Increasingly sophisticated technology and information systems provide their own risks, namely with the presence of cyber of cyberspace (cybercrime). The fundamental foundation of the emergence of crime, whatever its type and kind, is still largely based on the profit and personal gain motive.*

Information related to COVID-19 patients is sensitive information in the community lately. Some parties refuse to disseminate COVID-19 patient data due to privacy and security reasons, while those who support it reason that it needs to be done in the context of contact tracing in order to prevent the dissemination of the COVID-19 pandemic.

With the case of selling COVID-19 patient data through an online forum, demanding a study in the aspect of the impact of COVID-19 patient data distribution. In addition, the study was also carried out related to arrangements in the field of health, the field of public information disclosure, and the field of information and electronic transactions to find out what was the basis of the Government in determining public policy.

In this case, the Government implement public policy to disseminate data on COVID-19 patients on a limited basis, namely by not providing detailed information.

Keywords: *COVID-19 Patient Data, Public Information Disclosure, Privacy, Contact Tracing*

Abstrak: Semakin canggihnya sistem teknologi dan informasi memberikan risiko tersendiri, yaitu dengan adanya kejahatan siber atau dunia maya (*cybercrime*). Landasan fundamental timbulnya kejahatan, apapun jenis dan macamnya, sebagian besar masih didasarkan pada motif *profit* dan *personal gain*.

Informasi terkait dengan pasien COVID-19 merupakan informasi yang sensitif di masyarakat akhir-akhir ini. Beberapa pihak menolak untuk menyebarluaskan data pasien COVID-19 dengan alasan privasi dan keamanan, sedangkan pihak yang mendukungnya beralasan hal tersebut perlu dilakukan dalam rangka *contact tracing* demi mencegah penyebarluasan pandemi COVID-19.

Dengan adanya kasus penjualan data pasien COVID-19 melalui forum *online*, menuntut akan adanya kajian terkait dampak tersebarnya data paseien COVID-19. Selain itu, kajian juga dilakukan terkait dengan pengaturan di bidang kesehatan, bidang keterbukaan informasi publik, dan bidang informasi dan transaksi elektronik untuk mengetahui apa yang dijadikan landasan Pemerintah dalam menentukan kebijakan publik.

Dalam hal ini, Pemerintah melaksanakan kebijakan publik untuk melakukan penyebarluasan data pasien COVID-19 secara terbatas, yaitu dengan tidak memberikan informasi detail.

Kata Kunci: Data Pasien COVID-19, Keterbukaan Informasi Publik, Privasi, *Contact Tracing*

PENDAHULUAN

Secara konstitusional, Negara harus melindungi privasi dan data penduduk masyarakat. Ketentuan tersebut diatur dalam ketentuan Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUDNRI 1945) yang menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi. Perubahan teknologi digital dalam beberapa dekade terakhir telah membawa banyak perubahan bagi peradaban dunia. Perubahan tersebut terasa dampaknya bagi dunia sosial, yaitu bagaimana kita berkomunikasi, bertukar informasi, berpartisipasi dalam perdagangan, dan lain sebagainya. Semakin canggihnya sistem teknologi dan informasi memberikan risiko tersendiri, yaitu dengan adanya kejahatan siber atau dunia maya.

Kejahatan siber (*cybercrime*) saat ini tidak lagi dipandang sebagai *emerging threat*. Hal ini karena dampak nyata sudah terlihat mengakar dalam kehidupan kita sehari-hari. Landasan fundamental timbulnya kejahatan, apapun jenis dan macamnya, sebagian besar masih didasarkan pada motif *profit* dan *personal gain*. Hal yang berubah terletak pada alat, metode, dan sistem yang digunakan pada pelaku kejahatan untuk mencapai tujuan mereka. Teknologi dunia siber memberikan sarana baru bagi pelaku kejahatan untuk menyerang siapapun yang rentan dan memberikan histeria ketakutan kepada para korbannya. *Modern cybercrime*, tidak lagi membedakan target. Pemerintah, korporasi, termasuk individu dapat dieksploitasi untuk memperoleh keuntungan (Jeffray & Feakin, 2015).

Setiap masyarakat tentunya sering berinteraksi dengan Pemerintah untuk menerima pelayanan publik. Dalam pelayanan publik tersebut, biasanya dilakukan melalui proses pengumpulan dan pengolahan data. Ketika masyarakat membutuhkan pelayanan publik, data diperoleh melalui interaksi antara Pemerintah dengan masyarakatnya. Data yang dibutuhkan umumnya data terkait identitas masyarakat dan pelayanan terkait yang mereka butuhkan. Pemerintah kemudian menyimpan data dalam suatu *database*. Data tersebut digunakan oleh Pemerintah untuk memberikan pelayanan kepada masyarakat; data dianalisa oleh Pemerintah untuk memberikan keputusan atau tindakan terhadap permohonan pelayanan publik yang diajukan masyarakat (Scholta et al., 2019).

Pandemi COVID-19 saat ini memberikan dampak cukup besar bagi masyarakat. Dampak dirasakan masyarakat yaitu pada aspek kesehatan, sosial, dan ekonomi, termasuk meningkatnya jumlah penduduk miskin (Thaariq et al., 2020). Belum lama ini, heboh berita yang mengabarkan bahwa telah terjadi penjualan data penanganan kasus pandemi COVID-19 di Indonesia melalui forum *online* 'RaidForums'. Pelaku yang memakai akun bernama 'Database Shopping' berusaha menjual data tersebut kepada pihak yang berminat tanpa menyebut harga. Pelaku dalam hal ini memberikan bocoran data. Data yang dibocorkan terdiri atas nama, tanggal laporan, alamat lengkap, kondisi kesehatan, tanggal pengambilan sampel, riwayat kontak, dan sebagainya (Ramadhanny, 2020).

Informasi terkait dengan pasien COVID-19 merupakan informasi yang sensitif di masyarakat akhir-akhir ini. Kasus 230 ribu data tes COVID-19 warga Indonesia yang dipajang di forum *online* 'RaidForums' pada tanggal 18 Juni 2020 mengagetkan banyak orang. Data yang dijual dapat dikatakan cukup lengkap, mulai dari nama, umur, nomor telepon, alamat rumah, Nomor Identitas Kependudukan (NIK), hasil *rapid test*, hasil *Polymerase Chain Reaction* (PCR), hingga status terkait COVID-19. Menurut chairman dan pendiri Indonesia Cyber

Security Forum, Ardi Sutedja, data-data yang bocor mengkhawatirkan karena bukan hanya berisi data pribadi, namun juga data kesehatan.

Menurut Ardi Sutedja, data-data yang bocor tersebut berpotensi untuk semakin disalahgunakan. Data-data yang bocor dapat dimanfaatkan orang yang tidak bertanggung jawab untuk memalsukan identitas atau penipuan. Data-data kesehatan tersebut juga sangat bernilai bagi industri farmasi dan kesehatan karena dapat dijadikan data riset gratis bagi industri farmasi global. Apabila kebocoran data tersebut terbukti benar, maka akan berdampak buruk bagi penanganan COVID-19 di Indonesia. Kejadian tersebut tentunya dapat menimbulkan ketidakpercayaan publik terhadap kemampuan Pemerintah dalam mengelola serta melindungi data dan privasi pasien COVID-19. Hal ini karena data-data pasien COVID-19 pada dasarnya merupakan informasi rahasia (Tim - detikInet, 2020).

Hal serupa juga diungkapkan oleh pengamat keamanan siber, Pratama Persadha, yang mengatakan bahwa kebocoran data 230 ribu pasien COVID-19 di Indonesia memiliki risiko serius khususnya bagi pasien, karena terdapat data alamat rumah dan statusnya. Dalam hal ini pasien berisiko dijauhi secara sosial karena masih ada bagian di masyarakat yang bersikap berlebihan pada pengidap COVID-19. Sedangkan bagi negara, kebocoran data pasien COVID-19 berisiko menciptakan kegaduhan di tengah masyarakat. Hal ini karena masih banyak masyarakat yang mudah tersulut dengan isu COVID-19. Gesekan horisontal dapat timbul misalnya melakukan pengucilan bahkan pengusiran. Oleh karena itu, kasus kebocoran data pasien COVID-19 ini harus segera diselidiki dan peraturan hukum yang memayunginya harus ditegakkan (Haryanto, 2020b).

Di lain sisi, ada pihak yang berkehendak supaya data pasien COVID-19 dapat diketahui umum. Menurut mereka, hal tersebut dilandaskan pada prinsip keterbukaan informasi sekaligus untuk mempermudah proses pelacakan kontak (*contact tracking*) COVID-19. Oleh karena itu, perlu kajian mengenai dampak dan konsekuensi dari penyebarluasan data pasien COVID-19 dari sisi hukum. Sedangkan terkait bocornya data pasien COVID-19 perlu juga ditinjau dari sisi hukum, yaitu bagaimana hukum positif yang mengatur akan tindakan tersebut, baik apabila dilakukan oleh tenaga medis, maupun oleh orang lain, termasuk pula bagaimana jika perolehan data dilakukan secara sah atau secara melawan hukum. Hal ini merupakan kasus 'kekinian' yang belum banyak dibahas dalam bentuk penelitian ilmiah, yang mana dengan demikian di sinilah letak *state of the art* dari penelitian ini. Melalui penelitian ini, diharapkan memberi gambaran akan dampak yang ditimbulkan dari bocornya data pasien COVID-19, baik dari segi sosial maupun dari segi hukum.

RUMUSAN MASALAH

Berdasarkan uraian latar belakang di atas, rumusan masalah yang hendak dibahas dalam penelitian ini adalah: *Pertama*, bagaimana dampak bocornya data pasien COVID-19 di masyarakat? *Kedua*, bagaimana kebocoran data pasien COVID-19 ditinjau dari sisi hukum positif Indonesia?

METODE PENELITIAN

Penelitian ini dilakukan dengan menggunakan pendekatan perundang-undangan (*statute approach*), yaitu menelaah semua peraturan perundang-undangan yang terkait dengan permasalahan yang akan dibahas (Marzuki, 2019). Dalam hal ini peraturan perundang-undangan yang ditelaah yaitu terkait dengan keterbukaan data kesehatan pasien, baik

dalam lingkup pengaturan bidang kesehatan, bidang keterbukaan informasi publik, dan bidang informasi dan transaksi elektronik. Melalui pendekatan ini, dapat ditelaah bentuk konsistensi dan kesesuaian antar peraturan perundang-undangan, baik secara vertikal maupun secara horisontal. Kemudian, hasil telaah peraturan perundang-undangan tersebut diharapkan dapat diambil suatu masukan dalam menyelesaikan permasalahan yang ada di lapangan.

Sumber-sumber penelitian hukum diperlukan demi memecahkan permasalahan hukum selaigus untuk memberikan gambaran mengenai apa yang seharusnya dilakukan. Sumber-sumber penelitian hukum tersebut, dapat dibedakan menjadi bahan hukum primer dan bahan hukum sekunder. Bahan hukum primer yang digunakan dalam penelitian ini yaitu peraturan perundang-undangan di bidang kesehatan, bidang keterbukaan informasi publik, dan bidang informasi dan transaksi elektronik. Sedangkan untuk mempertajam pembahasan, digunakan bahan hukum sekunder yaitu berupa informasi dari media massa, buku, dan jurnal ilmiah demi memperoleh masukan dan keterangan tambahan.

PEMBAHASAN

1. Dampak Bocornya Data Pasien COVID-19 di Indonesia

Konsep mengenai privasi informasi telah lahir sebelum teknologi informasi dan komunikasi berkembang seperti saat ini. Pada tahun 1986, Mason memberikan pendapat bahwa meningkatkan pokok perhatian akan meningkatnya penggunaan teknologi informasi, atau 'era informasi', akan mengarah pada *four ethical issues*, yaitu *Privacy*, *Accuracy*, *Property*, and *Accessibility* (PAPA). Prediksi ini terbukti seluruhnya akurat, terutama terkait dengan privasi, yang mana hal ini senantiasa menjadi perhatian yang sering dibahas (Belanger & Crossler, 2011).

Pada dasarnya, privasi jika dikaitkan dengan perlindungan terhadap informasi elektronik, dapat dikategorikan menjadi *communication privacy* dan *information privacy* (Utama et al., 2016). *Communication privacy* merupakan privasi seseorang dalam berkomunikasi, dengan alat komunikasi seperti telepon, surel, atau bentuk komunikasi lainnya. Sedangkan *information privacy* merupakan privasi atas data informasi pribadi, seperti informasi mengenai keuangan, kesehatan, tempat tinggal, dan sebagainya. Konsep privasi, dalam hal ini mengatur mengenai hak-hak privasi seseorang, yaitu bagaimana seseorang dapat memperoleh dan pemberian akses terhadap informasi pribadinya.

Mengutip pandangan Immanuel Kant, bahwa setiap manusia harus diperlakukan dengan hormat. Salah satu cara memperlakukan manusia dengan hormat yaitu dengan menghargai adanya *individual autonomy*. Hal yang membedakan manusia dengan makhluk lain di muka bumi ini yaitu manusia memiliki kebebasan (*autonomus*). Landasan *autonomus* menurut Kant, yaitu rasionalitas dan moralitas. Oleh karena kita adalah makhluk yang *autonomus*, maka kita mampu berpikir rasional untuk mengambil keputusan (*making laws unto ourselves*), sebagai subyek dari hukum yang bermoral (Bowie & Jamal, 2006).

Joseph Kupfer menjelaskan pemahaman *moral autonomy* Kant dengan lebih luas yaitu dikaitkan dengan privasi sebagai sesuatu yang sifatnya *self-determining*. Privasi menurutnya, merupakan prakondisi yang dibutuhkan manusia sebagai makhluk yang *autonomus*. *"Privacy is necessary for an efficacious self-concept and an efficacious self-concept is in turn required if one is to be an autonomous self"*. Konsep privasi yaitu

mengizinkan kepada siapa kita dapat berbagi informasi personal. Kendali atas kepada siapa kita berbagi informasi personal tersebut dapat menjelaskan hubungan sosial kita dengannya, yaitu apakah teman atau sekedar kenalan, termasuk apakah orang atau pihak tersebut menurut kita dapat benar-benar dipercaya (*trustworthy*). Oleh karena itu, kita tidak dapat menjadi makhluk yang *autonomus* kecuali kita memiliki privasi atas informasi personal (Kupfer, 1987).

Suatu hal yang perlu dikaji yaitu sejauh mana hukum dapat melindungi privasi seseorang. Nilai moral atas *right to privacy* perlu disandingkan dengan pandangan utilitarianisme, yaitu apakah *right to privacy* benar-benar sudah masuk akal untuk dilaksanakan. Atau dengan kata lain, apakah implementasi nilai moral dalam perlindungan atas privasi tersebut justru akan menganggu kepentingan masyarakat. Sebagaimana Gerald Dworkin pernah katakan, *"The right to privacy cannot be absolute; it must yield on occasions to other interesets which society considers to be of greater importance"* (Corlett, 2002).

Ketika pertama kali Pemerintah Indonesia mengumumkan secara resmi dua orang yang terjangkit virus Covid-19, banyak masyarakat yang keberatan dengan dibukanya informasi pada publik terkait nama, tempat domisili, dan riwayat perjalanan dari pasien. Namun, sejalan dengan semakin besarnya jumlah orang yang terjangkit, hasil survei persepsi publik yang diadakan Lembaga Ilmu Pengetahuan Indonesia (LIPI) bersama sejumlah perguruan tinggi seperti Universitas Indonesia (UI), Institut Teknologi Bandung (ITB), dan Universitas Gajah Mada (UGM) menunjukkan ada perubahan sikap mayoritas responden. Berdasarkan survei yang mereka lakukan pada 20-21 Maret 2020, diketahui bahwa mayoritas responden sebesar 61,2% menyetujui nama pasien positif COVID-19 dibuka ke publik. Kemudian, yang menyetujui alamat domisilinya dibuka sampai tingkat kecamatan sebesar 64%, lalu dibuka sampai kelurahan sebanyak 60,8% (Mappapa, 2020).

Desakan keterbukaan informasi dari Pemerintah terkait dengan COVID-19 datang dari kalangan dokter. Dalam hal ini, Ketua Umum Pengurus Pusat Ikatan Dokter Anak Indonesia (PP IDAI), Aman B. Palungan, yang menginginkan penyampaian data pasien COVID-19 yang dirawat. Transparansi hasil tes dan klaster secara *real time* perlu dilakukan untuk memudahkan upaya *contact tracing* sehingga dapat meminimalkan penyebaran virus. Selain itu, Ketua Umum PB Ikatan Dokter Indonesia, Daeng Mohammad Faqih, yang menekankan pentingnya informasi terkait siapa nama pasien dan tempat tinggalnya untuk melakukan *contact tracing* secara ekfektif. Dibukanya rahasia kedokteran tersebut dilakukan dengan mempertimbangkan kepentingan masyarakat (JawaPos.com, 2020).

Merujuk pada technical guidance regarding contact tracing in the context of COVID-19 yang diterbitkan WHO pada tanggal 10 Mei 2020, dijelaskan bahwa COVID-19 disebabkan oleh virus SARS-CoV-2 yang menyebar dari orang-ke-orang melalui *droplet* dan hubungan kontak. *Contact tracing* merupakan salah satu strategi komprehensif untuk mengendalikan penyebaran virus tersebut. *Contact tracing* pada dasarnya merupakan suatu *process of identifying, assessing, and managing people who have been exposed to a disease to prevent onward transmission.*

Contact tracing penting dilakukan terhadap COVID-19 *case*, yaitu bukan hanya terhadap orang yang sudah *confirmed* (terkonfirmasi positif COVID-19), namun juga mereka yang masih *suspect* atau *probable* COVID-19 (di Indonesia diklasifikasikan sebagai orang dalam pemantauan dan pasien dalam pengawasan). *Contact* dalam hal ini, antara lain mereka yang dalam waktu 2 sampai dengan 14 hari: berada dalam jarak 1 meter dengan COVID-19

case selama lebih dari 15 menit; melakukan kontak fisik langsung dengan COVID-19 *case*; dan memberikan perawatan langsung kepada pasien dengan COVID-19 tanpa menggunakan perlengkapan yang memadai. Data *contact* tadi lalu dimasukkan ke dalam suatu *database* untuk kemudian dilakukan monitoring secara berkala.

Tak dapat dipungkiri, *contact tracing* memang merupakan upaya pencegahan penyebaran lebih lanjut COVID-19 di Indonesia. Namun, dalam *technical guide* terkait dengan *contact tracing* tersebut, WHO tetap menekankan akan pentingnya *data protection*, yaitu disebutkan bahwa:

> *"The ethics of public health information, data protection, and data privacy must be considered at all levels of contact tracing activities, in all training activities for contact tracing, and when implementing contact tracing tools. In particular:*
>
> - *Safeguards must be in place to guarantee privacy and data protection in accordance with the legal frameworks of the countries where systems are implemented.*
> - *Everyone involved in contact tracing must adhere to the ethical principles of handling personal information, to ensure responsible data management and respect for privacy throughout the process.*
> - *How data will be handled, stored, and used needs to be communicated to those concerned in a clear and transparent manner. This is important for buy-in and engagement as well as to avoid misperceptions that could jeopardize the effectiveness of a contact tracing programme.*
> - *Digital tools used for contact tracing should be assessed before use to ensure safeguarding data protection according to national regulations."*

Dengan kata lain, mereka yang yang terlibat dalam proses pengumpulan, penyimpanan, dan penggunaan data harus memastikan tanggung jawabnya akan manajemen data dengan menghargai privasi berdasarkan ketentuan hukum masing-masing negara. Terkait dengan hal ini, maka kita perlu melihat ketentuan peraturan perundang-undangan di Indonesia.

Kitab Undang-Undang Hukum Pidana (KUHP), dalam ketentuan Pasal 322 mengatur bahwa mereka yang dengan sengaja membuka rahasia yang wajib disimpannya karena jabatan atau pencariannya diancam dengan pidana penjara paling lama sembilan bulan. Ketentuan dalam Pasal 322 KUHP tersebut merupakan delik aduan, yang berarti bahwa perbuatan membuka rahasia tersebut hanya dapat dituntut atas pengaduan orang yang rahasianya dibuka. Ketentuan larangan membuka rahasia di KUHP tersebut menurut PB IDI, dapat disimpangi dengan peraturan perundang-undangan lain berdasarkan asas *lex specialis derogat lex generalis*, yaitu ketentuan yang diatur dalam:

a. Pasal 48 Undang-Undang Nomor 29 Tahun 2004 tentang Praktik Kedokteran,
b. Pasal 57 Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan,
c. Pasal 38 Undang-Undang Nomor 44 Tahun 2009 tentang Rumah Sakit, dan
d. Pasal 73 Undang-Undang Nomor 36 Tahun 2014 tentang Tenaga Kesehatan.

Ketentuan Pasal 48 ayat (2) UU 29/2004 menyebutkan bahwa, rahasia kedokteran dapat dibuka hanya untuk kepentingan kesehatan pasien, memenuhi permintaan aparatur penegak hukum dalam rangka penegakan hukum, permintaan pasien sendiri, atau berdasarkan ketentuan perundang-undangan. Ketentuan Pasal 57 ayat (2) UU 36/2009 menyebutkan bahwa ketentuan mengenai hak atas rahasia kondisi kesehatan pribadi

tidak berlaku dalam hal: a. perintah undang-undang; b. perintah pengadilan; c. izin yang bersangkutan; d. kepentingan masyarakat; atau e. kepentingan orang tersebut.

Ketentuan Pasal 38 ayat (2) UU 44/2009 menyebutkan bahwa Rahasia kedokteran hanya dapat dibuka untuk kepentingan kesehatan pasien, untuk pemenuhan permintaan aparat penegak hukum dalam rangka penegakan hukum, atas persetujuan pasien sendiri, atau berdasarkan ketentuan peraturan perundang-undangan. Sedangkan ketentuan Pasal 73 ayat (2) UU 36/2014, menyebutkan bahwa Rahasia kesehatan Penerima Pelayanan Kesehatan dapat dibuka hanya untuk kepentingan kesehatan Penerima Pelayanan Kesehatan, pemenuhan permintaan aparatur penegak hukum bagi kepentingan penegakan hukum, permintaan Penerima Pelayanan Kesehatan sendiri, atau pemenuhan ketentuan Peraturan Perundang-undangan.

Dengan demikian, dapat dipahami bahwa keempat ketentuan peraturan perundang-undangan di bidang kesehatan tersebut mengatur mengenai rahasia kedokteran. Rahasia kedokteran, sebagai segala sesuatu yang berhubungan dengan hal yang ditemukan oleh dokter, tenaga medis, atau jasa pelayanan kesehatan dicatat sebagai rekam medis yang dimiliki pasien dan sifatnya rahasia. Rahasia tersebut maksudnya hanya dapat dibuka oleh orang/pasien yang bersangkutan, dalam rangka kepentingan masyarakat, atau berdasarkan ketentuan peraturan perundang-undangan. Yang menjadi pertanyaan, yaitu apakah kepentingan masyarakat sudah tepat menjadi justifikasi untuk membuka data pasien COVID-19 ke khalayak umum.

Belum adanya vaksin COVID-19, prediksi akan adanya *second wave*, tertularnya kembali (*repeat of contagion*), kematian, *lockdown*, dan potensi kehancuran perekonomian, dapat menimbulkan tegangan dan kecemasan pada tingkat internasional dan domestik (Bet-El, 2020). COVID-19 merupakan ancaman terbesar di dunia saat ini. Terus menjalarnya penderita COVID-19 dapat membahayakan tatanan sosial masyarakat bukan hanya domestik, tapi juga internasional. Oleh karena itu, Pemerintah harus memikirkan skema kebijakan publik yang dapat keamanan dan keutuhan Negara Kesatuan Republik Indonesia.

Sebagaimana kita ketahui, pandemi COVID-19 menimbulkan kepanikan dunia. Tidak ada masyarakat manapun yang siap menghadapinya. Beberapa orang melakukan tindakan yang kurang pantas secara moral dan etika. Presiden Amerika Serikat, Donald Trump, beberapa kali mengeluarkan ucapan yang dianggap menghina Negara Tiongkok dengan menyebut COVID-19 sebagai *China Virus*, atau yang terakhir dengan sebutan virus *Kung Flu*. Tak dapat dipungkiri, pandemi COVID-19 telah menimbulkan diskriminasi dan stigma pada kalangan tertentu, termasuk pada pasien COVID-19.

Mengatasi pandemi COVID-19 secara medis memang sulit, tetapi yang lebih sulit yaitu keluar dari ketakutan dan kepanikan yang disebabkan olehnya. Ketakutan dan kepanikan akan jatuhnya korban akibat virus COVID-19 itu sendiri dapat menimbulkan korban, karena di sini kita bicara akan emosi dan sensitivitas masyarakat (Malik & Naeem, 2020). Di Indonesia ketakutan dan kepanikan telah mengakibatkan tindakan diskriminasi dan stigma. Tentu kita tak lupa, betapa banyaknya penolakan terhadap tenaga asing yang masuk ke Indonesia, terlebih ketika datangnya dari Tiongkok. Selain itu, diskriminasi dan pengucilan juga terjadi pada tenaga medis yang menangani pasien COVID-19. Mereka ditolak untuk kembali ke lingkungan tempat mereka tinggal. Penolakan akan penguburan jenazah pasien COVID-19 di berbagai tempat juga merupakan bukti nyata akan adanya diskriminasi pasien COVID-19.

Pemerintah Indonesia, hingga saat penelitian ini dilakukan, tidak pernah menyampaikan informasi secara detail pasien COVID-19 di Indonesia. Merujuk pada laman resmi Gugus Tugas Penanganan COVID-19, covid19.go.id, Pemerintah hanya memberikan informasi jumlah dan peta sebaran hingga tingkat provinsi dan kabupaten/kota. Laman tersebut memuat informasi jumlah beserta sebaran pasien yang terkonfirmasi positif, pasien dalam perawatan, sembuh, dan meninggal serta informasi terkait, seperti berita terkini, edukasi, tanya jawab, dan sebagainya. Sedangkan Pemerintah Provinsi DKI Jakarta, melalui laman resminya corona.jakarta.go.id, hanya memberikan informasi jumlah dan peta sebaran hingga tingkat kelurahan. Dengan kata lain, tidak ada informasi detail hingga nama yang terkonfirmasi positif, termasuk detail alamat lengkapnya.

Merujuk pada ketentuan umum Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (UU KIP), dapat kita ketahui bahwa Pemerintah, melalui badan publik, menyimpan dan mengelola informasi publik. Informasi publik tersebut, terbagi ke dalam 2 (dua) jenis, yaitu informasi yang wajib disediakan dan diumumkan serta informasi yang dikecualikan. Terkait dengan data kesehatan pasien, sebagaimana disebutkan dalam ketentuan Pasal 17 huruf h angka 2, termasuk ke dalam informasi yang dikecualikan, yaitu informasi publik yang apabila dibuka dan diberikan dapat mengungkap rahasia pribadi, seperti riwayat, kondisi dan perawatan, pengobatan kesehatan fisik, dan psikis seseorang. Oleh karena itu, maka data pasien COVID-19 berdasarkan UU KIP merupakan informasi yang harus dirahasiakan. Ketentuan larangan mengungkap data pasien tersebut, sebagaimana disebutkan dalam ketentuan Pasal 18 ayat (2) huruf a UU KIP, hanya dapat dikecualikan antara lain apabila pihak yang rahasianya diungkap memberikan persetujuan tertulis.

Sedangkan ketentuan Pasal 10 UU KIP, menyebutkan bahwa badan publik wajib mengumumkan secara serta merta suatu informasi yang dapat mengancam hajat hidup orang banyak dan ketertiban umum. Penyebarluasan informasi publik tersebut disampaikan dengan cara yang mudah dijangkau masyarakat dan dengan bahasa yang mudah dipahami. Sepintas, ketentuan yang dapat dijadikan landasan untuk membuka data pasien COVID-19. Namun, perlu diketahui bahwa, batasan penyebarluasan informasi tersebut, yaitu demi hajat hidup orang banyak dan ketertiban umum. Oleh karena itu, jangan sampai penyebarluasan informasi data pasien COVID-19 justru dapat merusak ketertiban umum.

Lebih lanjut, pengaturan mengenai informasi yang dikecualikan berpedoman pada asas kerahasiaan. Sebagaimana disebutkan dalam ketentuan Pasal 2 ayat (2) UU KIP, bahwa informasi publik yang dikecualikan bersifat ketat dan terbatas. Sedangkan ketentuan Pasal 2 ayat (4) UU KIP, menjelaskan bahwa informasi yang dikecualikan bersifat rahasia sesuai dengan undang-undang, kepatutan, dan kepentingan umum yang didasarkan pada pengujian mengenai konsekuensi yang timbul jika suatu informasi yang diberikan kepada masyarakat serta telah dipertimbangkan dengan seksama bahwa menutup informasi publik tersebut justru dapat melindungi kepentingan yang lebih besar dibandingkan membukanya atau sebaliknya.

Dengan demikian, kiranya dapat dipahami kiranya bahwa Pemerintah dalam hal ini, memposisikan data pasien COVID-19 sebagai informasi publik yang dikecualikan. Informasi publik yang dikecualikan tersebut bersifat ketat dan terbatas. Informasi data pasien COVID-19 tentunya tidak benar-benar tertutup. Dalam hal ini, informasi data pasien COVID-19 digunakan oleh pihak-pihak terkait dalam penanganan COVID-19 dan

diberikan secara terbatas kepada masyarakat. Terbatas maksudnya tidak sampai ke detail nama dan alamat lengkap, namun pada *scope* tertentu, seperti kelurahan dan kabupaten/kota.

2. Kajian Yuridis Kasus Bocornya Data Pasien COVID-19 di Indonesia

Identitas pada dasarnya merupakan *person's uniqueness* yang membedakan antara orang yang satu dengan orang lainnya. Dalam identitas terdapat atribut pribadi yang membuatnya dapat dikenali (*recognizable*). Ketika bicara mengenai sistem manajemen data identitas, di dalamnya terdapat dua hak asasi manusia yang saling berkaitan, yaitu *right to privacy* dan *right to data protection* (Kulhari, 2018). Kedua hak asasi manusia tersebut, sering kali dilanggar, terlebih di zaman perkembangan teknologi dan informasi yang semakin pesat.

Pemanfaatan teknologi informasi, media, dan komunikasi telah mengubah perilaku masyarakat dan peradaban dunia secara global. Teknologi informasi menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, juga menjadi sarana efektif perbuatan melawan hukum. Perkembangan ilmu pengetahuan dan teknologi membawa perubahan pada pola perilaku manusia di segala aspek kehidupan. Dalam hal ini, kemajuan teknologi seperti komputer dan internet memunculkan jenis kejahatan baru yang disebut *cybercrime*, yang merupakan bentuk atau dimensi baru kejahatan masa kini (Jaya, 2018).

Aktivitas pokok dari *cybercrime* adalah penyerangan terhadap *content*, *computer system*, dan *communication system* di dalam *cyberspace*. Fenomena *cybercrime* memang harus diwaspadai karena kejahatan ini agak berbeda dengan kejahatan lain pada umumnya. *Cybercrime* dapat dilakukan tanpa mengenal batas teritorial dan tidak memerlukan interaksi langsung antara pelaku dengan korban kejahatan (Pahajow, 2016). Oleh karena itu, diperlukan instrumen hukum yang komprehensif dalam menangani *cybercrime*.

Bocornya data pasien COVID-19 di Indonesia tentunya memprihatinkan, karena informasi terkait dengan pasien COVID-19 merupakan informasi yang sensitif di masyarakat. Dalam hal ini, seseorang melakukan praktek jual beli di dunia maya. Obyek jual beli tersebut berupa data pasien COVID-19 yang diduga diperoleh secara ilegal. Oleh karena baik tindakan dilakukan di dunia maya serta atas obyek yang berupa informasi elektronik yang diduga diakses secara ilegal, maka rasanya tak salah jika kita menyebut tindakan tersebut sebagai *cybercrime*. Bahkan, lebih jauh lagi, tindakan tersebut sebenarnya juga dapat digolongkan sebagai *cyberterror* karena bocornya data pasien COVID-19 dapat menimbulkan kecemasan di masyarakat.

Terkait dengan kerahasiaan data pribadi, khususnya dalam konteks data pasien COVID-19, saat ini Indonesia memiliki beberapa peraturan perundang-undangan yang mengaturnya, antara lain:

a. Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan.
   Ketentuan Pasal 79 ayat (1) menyebutkan bahwa data dan dokumen kependudukan wajib disimpan dan dilindungi oleh negara. Sedangkan ketentuan Pasal 86 ayat (1) menyebutkan bahwa Menteri sebagai penanggung jawab memberikan hak akses kepada petugas penyelenggara dan instansi pelaksana untuk memasukkan, menyimpan, membaca, mengubah, meralat dan menghapus, mengkopi data, serta mencetak data pribadi. Terdapat ancaman pidana bagi setiap orang yang tanpa hak mengakses database kependudukan, sebagaimana yang diatur dalam ketentuan

Pasal 95 UU 23/2006, dipidana dengan pidana penjara paling lama dua tahun dan/atau denda paling banyak dua pulih lima juta rupiah.

b. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik.
Ketentuan Pasal 17 huruf h angka 2, menyebutkan bahwa setiap badan publik wajib membuka akses bagi setiap pemohon informasi publik untuk mendapatkan informasi publik, kecuali informasi publik yang apabila dibuka dan diberikan kepada pemohon informasi publik dapat mengungkap rahasia pribadi, yaitu riwayat, kondisi dan perawatan, pengobatan kesehatan fisik, dan psikis seseorang. Sedangkan untuk ancaman pidana, ketentuan Pasal 54 mengatur bahwa setiap orang yang dengan sengaja atau tanpa hak mengakses, memperoleh, dan/atau memberikan informasi yang dikecualikan tersebut dipidana dengan pidana penjara paling lama dua tahun dan pidana denda paling banyak sepuluh juta rupiah.

c. Undang-Undang Nomor 11 Tahun 2008 *jo*. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.
Ketentuan Pasal 30 ayat (2) *jo*. Pasal 46 ayat (2) UU ITE menyebutkan bahwa setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik dipidana dengan pidana penjara paling lama tujuh tahun dan/atau denda paling banyak tujuh ratus juta rupiah.

Sedangkan ketentuan Pasal 31 ayat (1) *jo*. Pasal 47 UU ITE menyebutkan bahwa setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas informasi elektronik dan/atau dokumen elektronik dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain, dipidana dengan pidana penjara paling lama sepuluh tahun dan/atau denda paling banyak delapan ratus juta rupiah.

Seiring berjalannya waktu, kasus kebocoran data-data pasien COVID-19 di Indonesia tersebut disanggah oleh Badan Siber dan Sandi Negara (BSSN). BSSN menegaskan tidak ada penjualan 230 ribu data pribasi pasien COVID-19 di Indonesia. Untuk mengungkap praktek penjualan data ilegal di dunia maya tersebut, BSSN telah berkoordinasi dengan Kementerian Kesehatan dan Gugus Tugas terkait, untuk kemudian memastikan bahwa tidak ada akses yang tidak sah yang berakibat kebocoran data pada sistem elektronik dan aset informasi aktif penanganan pandemi COVID-19 (Haryanto, 2020a). Meski demikian, klarifikasi tentunya tidak dapat menghalangi atau menghentikan aparat penegak hukum untuk mengusut kasus tersebut.

Sebagaimana telah disebutkan sebelumnya, informasi mengenai data pasien COVID-19 di Indonesia merupakan data yang sensitif di masyarakat, karena dapat menimbulkan tindakan diskriminatif dan stigma di masyarakat. Oleh karena itu, penyidik dalam hal ini dapat merujuk pada ketentuan Pasal 28 ayat (2) *jo*. Pasal 45A ayat (2) UU ITE, disebutkan bahwa setiap orang yang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA) dipidana dengan pidana penjara paling lama enam tahun dan/atau denda paling banyak satu miliar rupiah.

Ketentuan Pasal 5 ayat (1) dan ayat (2) UU ITE merupakan landasan bahwa informasi elektronik, dokumen elektronik, dan/atau hasil cetaknya merupakan alat bukti hukum

yang sah. Dalam hal ini, informasi elektronik, dokumen elektronik, dan/atau hasil cetaknya tersebut merupakan perluasan dari alat bukti berdasarkan ketentuan Pasal 184 KUHAP. Penjualan data pasien COVID-19 di forum *online* merupakan suatu proses pengolahan informasi elektronik dan/atau dokumen elektronik, hasil *print-out* atau *screenshot*-nya pun dapat dikatakan sebagai hasil cetak dari dokumen elektronik. Oleh karena itu, polisi dapat menggunakan hal tersebut sebagai bukti permulaan untuk melakukan pertimbangan apakah terdapat suatu perkara pidana.

PENUTUP

Dari pembahasan yang telah dilakukan, dapat disimpulkan bahwa data pasien COVID-19 merupakan data yang bersifat rahasia. Jika merujuk pada Undang-Undang Keterbukaan Informasi Publik, data pasien COVID-19 termasuk dalam klasifikasi informasi publik yang dikecualikan. Oleh karenanya, data tersebut tidak dapat disebarluaskan atau dibocorkan begitu saja. Dalam hal ini, terdapat ketentuan yang membatasinya, yaitu harus atas persetujuan pasien. Informasi yang dikecualikan tersebut bersifat rahasia sesuai dengan undang-undang, kepatutan, dan kepentingan umum yang didasarkan pada pengujian mengenai konsekuensi yang timbul jika suatu informasi yang diberikan kepada masyarakat serta telah dipertimbangkan dengan seksama bahwa menutup informasi publik tersebut justru dapat melindungi kepentingan yang lebih besar dibandingkan membukanya atau sebaliknya.

Sedangkan terkait dengan penegakan hukum, dengan berpegang pemahaman bahwa tindakan jual-beli data pasien COVID-19 dapat menimbulkan keresahan di masyarakat, menimbulkan tindakan diskriminasi, dan stigma. Maka dapat berpegang pada ketentuan Pasal 28 ayat (2) *jo*. Pasal 45A ayat (2) UU ITE yang menyebutkan bahwa setiap orang yang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA) dipidana dengan pidana penjara paling lama enam tahun dan/atau denda paling banyak satu miliar rupiah.

Adapun saran yang dapat diambil, yaitu Pemerintah supaya menginformasikan kepada khalayak, alasan dan pertimbangan dari tidak dilepasnya informasi mengenai data detail pasien COVID-19. Manfaat keterbukaan data pasien COVID-19 untuk memudahkan upaya *contact tracing* perlu dikaji lebih jauh, khususnya terkait dampak yang mungkin ditimbulkan. Perlu disusun skema pembinaan masyarakat bagaimana menghadapi pasien COVID-19. Jangan sampai, tersebarnya informasi pasien COVID-19 justru mengakibatkan orang menyembunyikan penyakitnya atau tidak mau menerima perawatan kesehatan karena khawatir akan potensi diskriminasi yang akan diterimanya. Jika hal ini terjadi, maka tujuan dari *contact tracing* tidak akan tercapai.

DAFTAR PUSTAKA

Belanger, F., & Crossler, Ro. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, *35*(4).

Bet-El, I. (2020). COVID-19 and the Future of Security and Defence. *European Leadership Network*.

Bowie, N. E., & Jamal, K. (2006). Privacy Rights on the Internet: Self-Regulation or Government Regulation? *Business Ethics Quarterly*, *16*(3).

Corlett, J. A. (2002). The Nature and Value of The Moral Right to Privacy. *Public Affairs Quarterly*, *16*(4).

Haryanto, A. T. (2020a). *BSSN Pastikan Tak Ada Kebocoran Data 230 Ribu Pasien COVID-19 Indonesia*. detikInet. https://inet.detik.com/security/d-5062656/bssn-pastikan-tak-ada-kebocoran-data-230-ribu-pasien-covid-19-indonesia

Haryanto, A. T. (2020b). *Indonesia Harus Belajar dari Isu Kebocoran 230 Ribu Data COVID-19 RI*. detikInet. https://inet.detik.com/security/d-5062785/indonesia-harus-belajar-dari-isu-kebocoran-230-ribu-data-covid-19-ri

JawaPos.com. (2020). *IDI Minta Data Pasien Korona Dibuka Demi Memudahkan Penelusuran Kontak*. JawaPos.com. https://www.jawapos.com/nasional/17/03/2020/idi-minta-data-pasien-korona-dibuka/

Jaya, N. S. P. (2018). *Hukum dan Hukum Pidana di Bidang Ekonomi Edisi Revisi*. Badan Penerbit Universitas Diponegoro.

Jeffray, C., & Feakin, T. (2015). Underground web The cybercrime challenge. *Australian Strategic Policy Institute*, *Special Report*.

Kulhari, S. (2018). The Uneasy Case for Blockchain Technology to Secure Privacy and Identity. In *Building-Blocks of a Data Protection Revolution*. Nomos Verlagsgesellschaft mbH.

Kupfer, J. (1987). Privacy, Autonomy, and Self-Concept. *American Philosophical Quaarterly*, *24*(1).

Malik, S., & Naeem, K. (2020). Impact of COVID-19 Pandemic on Women Health, livelihoods & domestic violence. *Sustainable Development Policy Institute*. https://about.jstor.org/terms

Mappapa, P. L. (2020). *Survei LIPI-UI-ITB-UGM: Mayoritas Setuju Data Pribadi Pasien Corona Dibuka*. detikNews. https://news.detik.com/berita/d-4955689/survei-lipi-ui-itb-ugm-mayoritas-setuju-data-pribadi-pasien-corona-dibuka/2

Marzuki, P. M. (2019). *Penelitian Hukum; Edisi Revisi*. Prenadamedia Group.

Pahajow, A. A. J. (2016). Pembuktian terhadap Kejahatan Dunia Maya dan Upaya Mengatasinya menurut Hukum Positif di Indonesia. *Lex Crimen*, *V*(2).

Ramadhanny, F. (2020). *Alamak! 230 Ribu Data Tes COVID-19 Warga Indonesia Dijual Online*. detikInet. https://inet.detik.com/security/d-5061003/alamak-230-ribu-data-tes-covid-19-warga-indonesia-dijual-online

Scholta, H., Mertens, W., Kowalkiewicz, M., & Becker, J. (2019). From one-stop shop to no-stop shop: An e-government stage model. *Government Information Quarterly*, *36*(1). https://doi.org/10.1016/j.giq.2018.11.010

Thaariq, R. M., Wahyu, M. F. R., Ningrum, D. R., & Aidha, C. N. (2020). Kemiskinan Multidimensi dan Risiko Covid-19 di Indonesia. *Prakarsa Working Paper*, *1*.

Tim - detikInet. (2020). *Ini Bahayanya Jika Data COVID-19 Warga Indonesia Bocor*. detikInet. https://inet.detik.com/security/d-5061341/ini-bahayanya-jika-data-covid-19-warga-indonesia-bocor

Utama, A. N., Jaya, N. S. P., & Purwoto. (2016). Analisis Yuridis Tindakan Mengakses Informasi Secara Elektronik secara Ilegal Berdasarkan Kebijakan Hukum Pidana di Indonesia. *Diponegoro Law Review*, *5*(2).