Jurnal Kewarganegaraan
Vol. 7 No. 2 Desember 2023
P-ISSN: 1978-0184 E-ISSN: 2723-2328

Pelindungan Data Pribadi dalam Tindakan Doxing Berdasarkan Undang-Undang Nomor 27 Tahun 2022

Jeane Neltje Saly[1] Lubna Tabriz Sulthanah[2]
Universitas Tarumanagara[1,2]
Email: jeanes@fh.untar.ac.id[1] lubna.207231020@stu.untar.ac.id[2]

Abstrak
Pesatnya pemanfaatan TIK dan tanpa batas bisa memberikan kemudahan atau bisa menjadi sarana dilakukannya cybercrime khususnya doxing. Doxing dilakukan dengan cara mengumpulkan dan menyebarluaskan data pribadi tanpa persetujuan. Dilakukannya penelitian ini untuk menjawab bagaimana langkah pemerintah dalam menangani doxing data pribadi dan bagaimana sanksi yang diterapkan. Metode penelitian menggunakan yuridis-normatif dengan teknis analisis data deskriptif kualitatif yang menghasilkan data deskriptif terhadap permasalahan yang kemudian diuraikan dalam bentuk kalimat logis dan efektif. Temuan dalam penelitian ini menunjukkan bahwa adanya upaya pemerintah dalam menangani doxing yaitu dengan diundangkannya UU PDP dimana bagi yang mengumpulkan dan mengungkapkan data pribadi yang bukan miliknya tanpa persetujuan yang mengakibatkan kerugian, maka akan dikenakan sanksi.
Kata Kunci: Data Pribadi, Doxing, Undang-Undang Pelindung Data Pribadi

PENDAHULUAN

Semakin pesatnya pemakaian dan pendayagunaan atas Teknologi Informasi dan Komunikasi (TIK), maka banyak membawa perubahan yang dinamis dan menjadi kebutuhan dalam kehidupan bermasyarakat, terutama kemudahan untuk berkomunikasi. Era ini sangat berbeda dengan sebelumnya dimana manusia masih bergantung pada Sumber Daya Alam (SDA) sekitar untuk memenuhi kebutuhan hidupnya (Makarim, 2005,h.27). Kehadiran TIK telah menghapus batasan-batasan (borderless) dalam mengakses seluruh dunia. Ini berarti bahwa setiap individu dapat mengakses berbagai sumber daya melalui koneksi internet. Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) memberikan hasil dari penilikannya yang memperlihatkan jumlah pemakai internet di seluruh Indonesia saat ini menyentuh angka 215.626.156 jiwa, artinya 78,19% dari keseluruhan penduduk Indonesia sebanyak 275.773.901 jiwa telah menggunakan internet. Maka bisa terlihat cukup konsumtifnya penggunaan internet oleh masyarakat Indonesia.

Berkembangnya TIK memiliki potensi untuk menjadi pedang bermata dua. Alasannya adalah jika dilihat dari satu sisi maka itu akan memberikan kemudahan dalam kehidupan manusia, tetapi jika dilihat dari sisi lainnya maka TIK dapat berubah menjadi sarana untuk dilakukannya perbuatan melawan hukum. Tidak adanya batasan interaksi antara ruang publik dengan kehidupan pribadi menyebabkan orang dan/atau sekelompok orang memanfaatkannya untuk beraksi demi mencari keuntungan melalui internet(Fauzi, Elfian&Nabila Alif,2022,h.5). Hal itu tidak bisa kita hindari dikarenakan hampir setiap kegiatan yang dilakukan dalam kehidupan di saat bertumbuhnya pengguna internet pada era digital ini menggunakan dan membutuhkan data pribadi. Hal tersebut diiringi dampak yang signifikan dalam transformasi yang tentunya perlu disadari bahwa informasi memiliki peran vital di kehidupan kita sebagai masyarakat yang harus dijaga terutama mengenai data pribadi. Karena semakin tinggi pemanfaatan teknologi maka akan berbanding lurus dengan jumlah serangan siber yang akan muncul.

Pada umumnya, data pribadi mencakup informasi faktual mengenai individu dan mengandung data informasi yang sifatnya privasi, oleh karena itu individu yang bersangkutan harus mengamankannya demi penggunaan pribadi atau membatasi akses ke data pribadi tersebut. Pada saat yang sama, dalam pengartian yang jelas, data pribadi merupakan suatu informasi yang dapat mencerminkan diri seseorang dan dapat membedakan karakteristik bagi satu individu dengan individu lainnya(Rosadi,DS,2015,h.30). Sesuai dengan definisi data pribadi menurut Pasal 1 Angka 1 Undang-Undang Nomor 27 Tahun 2008 tentang Pelindungan Data Pribadi (UU PDP) disebutkan bahwa "data pribadi merupakan data orang perseorangan yang teridentifikasi atau dapat diidentifikasi sendiri atau dikombinasi dengan informasi lainnya baik langsung maupun tidak langsung melalui sistem elektronik dan nonelektronik". Sedangkan berdasarkan terjemahan pengertian dari CNIL mengenai definisi dari data personal adalah berkaitan dengan kartu identitas yang kita miliki seperti Kartu Tanda Penduduk (KTP), Surat Izin Mengemudi (SIM), data mengenai kondisi fisik seseorang, data kesehatan seseorang, data kondisi ekonomi, data biometrik seperti sidik jari, retina mata maupun wajah seseorang hingga DNA. Berdasarkan Pasal 4 Ayat (1) dan (2) UU PDP definisi data pribadi dibagi menjadi dua kategori yaitu data pribadi yang bersifat spesifik dan data pribadi yang bersifat umum. Data spesifik mencakup informasi kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, data keuangan pribadi, dan data lainnya sesuai dengn ketentuan perundang-undangan. Sedangkan data umum terdiri dari identitas diri seperti nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan dan data pribadi apapun yang dapat digunakan untuk mengidentifikasi seseorang.

Keamanan siber kemudian menjadi salah satu permasalahan di Indonesia yang harus dicarikan jalan keluarnya. Kurangnya kesadaran masyarakat mengenai data pribadi miliknya menyebabkan berbagai jenis ancaman siber yang akan menyebabkan terciptanya ruang atas sejumlah pelanggaran dan penyalahgunaan data pribadi. Kejahatan siber (*cybercrime*) memiliki beberapa ciri-ciri seperti tindakannya tidak mengakibatkan kekerasan fisik (*non violence*) ; kurangnya kontak fisik antara pelaku dengan korban (*minimize of physical contact*) ; tindakannya bergantung pada pemanfaatan teknologi dan peralatan (*equipment*) seperti jaringan telekomunikasi, media dan informatika secara global (Bagiartha, I Putu Pasek,2021,h.92). *Cybercrime* banyak jenis salah satunya yang sesuai dengan ciri-ciri tersebut adalah doxing. Doxing merupakan kejahatan yang dilakukan di internet dengan cara menargetkan dan menggabungkan informasi pribadi yang bukan miliknya yang dilakukan tanpa persetujuan kemudian disebarluaskan. Penyebaran informasi melalui internet didasari dengan keterkaitannya mengenai pelindungan Hak Asasi Manusia sehingga dalam penggunaan informasi tersebut harus mendapat izin dari pemilik data. Tindakan doxing dengan niat jahat yang berbahaya sering kali dilakukan dengan maksud untuk mengancam, mengintimidasi serta dapat membahayakan fisik ataupun mental. Meskipun pengumpulan dan penyebaran data pribadi merupakan pelanggaran terhadap privasi seseorang.

Doxing seringkali ditemukan berbentuk postingan berisi informasi pribadi berupa foto, video, ataupun cerita yang memiliki tujuan untuk membangkitkan dan/atau menggiring opini. Perilaku doxing tidak terlepas dari adanya kebebasan berpendapat dalam kerangka gagasan Franklin De Roosevelt, *The Four Freedoms* tentang empat kebebasan yang telah menjadi standar kebangkitan Hak Asasi Manusia yaitu "kebebasan berpendapat ; kebebasan beribadah ; kebebasan dari kekurangan ; dan kebebasan dari rasa takut". Namun apabila kebebasan berpendapat tersebut dilaksanakan tanpa memerlihatkan standar dan etika maka akan melanggar perlindungan hak pribadi seseorang. Mudahnya dalam memperoleh data pribadi karena kelalaian pengguna dalam mengunggah informasi pribadi dapat menjadi faktor penyebab terjadinya doxing.

Penggunaan data pribadi memerlukan tata kelola yang baik dalam pengolahan data tersebut untuk bisa meminimalisir kejahatan siber yang bisa saja terjadi. Oleh karena itu, diperlukan peraturan yang ketat dan komprehensif untuk menjamin pelindungan penuh terhadap data pribadi. Indonesia sebagai negara hukum (*rechstaat*) harus hadir untuk mengatur segala tingkah laku masyarakat berdasarkan asas persamaan di depan hukum dan memberikan jaminan perlindungan atas hal tersebut yang dituangkan dalam bentuk peraturan yang mengikat seperti yang sudah ditetapkan dalam pasal 1 ayat (3) UUD NRI Tahun 1945. Hak atas privasi telah tercantum dalam Pasal 28G ayat (1) UUD NRI Tahun 1945 yang menyatakan bahwa setiap orang berhak untuk melindungi data identitasnya dan hak atas keamanan. Ketentuan ini ditegaskan kembali dalam Pasal 29 ayat (1) dan Pasal 30 Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia (UU HAM) yang mana dalam ketentuan ini mengakui bahwa hak atas privasi merupakan Hak Asasi Manusia menurut hukum Indonesia.

Mengingat bahwa doxing dapat mengancam privasi seseorang (*right to privacy*), terlebih lagi mengingat pesatnya perkembangan teknologi informasi dan cepatnya penyebaran data di internet, membuat data akan rentan terjadinya penyalahgunaan data. Sehingga doxing merupakan bagian dari Hak Asasi Manusia yang harus diatur dan dilindungi oleh negara, karena tindakan doxing sangat minim bahkan tidak adanya kontak langsung antar pelaku dengan korban sehingga tentunya perlu mendapat perhatian yang serius. Pada penelitian yang serupa yang ditulis oleh Dinda Salsabila, dkk dengan judul "Tindakan Doxing di Media Sosial Berdasakan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Dikaitkan Dengan Konsep Perlindungan Privasi". Karena baru diberlakukannya UU PDP, dalam penelitian tersebut mengulas mengenai prinsip-prinsip pelindungan data pribadi dari tindakan doxing dengan merujuk pada UU ITE. Mengidentifikasi permasalahan dari latar belakang dalam penelitian ini, penulis akan membahas permasalahan dengan perumusan sebagai berikut : Pertama, bagaimana upaya pemerintah dalam menangani pelindungan data pribadi terhadap doxing jika dikaitkan dengan UU PDP? dan yang kedua, bagaimana UU PDP dapat memberikan sanksi kepada pelaku doxing?

METODE PENELITIAN

Metode penelitian dalam penulisan ini adalah penelitian yuridis-normatif dengan landasan analisis studi kepustakaan. Pendekatan masalah yang digunakan berdasarkan pendekatan undang-undang dengan menggunakan sumber data sekunder sebagai sumber utamanya yaitu pencarian dokumen-dokumen kepustakaan seperti buku, jurnal referensi yang berhubungan dengan penelitian. Mengenai teknis analisis data yang digunakan adalah deskriptif kualitatif, artinya penelitian akan menghasilkan data deskriptif tentang permasalahan dan upaya untuk penyelesaiannya serta diuraikan dalam bentuk kalimat yang logis dan efektif.

HASIL PENELITIAN DAN PEMBAHASAN

Upaya Pemerintah dalam Pelindungan Data Pribadi

Pada tahun 2019, Presiden Joko Widodo melakukan pidato kenegaraan dalam acara Ulang Tahun ke-74 yang disampaikannya dalam Sidang Bersama Dewan Perwakilan Rakyat (DPR) dan Dewan Perwakilan Daerah (DPD) menyampaikan bahwa salah satu masalah kejahatan siber, yaitu penyalahgunaan data, harus secepatnya diatasi dengan membuat regulasi pelindungan data pribadi yang mengadopsi beberapa hal, yaitu menciptakan rasa aman, memudahkan, dan mendorong inovasi. Kemudian berlajut pada 24 Januari 2020, melalui Surat Presiden RI, draf Rancangan Undang-Undang Pelindungan Data Pribadi dibahas bersama DPR. Kemudian pada 20 September 2022, rancangan tersebut disahkan menjadi Undang-Undang

Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) dan mulai diundangkan pada 17 Oktober 2022. UU PDP mengatur tentang pemrosesan data yang mencakup tiga hal utama, yaitu mendapatkan/*obtaining*, menyimpan/*holding*, merekam/*recording*, menyebarluaskan/sharing (Lyod, Ian J,2014, h.52). Melalui diundangkannya UU PDP, diharapkan dapat menumbuhkan kesadaran masyarakat terhadap pentingnya data pribadi. Sebelumnya, Indonesia tidak memiliki aturan spesifik yang mengatur mengenai doxing. Dalam UU PDP tidak secara tegas menggunakan istilah "doxing" melainkan menggunakan istilah "dilarang secara melawan hukum mengungkapkan data pribadi yang bukan miliknya", sebagaimana tercantum dalam Pasal 65 ayat (2).

Terkait asas-asas pembentukan peraturan terkait pelindungan data pribadi, hal ini sudah tercantum pada Pasal 3 UU PDP mengatur bahwa UU PDP memiliki asas perlindungan, kepastian hukum, kepentingan umum, kemanfaatan, kehati-hatian, keseimbangan, akuntabilitas, dan kerahasiaan. Dalam mengimplementasikan UU PDP, kepentingan utama adalah kepentingan masyarakat. Asas kemanfaatan dalam UU PDP mengandung makna bahwa adanya UU PDP harus melayani kepentingan nasional demi mewujudkan cita-cita untuk terciptanya kesejahteraan masyarakat. Jika dikaitkan dengan asas keseimbangan, maka hal ini mencakup upaya untuk menjaga data pribadi dengan tetap menjaga keseimbangan antara hak terkait data pribadi dan hak sah negara berdasarkan kepentingan umum.

Klasifikasi Tindakan Doxing

Doxing berasal dari kata "Dox" yang merupakan singkatan dari kata "Dokumen". Secara etimologi berasal dari ungkapan "dropping dox" atau "dropping documents". Menurut terjemahan Oxford British and World English Dictionary, "doxing berarti mencari dan menyebarluaskan atau mengunggah informasi pribadi tentang orang tertentu di internet", seringkali dengan maksud atau tujuan kejahatan. David M. Douglas melalui tulisannya mengenai Analisis Konseptual Doxing (2016) menyampaikan pendapatnya terkait doxing bahwa doxing tidak semuanya diniati dengan niat yang jahat. Kemudian mengkategorikan doxing sebagai berikut:

1. Deanonymizing. Tindakan doxing yang mempublikasikan informasi berupa identitas pribadi milik seseorang dan/atau sekelompok orang yang identitasnya tidak diketahui (anonim) oleh publik atau dikenal dengan memiliki nama samaran. Deanonymizing sangat memengaruhi kerahasiaan identitas seseorang dan dapat mengintimidasi bagi seseorang dan/atau sekelompok orang yang memang tidak ingin diketahui identitasnya oleh publik sebagai bentuk kebebasan berekspresi.
2. Targeting. Tindakan doxing ini mempublikasikan informasi mengenai keberadaan fisik seseorang, dalam artian tindakan ini dapat melacak sampai ditemukan lokasi tempat keberadaaannya dalam waktu yang nyata. Melalui targeting dapat meningkatkan kemungkinan seseorang dan/atau sekelompok orang secara fisik dapat ditemukan dan diketahui domisili tempat dia tinggal. Hal ini dapat membahayakan karena bisa jadi mengakibatkan seseorang dalam kondisi terancam terutama bahaya secara fisik seperti serangan. Tindakan doxing ini dilakukan setelah dilakukannya deanonymizing.
3. Delegitimizing. Tindakan ini mempublikasikan informasi pribadi seseorang dan/atau sekelompok orang dengan tujuan untuk merusak atau menjatuhkan kredibilitas, reputasi ataupun karakter. Maksud dilakukannya doxing ini adalah untuk mempermalukan, menghina, dan menjatuhkan seseorang dengan menggunakan data pribadinya yang mudah disalahpahami atau informasi yang memang rahasia.

Julia M. MacAllister melalui tulisan dalam jurnalnya (2017) mengklasifikasikan beberapa tujuan dilakukannya yaitu:

1. Doxing untuk tujuan jahat. Jenis doxing ini adalah dimana individu melakukan doxing pada orang lain hanya untuk menimbulkan kerugian, kesusahan atau rasa malu yang dapat dimotivasi oleh balas dendam, kemarahan, atau sebatas hanyakeinginan untuk melecehkan seseorang. Melalui internet, memungkinkan doxing yang dilakukan akan menimbulkan kerugian yang besar dibandingkan dengan pelecehan secara langsung.
2. Doxing untuk tujuan politik. Doxing dengan tujuan politik untuk meningkatkan transparansi, mengungkap apa yang mereka anggap tidak adil atau menungkap informasi yang layak diberitakan untuk kepentingan publik.
3. Doxing untuk tujuan pengaturan mandiri. Pengungkap yang memanfaatkan kategori doxing ini untuk mengungkap identitas orang lain yang kehilangan dukungan rekan-rekannya karena berbagai alasan.

Jika dikaitkan dengan UU PDP, ketentuan mengenai doxing dalam UU PDP tidak memperlihatkan perbedaan bentuk dan tujuan doxing. Dalam UU PDP seolah-olah menggeneralisasi bahwa bisa mengkriminalisasi doxing dengan hukuman yang sama (Putri, Nafila Andriana, 2023, h.106). Terdapat beberapa hal yang perlu diperhatikan setelah mengetahui konsep dilakukannya doxing, yaitu (Salsabila, Dinda CS, 2023, h.84):

1. Apakah terdapat persetujuan (*consent*) terhadap terungkapnya data
2. Isi atau rupa data pribadi yang diungkapkan
3. Cara dalam memperoleh data pribadi
4. Akibat yang diderita korban
5. Motif terjadinya doxing.

Sanksi Hukum terhadap Doxing

Tindakan doxing, terutama yang bersifat negatif, tidak dapat dibenarkan dalam keadaan apa pun. Doxing secara tidak langsung dapat ditemukan dalam Pasal 67 ayat (1) UU PDP yang menyatakan barangsiapa dengan sengaja dan melanggar hukum mengakses atau mengumpulkan data pribadi yang bukan miliknya dengan maksud mendapatkan keuntungan pribadi atau keuntungan orang lain, yang berpotensi merugikan individu yang data pribadinya terlibat, akan dikenakan pidana penjara hingga lima tahun dan/atau denda maksimal Rp 5.000.000.000 (lima miliar rupiah). Selanjutnya, pada pasal 67 ayat (2) UU PDP, dengan tegas diatur bahwa siapa pun yang dengan sengaja dan melanggar hukum mengungkapkan data pribadi yang bukan miliknya akan dikenakan pidana penjara hingga empat tahun dan/atau denda maksimal Rp 4.000.000.000 (empat miliar rupiah).

KESIMPULAN

Berdasarkan pada pembahasan sebelumnya, dapat disimpulkan bahwa tindakan doxing merupakan salah satu *cybercrime* yang kegiatannya berupa mengumpulkan dan menyebarluaskan data seseorang dan/atau sekelompok orang yang sudah ditargetkan tanpa melalui izin dari yang memiliki data dengan tujuan tertentu seperti mengancam dan mengintimidasi. Dalam hal menangani dan mencegah *cybercrime* terutama doxing, pemerintah telah berupaya dengan cara mengeluarkan regulasi yaitu diundangkannya UU PDP. Terminologi sanksi yang diterapkan atas pelanggaran tersebut telah diuraikan dalam Pasal 67 ayat (1) dan (2) UU PDP. Pasal 67 ayat (1) menggambarkan bahwa seseorang yang dengan sengaja dan secara ilegal mengakses atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk memperoleh keuntungan dapat mengakibatkan kerugian bagi subjek data pribadi tersebut, dan sebagai konsekuensinya, dapat dikenakan pidana penjara dengan

jangka waktu maksimal lima tahun dan/atau pidana denda dengan jumlah maksimal Rp 5.000.000.000 (lima miliar rupiah). Sementara itu, jika individu tersebut dengan sengaja dan melanggar hukum dengan mengungkapkan data pribadi yang bukan miliknya, maka ia dapat dikenakan sanksi pidana penjara dengan durasi maksimal empat tahun dan/atau pidana denda dengan jumlah maksimal Rp 4.000.000.000 (empat miliar rupiah).

Saran untuk kita sebagai masyarakat sebagai pengguna internet, diharapkan menggunakan internet dengan bijak mengingat maraknya berbagai jenis *cybercrime* yang terjadi. Masyarakat harus sadar akan pentingnya menjaga data pribadi miliknya terutama untuk menghindari doxing dengan cara jangan terlalu banyak mengunggah atau menyebarluaskan informasi-informasi yang berkaitan dengan data pribadi ke internet dan hati-hati dalam memberikan informasi data pribadi. Sejalan dengan upaya masyarakat dalam menjaga data pribadinya, bagi pemerintah selain mengeluarkan regulasi mengenai pelindungan data pribadi, juga harus jelas mengatur mengenai tugas dan fungsi Lembaga Otoritas Pelindungan Data Pribadi yang nantinya akan berada di bawah dan bertanggungjawab langsung kepada presiden.

DAFTAR PUSTAKA

Andriana Putri, Nafila (2023). Doxing untuk Malicious Purposes vs Doxing untuk Political Purposes : Urgensi Pengklasifikasian Ancaman Hukuman Bagi Para Pelaku Doxing dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Padjajaran Law Review, 11(1). https://doi.org/10.56895/plr.v11i1.1286

APJII, "Survei APJII Pengguna Internet di Indonesia Tembus 215 Juta Orang", terbit pada 10 Maret 2023, diakses melalui https://apjii.or.id/berita/d/survei-apjii-pengguna-internet-di-indonesia-tembus-215-juta-orang pada 2 Oktober 2023.

Bagiartha,I Putu Pasek, 'Perilaku Doxing dan Pengaturannya dalam Positivisme Hukum Indonesia', *Jurnal Hukum Agama Hindu Widya Kerta*', vol.4 no.2 (2021), hlm 92.

CNIL, 'Personal Data: definition',diakses melalui https://www.cnil.fr/en/personal-data-definition pada 2 Oktober 2023.

Douglas, David M, 'Doxing: A Conceptual Analysis', Ethics and Information Technology 18 (3), 2016, hlm. 200

Fauzi,Elfian dan Nabila Alif RS, 'Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi'. Jurnal Lex Renaissance, vol.7 no.3 (2022), hlm 5.

Lyod, Ian J, Information Technology Law, United Kingdom : Oxford University Press, 2014, hlm.52

MacAllister, Julia M.'The Doxing Dilemma : Seeking A Remedy for the Malicious Publication of Personal Information', Fordham Law Review, Vol. 85, Issue 5, 2017, 2457

Makarim, Edmon,'Pengantar Hukum Telematika : Suatu Kompilasi Kajian', (Jakarta : Raja Grafindo, 2005), hlm. 27.

Rosadi, Shinta Dewi, 'Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional, Cetakan Pertama', (Bandung : PT Refika Aditama, 2015), hlm. 30.

Salsabila, Dinda CS. (2023). Tindakan Doxing di Media Sosial Berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahn Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Dikaitkan dengan Konsep Perlindungan Data Privasi. Jurnal Qiyas, 8(1). http://dx.doi.org/10.29300/qys.v8i1.10332

Undang-Undang Nomor 27 Tahun 2002 tentang Pelindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820)