CASELAW Journal of Law
Case Law | Journal of Law
e-ISSN 2746-5780
Volume : 5 No : 1, Januari 2024
Available online at :https://ojs.unigal.ac.id/index.php/caselaw/index

ANALISISIS KEBIJAKAN INDONESIA TERKAIT DENGAN PERLINDUNGAN DATA DIRI WARGA NEGARA INDONESIA

ANALYSIS OF INDONESIAN POLICY RELATED TO PROTECTING PERSONAL DATA OF INDONESIAN CITIZENS

Tiyas Sintiya[1], Retnandika Yulianto[2]

Received: December 2023	Accepted: December 2023	Published: January 2024

Abstrak

Dunia sekarang telah memasuki era society 5.0, yang artinya manusia sudah harus lebih siap untuk hidup berdampingan dengan kebaharuan teknologi yang begitu pesat, bukan hanya manusia tetapi juga pemerintah suatu negara. Karena pada era ini semua data akan dikumpulalkan dalam Big Data yang dapat mempermudah pengarsipan dari suatu instansi maupun pemerintah. Era ini tidak hanya menawarkan keuntungan tetapi juga memberikan risiko yang sama besarnya salah satunya adalah peretasan data diri ataupun memanipulasi data diri seseorang dengan tujuan yang beragam mulai dari penjualan data diri maupun untuk kebutuhan politik. Oleh karena itu pada tulisan ini ingin mengkritsi bagaimana kebijakan pemerintah serta langkah-langkah pemerintah Indonesia untuk melindungi data diri warga negara Indonesia. Pada penelitian ini akan menggunakan teori keamanan dengan pendekatan *human security* dan juga *cyber security* untuk dapat mengetahui urgensi yang ditawarkan era society 5.0 dan untuk memandang sejauh mana ketepatan pemerintah Indonesia dalam membuat suatu kebijakan.
Kata kunci: era society 5.0, keamanan, human security, cyber security, kebijakan pemerintah Indonesia, perlindungan data diri

Abstract

The world has now entered the era of society 5.0, which means that humans must be better prepared to live side by side with the novelty of technology that is so rapid, not only humans but also the government of a country. Because in this era all data will be collected in Big Data which can facilitate archiving from an agency or government. This era not only offers benefits but also provides an equally large risk, one of which is hacking personal data or manipulating one's personal data for various purposes ranging from selling personal data to political needs. Therefore, in this paper, I want to criticize the government policies and the steps taken by the Indonesian government to protect the personal data of Indonesian citizens. In this study, we will use security theory with a human security approach and also cyber security to be able to find out the urgency offered by the era of society 5.0 and to see the extent to which the Indonesian government is accurate in making a policy.
Keywords: *society 5.0 era, security, human security, cyber security, Indonesian government policy, personal data protection*

[1] Universitas Paramadina. Email : tiyas.sintiya@students.paramadina.ac.id
[2] Universitas Slamet Riyadi. Email : retnandika.yulianto@unisri.ac.id

PENDAHULUAN

Di dunia yang dewasa dan telah memasuki era society 5.0, masyarakat ditawarkan berbagai dampak positif maupun negatif. Adapun manfaat serta keuntungan yang didapatkan seperti dapat terhubunganya dunia nyata dan dunia maya secara efektif dan efisien serta dipercaya dapat menyelesaikan masalah yang terjadi antara satu negara dengan negara lainnya. Sedangkan dampak negatif yang dihadirkan dari perkembangan teknologi ini adalah berupa pemanasan global, kesenjangan ekonomi, terorisme, dan juga kebocoran data diri dari suatu negara (Yunanda et al, 2022). Era society 5.0 memiliki pengertian bahwa pada era ini manusia lebih cenderung berpusat pada teknologi. Adapun tantangan yang akan dihadapi oleh masyarakat di era ini adalah adanya akumulasi data yang relative meningkat, serta ditakutkan karena banyaknya data yang tersedia masyarakat akan disulitkan untuk dapat memilah serta memilih data mana yang bersifat kridibel serta akurat. Selain itu, potensi adanya kebocoran data juga menjadi poin penting yang harus dilihat pada era ini (Khaerunisa, 2021). Padahal sejatinya data diri, baik berupa identitas digital maupun data pribadi merupakan sesuatu yang sangat harus dijaga keamanannya karena rentan untuk disalah gunakan seperti digunakan untuk meretas rekening keuangan seseorang, data yang bocor dapat digunakan untuk memetakan profil pemilik data salah satunya untuk keperluan politik (DPT), serta tindakan kriminal lainnya seperti pemerasan yang dilakukan secara online dan sebagainya (Vidi, 2021).

Indonesia menjadi salah satu negara yang pernah mengalami kebocoran data diri yang terjadi di tahun 2021 pada kasus bocornya data diri pengguna jaminan kesehatan BPJS. Sekitar 279 juta data warga negara Indonesia termasuk didalamnya data pasien yang meninggal dunia serta 20 juta memiliki foto personal, dicurigai telah diretas dan diperjual belikan di forum daring (BBC, 2021). Walaupun pemerintah Indonesia dengan cepat memutus penyebaran data yang lebih luas dengan memutuskan akses dengan pengunduh data pribadi tersebut, tetapi tindakan tersebut dinilai tidak cukup berdampak karena beberapa data tersebut telah tersebar luas. Indonesia diketahui telah merancang Undang-Undang khusus perlindungan data diri warga negaranya sejak tahun 1945 pasal 28G yang berbunyi “Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaanya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.” Kemudian pasal ini di pada tahun 1999 dimasukan kedalam Undang-undang mengenai HAM (Hak Asasi Manusia), tidak hanya itu ditahun 2006 pasal ini diperbaharui lagi dan masuk kedalam UU 23 tahun 2006 jo 24/2013 mengenai administrasi kependudukan yang berbunyi pada pasal 1 nomor 22 “Data Pribadi dan perseorangan tertentu yang disimpan, dirawat dan dijaga kebenerannya serta dilindungi

kerahasiannya." Dan pasal 79 yang berbunyi. (1) Data perseorangan dan dokumen kependudukan wajib disimpan dan dilindungi kerahasiannya oleh Negara. (2) Menteri sebagai penanggung jawab memberikan hak akses Data Kependudukan kepada petugas provinsi dan petugas Instansi Pelaksana serta pengguna. (3) Petugas dan pengguna sebagaimana dimaksud pada ayat (2) dilarang menyebarluaskan Data Kependudukan yang tidak sesuai dengan kewenngannya. (4) Ketentuan lebih lanjut mengenai persyaratan, ruang lingkup, dan tata cara mengenai pemberian hak akses sebagaimana dimaksud pada ayat (2) diatur dalam perturan Menteri. Serta pada Undang-undang ini mengatur bagaimana suatu instansi harus melindungi data diri/pribadi seseorang seperti yang tertera pada PP 82/2012, PP 71/2019, PP 80/2019 yang berbunyi "Data pribadi adalah setiap data tentang seseorang baik yang terindentifikasi dan/atau dapat diindentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung mauapun tidak langsung melalui Sistem Elektronik dan/atau nonelektronik." Serta pasal 14 yang menjelaskan mengenai prinsip-prinsip dalam melindungi Data Pribadi (Plate 2020).

Indonesia sebagai salah satu negara yang memiliki jumlah penduduk terbanyak di dunia, sudah sepatutnya memperhatikan keamanan dari data diri warga negara ditengah kemajuan jaman dan kejahatan dunia *cyber*. Diketahui sebanyak 28 juta orang dengan presentase sebesar 13%, cukup aktif melakukan transaksi online. Ditunjang oleh kapasitas negara ini yang memiliki sebanyak 49 juta UMKM (SME's) menjadi pemerintah Indonesia berkeinginan untuk membuat Indonesia menjadi pengguna digital ekonomi terbesar di Asia Tenggara yang diperkirakan bahwa pada tahun 2020 mampu menyerap 26 juta lebih tenaga kerja baru (Olisias Gultom), tidak hanya itu per Juni tahun 2022 tercatat sebanyak 241,79 Juta jiwa peserta JKN (Jaminan Kesehatan Negara) (Anathia et al*.,* 2019). Banyaknya persentase pengguna *platform* belanja online serta data diri pengguna JKN (jaminan Kesehatan Negara) menyebabkan resiko peretasan juga semakin pesat untuk dilakukan, Hak atas privasi atau *privacy right* merupakan salah satu hak yang sangat fundamental dalam hak asasi manusia (Kominfo*,* 2019). Hak atas privasi walaupun bukan hak asasi yang absolut akan tetapi perlindungan hukum akan hak privasi tetap sangat krusial di era ekonomi digital dan *era society* 5.0 ini. Sudah seharusnya pemerintah menyediakan pengamanan yang sangat ketat ditengah gempuran perbaharuan teknologi yang kian pesat ini. Oleh sebab itu pada jurnal ini, penulis mencoba untuk melihat sejauh mana kebijakan pengamanan pemerintah terhadap keamanan data warga negara Indonesia, pada penelitian ini mencoba menganalisis menggunakan teori keamanan dengan sudut pandang *human security* dan juga *cyber security.*

METODOLOGI

Dalam jurnal ini menggunakan metode penelitian deskriptif kualitatif. Merupakan suatu metode untuk dapat mengeksplorasi makna dari suatu individu maupun suatu kelompok orang yang bisa dianggap sebagai sumber dari masalah sosial atau kemanusian yang terjadi (JW Creswell, 2018).. Pengguanaan metode deskriptif kualitatif untuk dapat memberikan penekanan terhadap narasi yang lebih detail dalam kasus yang sedang diteliti. Sehingga dapat menjadi penunjang dalam mengkaji kebijakan yang dikeluarkan oleh pemerintah dan melindungi data diri warga negara terhadap perentasan data diri. Data yang digunakan didapatkan dari buku, jurnal, dokumen, dan artikel, baik yang dikeluarkan oleh pemerintah maupun media massa yang memiliki korelasi dengan penelitian ini. Dalam penelitian ini menggunankan data yang kredibel sebagai penunjang penelitian (Sugiyono, 2012).

HASIL PENELITIAN DAN PEMBAHASAN

1. Pengertian Mengenai Data Diri (Data Privasi) di Era Society 5.0

Umat manusia sekarang telah memasuki era society 5.0 yang memiliki pengertian bahwa pada era ini manusia dapat dengan mudah menyelesaikan berbagai masalah ataupun tantnagan dengan memanfaatkan semua inovasi yang ditawarkan di era revolusi industri 4.0 yang hadir sebagai pusat teknologi. Pada era ini juga sejumlah informasi dari berbagai sensor wilayah fisik diakumulasikan kedalam dunia maya, adapun itu termasuk big data yang dapat dianalisis menggunakan artificial intellegence (IA) yang hasilnya akan dikembalikan ke wilayah fisik (dunia nyata) untuk dapat diamnfaatkan oleh masyrakat (Widiatmanti, 2021). Adapun para ahli juga mengatakan bahwa revolusi industri 4.0 berarti bahwa kita telah memasuki era disrupsi digital dan revolusi digital, adapun revolusi digital menjadi penyebabkan revolusi inustri 4.0 terjadi penyebarluasaan alat-alat informasi komunikasi, sedangkan era society 5.0 memiliki arti bahwa masyarakat telah berbagi pengerahuan dan juga informasi dan kerjasama secara nyata akan sulit untuk dilakukan (Yunanda et al., 2022).

Karena terdapat batasan-batasan seperti dikarenakan banyaknya informasi yang ditawarkan menyebabkan akan cenderung sulit untuk mengolah dan menganalisis informasi yang tepat. Serta pada revolusi digital dipercaya telah menawarkan adanya sebuah inovasi yang baru dalam hal memperoleh kapasitas, menyimpan, memanipulasi, dan mentransmisikan volume data secara nyata (*real time*) secara luas dan kompleks (Malik, 2013). Oleh sebab itu, revolusi digital juga dipercaya memiliki kesemaan dengan revolusi data, adanya perkembangan ini disebut sebagai pendorong pengumupalan berbagai data, para pemerintah negara dan juga swasta juga bersaing untuk dapat memperbesar data penyimpanan mereka dan diduga semakin

melakukan pengahapusan data, era baru pengelolaan data inilah yang biasa disebut sebagai big data (Djafar, 2019).

Perdebatan mengenai definisi sebernarnya dari big data sendiri masih menjadi perbincangan yang masih diperdebatkan hingga saat ini, menyebakan adanya silang pendapat atau pengertian yang berbeda antara satu ahli dengan ahli lainnya, seperti dari sudut pandang ilmu komputer yang menyatakan bahwa big data atau revolusi data merupakan sesuatu yang sering diangap sebagai suatu substansi dari sebuah inovasi teknologi. Tetapi pada jurnal ini merujuk pada definisi yang dikemukan kan oleh C. L. Philip Chen and C. Y. Zhang (2014) yang mengatakan bahwa big data merupakan suatu istilah yang sering digunakan untuk menunjukan sekumpulan data yang sangat besar yang didalamnya terdapat struktur yang lebih bervariasi dan juga kompleks yang hasil akhirnya dapat diolah sedemikian rupa sehingga dapat menciptakan sebuah solusi maupun kesimpulan.

Memasuki era society 5.0, dimana manusia dipaksa untuk hidup berdampingan dengan kebaharuan teknologi yang cukup pesat menjadikan penggunaan big data yang sejatinya memiliki elemen-elemen pendukung yang harus di perhatikan salah satunya yang berkaitan dengan privasi atau perlindungan data pribadi. Lebih khususnya yang menyangkut pada penggabungan dataset yang dipercaya dapat memudahkan identifikasi individu ataupun kelompok individu, yang berpotensi membahayakan pribadi orang tersebut. Oleh sebab itu, perlu untuk suatu instansi ataupun pemerintah memperhatikan langkah-langkah perlindungan dari data diri tersebut berupa kebijakan yang tepat sehingga dapat meminimalisir penyalahgunaaan taupun kesalahan dalam penangganan data. Khsusunya, bila ada peningkatan massif dalam hal pengumpulan atau pengolahan data ini harus tetap dilakukan dengan pedoman penghormatan pada hak privasi dari pengguna, oleh karenanya proses serta tujuan akan berpacu pada bagaimana cara melindungi dan tidak mengesampingkan hak-hak privasi dari masyarakat dan juga pengguna jasa(Djafar, 2019).

Sedangkan data diri sendiri berarti bahwa sesuatu hak yang melekat pada diri pribadi, isu ini menjadi penting untuk diteliti setalah hukum Inggris berbicara mengenai pentingnya menjaga dan memberikan perlindungan terhadap hak atas privasi seseorang. Data pengguna yang tercatat dalam suatu instansi swasta maupun pemerintahan berguna untuk dijadikan sebagai alat dapat meningkatkan kualitas produk oleh penginisiasi, dengan kata lain penginisasi akan dapat mengenali para pengguna maupun penerima jasa untuk dapat meningkatkan keungulan dan memperkuat basis pasar mereka(Prayoga et al. 2022). Namun ini dikhwatirkan akan beresiko pada kerentanan data pelanggan yang dapat dimanfaatkan untuk hal yang tidak di inginkan seperti diperjual beli kan maupun kerentanan terhadap bahaya dari adanya perentasan

yang dilakukan oleh pihak eksternal (Prayoga et al. 2022). Akibatnya para pengguna jasa ataupun pelanggan akan mengalami kerugian baik secara psikologis, emosional, maupun materil pada saat pelanggaran terjadi, terlepas dari apakah data diri mereka disalah gunakan atau tidak. Ini cenderung dapat terjadi karena adanya kepercayaan dari pengguna jasa ataupun pelanggan yang diberikan sepenuhnya kepada penginisasi bahwa data mereka akan aman, serta adanya kepercayaan dari pelanggan ataupun pengguna jasa bahwa akar atau awal dari terjadinya krisis adalah endemik untuk seluruh kategori atau industri. Oleh sebab itu suatu instansi swasta ataupun pemerintahan memerlukan sistem pengamanan data yang kuat agar hal-hal yang tidak diinginkan berupa peretasan tidak dapat dilakukan serta didukung oleh undang-undang ataupun kebijakan yang sejalan dengan pengamanan data diri dari pelanggan dan juga pengguna jasa.

2. Penting keamanan Data Diri

Keamanan Manusia (*Human Security*)

Konsep *human security* atau keamanan manusia pertama kali dikenalkan oleh UNDP (*United Nations Development Program*) pada tahun 1994. Dalam agendanya UNDP mengatakan bahwa konsep *human security* mencakup keamanan ekonomi, keamanan pangan, keamanan kesehatan, keamanan lingkungan hidup, keamanan personal, keamanan komunitas, dan keamanan politik. Ketujuh konsep tersebut dibagi menjadi dua komponen utama dalam *human security* yaitu *freedom from fear* dan juga *fredom from want*.

Anuradha M Chenoy juga memberikan definisi mengenai *human security*, Chenoy menjelaskan bahwa *human security* merupakan perlindungan bagi individu-individu dari suatu resiko yang dapat mengancam keamanan fisik dan psikologis, martabat dan kesejahteraan mereka. Ketika suatu obyek yang ditujukan adalah individu maka keamanan yang dimaksud itu bukan hanya sekesdar kondisi untuk bertahan hidup saja tetapi juga menyangkut kesejahteraan dan martabat dirinya sebagai manusia. Oleh sebab itu, lingkungan yang dimaksud harus mampu menyediakan keamanan manusia bagi penduduknya yang dapat menciptakan kestabilan dan rasa aman bagi penduduknya.

Sedangkan menurut Amartya (Sen, 2005) *human security* merupakan konsep keamanan yang didasari oleh kehidupan individual manusia yang dinilai memiliki nilai yang bertentangan dengan konsep keamanan militer dan juga bentuk apresiasi terhadap peran masyarakat (*The role of society*) dengan membuat kehidupan manusia lebih aman. Selain itu, *Human Security* juga didasari oleh perhatian yang ditekankan pada hak-hak kemanusiaan mendasar (bukan keseluruhan) yang harus dijaga dan diwujudkan dalam konsep keamanan. Dari penjelasan tersebut, meskipun konsep *Human Security* terlihat familiar dan memang saling berkaitan erat dengan konsep *human development* dan *human rights* atau bahkan dengan konsep keamanan

nasional, tetapi menurut Amartya Sen konsep-konsep tersebut berbeda dari satu sama lain dari segi fokus atau *scope*. Sehingga, dinilai cukup penting untuk memisahkan perbedaan antara konsep-konsep tersebut.

Meluasnya pemahaman tentang konsep *human security* salah satunya dikarenakan adanya pengaruh terhadap kehidupan manusia secara langsung di era modern ini. Berbeda dengan konsep keamanan militer yang keamanan hanya dapat ditentukan oleh kemampuan dan kesiapan militer. Melainkan konsep *human security* lebih mengakomodasi keresahan masyarakat secara langsung dibanding dengan konsep keamanan nasional yang berfokus pada sektor militer dan keamanan negara. Konsep *Human security* juga saling mendukung satu sama lain dengan konsep kebebasan. Menurut *Commission on Human Security* (CHS, 2003) yang menyebutkan bahwa konsep *human security* dan konsep kebebasan memang memiliki keterkaitan, kebebasan sendiri dapat diartikan secara luas serta berkaitan dengan kondisi kehidupan manusia dan kemampuan untuk menentukan cara hidup bagi setiap individu, kebebasan juga dapat diartikan bebas dari kecemasan yang mengancam keamanan tiap individu.

Sedangkan menurut (Pulhin, 2014), *Human Security* merupakan kondisi dimana segala isu penting (budaya, materiil, dan non-materiil) yang berkaitan dengan kehidupan manusia termasuk kemampuan untu memiliki kehidupan yang bebas dan bermartabat dapat terjamin. Pulhin juga berpendapat bahwa terdapat fenomena yang mempengaruhi atau mengancam *human security* seperti markets, negara, masyarakat, kemiskinan, diskriminasi dalam bentuk apapun serta technological disasters (bencana teknologi). Sedangkan menurut UN Development programme tahun 1994, *Human Security* adalah kondisi dimana kebutuhan dan hak masyarakat secara individu dapat terpenuhi, terjamin, dan terlindungi yang terdiri dari Keamanan ekonomi (individu dan kebutuhan rumah tangga), Keamanan pangan (kebutuhan nutrisi masyarakat yang terutama perempuan dan anak-anak), Keamanan kesehatan (akses terhadap kebutuhan medis dan kesehatan masyarakat dapat terjamin dan terpenuhi), Keamanan lingkungan, Keamanan personal (menjamin keamanan tiap individu dari kejahatan atau ancaman fisik), Keamanan komunitas (menjamin interaksi sosial atau komunitas komunal terlindungi), dan Keamanan politik (menjamin tiap individu memiliki hak yang sama dalam partisipasi politik di berbagai sektor kehidupan bernegara) (Scott et al, 2018).

Personal security masuk kedalam bagian dalam tujuh kategori *human security* yang di jelaskan oleh UNDP, pada negara berkembangan pencapaian *personal security* menjadi suatu permasalahan karena adanya keterbatasan program, anggaran, dan political will. Seiring dengan kemajuan zaman, personal security mampu menjadi isu internasional yang memiliki kaitan erat hak asasi manusia (HAM) dan pembangunan manusia.

Semakin berkembangnya konsep keamanan diikuti dengan hadirnya berbagai ancaman yang dirasakan oleh masyarakat suatu negara menyebabkan konsep keamanan mengalami redefinisi dari keamanan tradisional hingga keamanan non tradisional yang kemudian diikuti dengan konsep *human security* yang juga mencakup mengenai *personal security* (keamanan personal), merupakan suatu konsep yang menyatakan bahwa individu merupakan objek yang harus dilindungi oleh negara bahkan dalam lingkup terkecil sekalipun. Dalam lingkup internasional, *personal security* menjadi suatu bagian penting dalam supremasi hak asasi manusia (HAM) dan regulasi internasional yaitu konsep *human security* yang dibentuk oleh PBB (Perserikatan Bangsa-Bangsa).

Oleh karena itu untuk mengamankan *personal security* perlu adanya cakupan dari *cyber security* yang merupakan bagian dari keamanan informasi yang berguna untuk melindungi sistem yang terhubung ke internet, termasuk didalannya perangkat keras, perangkat lunak, program, maupun data pribadi. *Cyber security* memiliki peranan penting karena mencakup semua organisasi pemerintahan, militer, maupun suatu perusahaan dalam melakukan aktivitas pengumpulan, pemrosesan, dan penyimpana data pada komputer dan perangkat lain yang dapat terhubung ke jaringan.

Data yang disimpan merupakan sesuatu informasi yang bersifat sensitif sehingga jika terdapat pengungkapan data yang dilakukan secara tidak sah akan dapat berdampak negatif. Keamanan informasi tersebut didasarkan pada proses maupun teknik yang digunakan untuk melindungi suatu informasi dan data pribadi dari akses yang tidak sah baik dalam bentuk cetak maupun elektronik. Informasi merupakan sesuatu yang sangat berniali bagi setiap individu maupun dalam dunia bisnis. Serta yang menjadi sesuatu yang vital bagi setiap organisasi untuk dapat melindungi keamanan informasi yang mencakup kerahasiaan, integritas, maupun ketersedian data.

Pernyataan di atas mampu menjadi bukti bahwa data pribadi masyarakat menjadi salah satu hak asasi manusia yang perlindungan dan keamanannya wajib dipenuhi oleh negara agar mampu meminimalisir adanya *cyber crime* dan mewujudkan poin-poin yang terdapat dalam konsep *human security*. *Cyber crime* sendiri merupakan kejahatan atau kriminalitas dalam ranah ruang siber (*cyberspace*), mengingat kejahatan terhadap personal atau individu sangat berkaitan dengan konsep *human security* dimana kondisi tersebut didasarkan pada adanya pemberian rasa aman terhadap masyarakat. Menurut *The Council of Europe's Cybercrime Treaty* definisi *cybercrime* sendiri adalah segala aktivitas yang merujuk pada pelanggaran yang terdiri dari aktivitas criminal terhadap data, konten, sampai pelanggangaran hak cipta. Sedangkan menurut Michael Aaron (Dennis, 2019) *cybercrime* memiliki definisi yang lebih luas yaitu kejahatan

computer yang melibatkan aktivitas ilegal, penipuan, perdagangan manusia (seperti pornografi pada anak usia di bawah umur), pelanggaran hak cipta, pencurian identitas, serta pelanggaran privasi. Senada dengan definisi tersebut, *The United Nations Manual on the Prevention and Control of Computer Related Crime* berpendapat bahwa *cybercrime* adalah pelanggaran atau aktivitas criminal yang terdiri dari penipuan, pemalsuan serta pelanggaran akses yang sah (privasi) (United Nations, 2022) .

Sehinga untuk meminimalisir terjadinya *cyber crime*, perlu adanya pertahanan siber (*cyber defense*) yang merupakan upaya untuk menanggulangi serangan siber yang menyebabkan terjadinya gangguan pada penyelenggaraan pertahanan negara sedangkan menurut Ineu (Rahmawati, 2017) *cyber defense* adalah strategi atau kebijakan untuk mengembangkan *cyber security* yang dibutuhkan sebagai instrumen pertahanan negara dalam menangkis segala ancaman (*cybercrime*) dalam lingkup ruang siber (*cyberscpace*) yang setiap saat dapat mengganggu keamanan negara melalui *cyberarmy* khususnya di Indonesia. Di Indonesia *Cyberarmy* dibentuk oleh Pusat Pertahanan Siber yang terdiri dari TNI AD, TNI AU, dan TNI AL serta para ahli di bidang teknologi dalam kalangan sipil.

Dalam konsep keamanan terdapat dua pendekatan yang dapat dijadikan acuan untuk dapat menganalisis kebijakan yang dikeluarkan oleh pemerintah. Yaitu: *Top-Down* yang menjelaskan mengenai negara sebagai penjamin keamanan memiliki tanggung jawab dalam perumusan visi misi pada setiap kebijakan yang mereka keluarkan untuk dapat memberikan keadilan bagi seluruh warga negara. Keterlibatan negara dalam sistem internasional, membuka asumsi bahwa intervensi antarnegara merupakan kesadaran bahwa dala dunia global relatif sulit untuk menutup diri dari ancaman-ancaman yang hadir secara transnasional. Sedangkan Bottom-Up lebih mengedepankan organisasi atau kelompok sosial (masyarakat sipil) dalam bagian dari kelompok-kelompok lokal sebagai aktor yang mampu dipercayai mempunyai akses terhadap suatu individu. Adapun kelonpok sosial tersebit dapat menjadi penyamvung persoalan individu-individu tersebut kepada *Top-Down.*

3. Analisis Kebijakan yang dikeluarkan oleh Pemerintah Indonesia terhadap Perlindungan Data Diri Warga Negara

Indonesia merupakan salah satu negara yang sering menjadi target kejahatan siber (*cybercrime*) dalam beberapa tahun terakhir. Hal tersebut diikuti dengan perkembangan digitalisasi yang cukup pesat dalam berbagai aspek kehidupan masyarakat Indonesia sehingga keamanan data penduduk menjadi sasaran kejahatan di dunia siber. Berdasarkan data dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) terdapat 196,7 juta jiwa atau sekitar 73,7% penduduk yang menggunakan internet pada tahun 2020. Peningkatan tersebut memicu

tumbuhnya potensi kejahatan siber di Indonesia, Badan Siber dan Sandi Negara (BSSN) mencatat bahwa terdapat serangan dalam ruang siber (*cyber space*) yang mencapai 495,3 juta serangan pada tahun 2020 yang mengalami peninangkatan sebanyak 41 persen dari tahun sebelumnya (Christianingrum & Aida, 2021)Sedangkan berdasarkan data yang dirilis oleh perusahaan keamanan siber Kapersky menyebutkan bahwa terdapat 11,8 juta ancaman siber yang terdeteksi dan diblokir pada periode Januari-Maret 2022. Berdasarkan data tersebut, Kapersky menyebutkan bahwa Indonesia menempati peringkat teratas sebagai negara yang memiliki potensi paling berbahaya dalam kegiatan internet di kawasan asia tenggara dan menempati peringkat 60 di dunia(Gian, 2022).

Perlindungan data pribadi sudah diakui oleh beberapa negara sebagai hak konstitusional yang juga diakui sebagai hak asasi manusia dalam hukum internasional yang diatur pada Pasal 12 dalam *the General Declaration of Human Rights* yang berisi tentang seseorang berhak atas perlindungan terhadap segala bentuk ancaman yang mengganggu privasi, keluarga, atau serangan terhadap reputasi dan kehormatan seseorang. Selain itu, bebas dari segalam macam bentuk ancaman/kejahatan yang mengganggu kehidupan manusia merupakan kondisi yang wajib dipenuhi untuk mencapai *Human Security*. Di Indonesia sendiri merujuk pada pasal Pasal 28G UUD 1945 perlindungan data pribadi merupakan salah satu hak asasi manusia yang wajib dilindungi. Oleh karena itu, negara wajib merumuskan kebijakan yang berpusat pada perlindungan data diri penduduk untuk menjamin kondisi keamanan manusia (*Human Security*), di Indonesia sendiri pengaturan perlindungan data pribadi tercantum dalam beberapa aturan perundang-undangan dan kebijakan sebelum disahkannya Undang-undang PDP dalam upaya mewujudkan keamanan data pribadi. Seperti aturan yang dirilis oleh Kominfo pada Peraturan Menteri Kominfo No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (Kominfo, 2016) dan kebijakan PSE (Penyelenggara Sistem Elektronik) yang tertuang pada Peraturan Menteri Kominfo Nomor 5 Tahun 2020.

Namun, sebelum adanya UU PDP di Indonesia, Indonesia belum/tidak memiliki UU ataupun aturan khusus yang mengatur tentang perlindungan data pribadi secara komprehensif yang menyebabkan berbagai bentuk masalah dalam ranah ruang siber (*cyber space*) seperti kepercayaan komunitas internasional terhadap Indonesia mengenai penyimpanan data yang berpengaruh pada investasi. Atau, terdapat beberapa pelanggaran terhadap hak konstitusional terkait perlindungan data pribadi seperti bocornya data pribadi pengguna BPJS kesehatan pada bulan Mei 2021. Menurut laporan CNN Indonesia terdapat sebanyak 279 juta data pengguna yang dibobol oleh hacker dan diperjual belikan. Data yang bocor tersebut terdiri dari data kependudukan TNI, Polri serta data pribadi penduduk (Nama lengkap, Nomor KTP, Nomor

telepon, Email, NID, dan alamat (Cnn Indonesia, 2021). Selain itu, kebocoran data juga dialami oleh PLN yang mengalami pembobolan data 17 juta pengguna dan Indihome yang mengalami kebocoran data 26 juta riwayat pengguna yang kemudian dijual di situs gelap, kedua perusahaan tersebut merupakan badan usaha dibawah naungan BUMN.

Maraknya isu kejahatan siber sepatutnya menjadi perhatian pemerintah karena ini telah tercantum dalam prinsip-prinsip perlindungan data pribadi sebagai hak konstitusional warga negara. Oleh karena itu, terdapat desakan terhadap pemerintah untuk segera menetapkan UU PDP yang sudah ditetapkan pada 20 September 2022. Undang-undang tersebut mengatur tentang perlindungan data pribadi secara komprehensif dan sesuai dengan prinsip cyber defense dalam upaya memperbaiki cyber security untuk menjamin keamanan manusia (*Human Security*). Selain itu, UU PDP juga disebut sebagai instrumen pemerintah untuk menjamin hak warga negara dan juga menjadi payung hukum terkait tata kelola dan perlindungan data. Jika melihat aturan yang digunakan oleh komunitas internasional seperti di negara-negara eropa, perlindungan data pribadi dianggap sebagai hak warga negara dalam *The European Union Charter of Fundamental Rights* dan diatur oleh *The General Data Protection* sebagai wujud lembaga pengawasan dan perlindungan bagi warga negara dalam hal data pribadi di ruang siber. Sedangkan Amerika Serikat sudah memberlakukan hukum perlindungan data pribadi yang tertuang pada *US Privacy Law* tahun 1974.

Dalam konsep *human security*, perlindungan data pribadi ditekankan pada prinsip terbebas dari segala bentuk ancaman kejahatan yang mengancam tiap individu, sehingga aturan atau produk UU yang dihasilkan negara wajib mengatur secara komprehensif dan sesuai dengan prinsip keamanan. Undang-undang PDP adalah aturan yang paling mendekati tuntutan tersebut. Undang-undang tersebut berisi tentang

1. Pasal 65 UU PDP: Larangan memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek data pribadi.
2. Pasal 65 UU PDP: Larangan untuk mengungkapkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek data pribadi.
3. Pasal 65 UU PDP: Larangan menggunakan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek data pribadi.

4. Pasal 66 UU PDP: Larangan membuat data pribadi palsu atau memalsukan data pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain.

Dalam aturan tersebut juga dijelaskan secara rinci mengenai jenis-jenis data pribadi yang wajib dilindungi jika merujuk pada UU Perlindungan Data Pribadi (PDP). Dengan ditetapkannya UU PDP tersebut, masyarakat berhak menuntut negara untuk mengupayakan keamanan serta perlindungan terhadap data pribadi yang merupakan hak konstitusional dan hak asasi manusia untuk memperoleh rasa bebas dari segala bentuk ancaman sesuai dengan konsep *human security*.

Keamanan data merupakan sesuatu yang sangat substansial, pemerintah Indonesia seharusnya mampu untuk menjamin keamanan dan kerahasiaanya agar data diri tersebut tidak disalahgunakan secara ilegal oleh pihak lain (Bunga, 2022).. Tetapi hingga saat ini pemerintah belum mampu untuk menerapkan kebijakan tersebut setelah kebocoran kembali terjadi pada tahun 2023 yang terjadi pada pelanggan IndiHome yang merupakan perusahaan milik pemerintah. Sebanyak 26 juta riwayat pencarian dan nama disertai Nomor Induk Kependudukan (NIK) pelanggan IndiHome bocor dan dibagikan secara gratis pada situs ilegal (BBC News, 2022)..

Pemerintah seharusnya sudah mampu memberikan hukum yang spesifik tentang perlindungan privasi dan data pribadi. Jaminan hukum bagi perlindungan warga negara Indonesia masih terkesan terpecah dalam setiap lembaga memiliki kebijakan yang tumpang tindih dengan lembaga lainnya (Bunga, 2022). Pemerintah Indonesia terkesan belum mampu untuk menjamin keamanan data diri dan memberikan sanski yang nyata bagi para pelanggar sehingga tidak dapat menjamin keberlangsungan hak asasi manusia melihat kebocoran data diri ini masih saja terjadi, sejatinya apabila pemerintah merujuk pada pendekataan *top-down* dalam konsep keamanan negara dianggap memiliki ruang lingkup dan kewenangan secara kapital yang luas untuk dapat merespon banyak sektor.

Jika pemerintah dapat memaksimalkan *power* yang ada pemerintah dapat menjamin keamanan data diri warga negara sehingga masyarakat dalam meraih poin yang telah tercantum pada konsep keamanan yaitu *freedom for want* dan juga *freedom from fear* yang menyangkut dengan keamanan ekonomi, keamanan pangan, keamanan kesehatan, keamanan lingkungan, keamanan pribadi, keamanan komunitas, dan juga keamanan politi. Melihat data diri warga negara yang terus bocor dapat menjadi bukti bahwa warga negara Indonesia masih jauh dari konsep *human security* ini (Boer den Monica & Wilde de Jaap, 2008)..

Pemerintah Indonesia sejatinya telah melakukan beberapa implementasi yang merujuk pada UU PDP, dengan mengarahkan para pimpinan tertinggi di instansi pemerintahan (Dukcapil) agar dapat komitmen untuk menjalankan kebijakan sesuai dengan pasal-pasal yang tertuang didalam UU PDP, pemerintah juga telah menetapkan sanksi bagi oknum yang melakukan pembocoran data pribadi di satker responden, pemerintah mengklaim melalui sensus yang dilakukan mayoritas responden telah menjalankan prinsip-prinsip yang telah tertuang pada UU PDP, masyarakat dinilai sudah sadar akan pentingnya isu-isu mengenai perlindungan data diri, pemerintah juga memberi pernyataan bahwa masyarakat sudah mulai menunjukan kepercayaan untuk pemerintah dapat mengesahkab RUU PDP (Kominfo, 2019).

Akan tetapi, kebijakan ini belum dapat terlaksana secara maksimal dikarenakan terdapat beberapa hambatan. Seperti, masih ditemukan adanya ADB (pengelola data pribadi) yang tidak mengetahui informasi terkait dengan perlindungan data pribadi dan peraturan yang tertuang dalam UU PDP, pemerintah dinilai belum memaksimalkan kegiatan sosialisasi dan pelatihan mengenai pentingnya UU PDP secara terstruktur, masih ditemukan beberapa Dukcapil yang memiliki SOP, mitigasi, resiko, dan landasan kerjasama dan hanya sedikit Dukcapil yang memiliki standar keamanan data dalam mengelola data pribadi, ditemukan masih ada satuan kerja yang tidak membatasi akses terhadap data pribadi (fisik & elektronik), dan pemerintah Indonesia sampai dengan saat ini diketahui belum mengeluarkan definisi yang jelas terkait dengan penghapusan data pribadi (Kominfo, 2019).

Hambat-hambatan tersebut sejatinya dapat diminimalisir apabila pemerintah dapat memaksimalkan kebijakan yang ada dengan memaksimalkan kinerja dari institusi BAPD (Badan Autoritas Perlindungan Data) dan melakukan sosialasi sejak dini mengenai pentingnya melindungi data diri pribadi kepada masyarakat Indonesia, melihat data yang dikeluarkan oleh databoks masyarakat Indonesia menduduki peringkat keempat dengan persentase 53,6% sebagai negara yang masyarakatnya memiliki kesadaran yang rendah terhadap perlindungan data diri berada di bawah Singapura, Malaysia, dan Filipina. Survei ini dilakukan dengan mengukur indikator perilaku berisiko dalam bermedia sosial, seperti mencantumkan nomor telepon, tanggal lahir, alamat rumah, rincian anggota keluarga, dan juga memasukan informasi mengenai lokasi terkini. Selain itu beberapa masyarakat Indonesia masih mudah mengaktivasi digital responden yang mengancam keamanan data pribadi, dengan mencoba melakukan instalisasi apalikasi ilegal dengan cara mengunggah foto KTP, hingga mengunggah tiket pesawat maupun kereta yang mencatumkan data pribadi masyarakat (Cindy, 2021)..

Menurut Kominfo, Indonesia telah mencapai persentase sebanyak 60% untuk permasalahan kesiapan implementasi regulasi mengenai perlindungan data pribadi di Dinas

Dukcapil Tingkat Kabupaten/Kota dengan aspek SDM yang mencapai angka keseluruhan paling tinggi (76,41%) (Kominfo, 2019). Pemerintah dapat memanfaatkan segala fasilitas yang ada untuk dapat mengedukasi masyarakat dan organisasi atau institusi terkait agar dapat memaksimalkan kinerjanya untuk dapat melindungi data diri warga negara Indonesia, agar Indonesia dapat menjalankan poin-poin yang telah tertuang dalam konsep keamanan manusia dengan salah satunya menyebutkan bahwa keamanan personal merupak satu dari sekian poin yang harus dipenuhi oleh negara agar masyarakat Indonesia secara keseluruhan dapat merasakan adanya *freedom for want* maupun *freedom for fear* dalam kehidupan mereka.

KESIMPULAN

Pemerintah Indonesia dinilai sudah cukup cakap dalam merumuskan undang-undang terkait dengan perumusan perlindungan data pribadi warganya tetapi pada segi kebijakan masih dinilai kurang efektif karna pengamanan pada sistem yang relatif cukup lemah dibandingan dengan negara lain, hal ini cukup disayangkan mengingat bahwa Indonesia merupakan salah negara dengan populasi terbanyak didunia sudah sepatutnya untuk dapat lebih memberi pengamanan yang ekstra baik dibidang keamanan tradisional maupun non-tradisional. Pemerintah sejatinya harus segara sadar bahwa dunia sekarang telah memasuki *era society* 5.0 yang menjadikan manusia dapat hidup berdampingan dengan pembaharuan teknologi yang cukup pesat, akan lebih baik jika perumusan yang telah dilakukan ini diimbangi dengan kebijakan yang sejalan karena pemerintah Indonesia sudah sangat baik dalam hal perumusan kebijakan yang tercantum pada pasal-pasal yang tertuang dalam naskah undang-undang.

DAFTAR PUSTAKA

Anathia, Ayu, D., Anindyajati, Titis., Ghoffar Abdul. "Perlindungan Hak Privasi Atas Data Diri Di Era Ekonomi Digital." Jakarta, 2019.

Annur, Cindy mutia. "Total 2.032 Tenaga Kesehatan Meninggal Akibat Covid-19 Hingga Oktober 2021." *Databoks*, no. November (2021): 2021.

Ayu, Gian, Mathilda. "Kaspersky Mencatat Indonesia HAdapi 11 Juta Serangan Siber Pada Kuarta Pertama 2022." *CloudComputing*. April 29, 2022. https://www.cloudcomputing.id/berita/kaspersky-mencatat-indonesia-hadapi-serangan-siber.

BBC.com. "BPJS Kesehatan: Data Ratusan Juta Peserta Diduga Bocor-'otomatis Yang Dirugikan Masyrakat' Kata Pakar." *BBC News Indonesia*. May 21, 2021. https://www.google.com/amp/s/www.bbc.com/indonesia/indonesia-57196905.amp.

BBC News. "Kebocoran Data Pribadi Dan Tanggungjawab Pemerintah: 'Tak Perlu Ada Gugaran, Kalau Regulator Berani Dan Tegas." *BBC News Indonesia*. 2022. https://www.bbc.com/indonesia/articles/19mdml39m2o.amp.

Boer den Monica & Wilde de Jaap. *The Viability of Human Security*. Amsterdam: Amsterdam University Press, 2008.

C. L. Philip Chen and C. Y. Zhang. ""Data-Intensive Applications, Challenges, Techniques and Technologies:" *A Survey on Big Data," Inf. Sci. (Ny)* 275 (2014): 314–47.

Christianingrum, Ratna., Aida, Ade Nurul. "Tantangan Penguatan Keamanan Siber Dalam Menjaga Stabilitas Keamanan." Pusat Kajian Anggaran Badan Keahlian DPR RI, 2021. https://pusatkajiananggaran.dpr.go.id/produk/detail-analisis-apbn/id.65.

Cnn Indonesia. "Rentetan Kasus Dugaan Kebocoran Data Kesehatan Pemerintah." *CNN Indonesia*. September 3, 2021. https://www.cnnindonesia.com/teknologi/20210903142047-185-689370/rentetan-kasus-dugaan-kebocoran-data-kesehatan-pemerintah#:~:text=Data BPJS Kesehatan,yang diduga milik BPJS Kesehatan.

Commission on Human Security. "Human Security Now." *United Nation Human Rights Office of The High Commissioner*. New York, 2003.

Creswell, JW. *Qualitative Inquiry And Research Design Choosing Among Five Approach*. 3rd ed. USA: Sage Publications Ltd, 2018.

Dennis., Aaron., Michael. "Cybercrime." Encyclopedia Britannica, 2019. https://www.britannica.com/topic/cybercrime.

Djafar, Wahyudi. "Hukum Perlindungan Data Pribadi Di Indonesia: Lanskap, Urgensi Dan Kebutuhan Pembaruan," 2019.

Iswandari Asika Bunga. "Jaminan Keamanan Data Pribadi Warga Negara Dalam Penyelenggaraan Urusan Pemerintahan Berbasis Elektronik (E-Goverment)." *Jurnal Program Hukum Fakultas Hukum Universitas Indonesia* 2 (1) (2022).

Johnny G. Plate. "PENJELASAN PEMERINTAH MENGENAI RANCANGAN UNDANG-UNDANG TENTANG PELINDUNGAN DATA PRIBADI." Jakarta, 2020.

Khaerunisa, Intan. "Tantangan Generasi Milenial Dalam Menghadapi Society 5.0." *Universitas Padjajaran*. January 28, 2021. https:ketik.unpad.ac.id/posts/1950/tantangan-generasi-milenial-dalam-menghadapi-society-5-0-1.

Kominfo. "Kemkominfo: Pertumbuhan e-Commerce Indonesia Capai 778 Persen."

SkalaNews.com, 2019. https://www.kominfo.go.id/content/detail/16770/kemkominfo-pertumbuhan-e-Commerce-Indonesiacapai-78-persen/0/sorotan_media.

———. "Peraturan Menteri Komunikasi Dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik." jdih.kominfo, 2016. https://jdih.kominfo.go.id/produk_hukum/view/id/553/t/peraturan+menteri+komunikasi+dan+informatika+nomor+20+tahun+2016+tanggal+1+desember+2016.

———. "Strategi Impelmentasi Regulasi Perlindungan Data Pribadi Di Indonesia." Jakarta, n.d.

Malik, P. "Governing Big Data: Principles and Practices." *IBM Journal Od Research and Development* 57 (2013): 1–13.

Prayoga, Dimas, Fisilmy Hayati, Hanif Athar, Yuana Putra, and Irfan Nur Rizki. "Risiko Keamanan Data Pribadi Pelanggan Dalam Penggunaan Big Data" 5, no. 3 (2022): 459–63.

Rahmawati, Ineu. "Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense." *Jurnal Pertahanan & Bela Negara* 7, no. 2 (2017): 55–70.

Sautunnida, Lia. "Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia: Studi Perbandingan Hukum Inggris Dan Malaysia." *Jurnal Ilmu Hukum* 20, no. 2 (2018): 369–84.

Scott, M, James., Carter, G, Ralph., Drury, Cooper, A. *IR: International, Economic, and Human Security in a Changing World*. 3rd ed. CQ Press, 2018.

Sen, Amartya. "Human Rights and Capabilities." *Journal of Human Development* 6, no. 2 (2005).

Sugiyono. *Metode Penelitian Kualitatif Dan R&D*. Bandung: Alfabeta Press, 2012.

United Nations. "Cybercrime." Office on Drugs and Crime, 2022. https://www.unodc.org/unodc/en/cybercrime/index.html.

Vidi, Adyaksa. "4 Risiko Kebocoran Data Pribadi Dan Cara Mengantisipasinya Dengan Mudah." *Liputan 6*. August 30, 2021. https;/m.liputan6.com/cek-fakta/read/4645011/4-resiko-kebocoran-data-pribadi-dan-cara-mengantisipasinya-dengan-mudah.

W, Neil Adger & Juan M. Pulhin. *Human Security*. United Kingdom & New York: Cambridge University Press, 2014.

Widiatmanti, Herru & Madya Widyaiswara. "Aparatur Sipil Negara Di Era Society 5.0 Harus Bersikap Dan Berpikir Maju." Kanwil DJKN Jawa Timur, 2021. https://www.djkn.kemenkeu.go.id/kanwil-jatim/baca-berita/28123/Aparatur-Sipil-Negara-Di-Era-Society-50-Harus-Bersikap-dan-Berpikir-Maju.html.

Yunanda, Winka Wino, Fiorentina Nulhakim, and Nadia Aurora Soraya. "STRATEGI MENJAGA KEDAULATAN BANGSA DEMI KEUTUHAN NEGARA KESATUAN REPUBLIK INDONESIA DI ERA SOCIETY 5 . 0 DALAM PERSPEKTIF." *Jurnal Kewarganegaraan* 6, no. 1 (2022): 1195–1202.