PERLINDUNGAN DATA PRIBADI DALAM PERSPEKTIF KEBIJAKAN HUKUM PIDANA

Abd. Rahman Saleh

Program Studi Hukum Keluarga Islam, Fakultas Syariah dan Ekonomi Islam
Universitas Ibrahimy Situbondo

Email: ars201171@gmail.com

Abstrak

Keberadaan data pribadi merupakan data privasi yang harus dilindungi undang-undang. Kemajuan zaman dan kemajuan teknologi informasi membuat segala sesuatu dapat diakses begitu luas. Demikian juga keberadaan data pribadi harus disimpan dengan kuat agar tidak ada yang mencuri data pribadi dan tidak diretas oleh pencuri data pribadi dengan tujuan untuk ditransaksikan. Pelanggaran data pribadi peserta BPJS Kesehatan oleh "Akun Kotz" yang merupakan pembeli dan penjual data pribadi menjadi catatan tersendiri bagi negara untuk hadir guna melindungi pemilik data pribadi agar tidak diretas dan ditransaksikan. Kebijakan hukum pidana adalah solusinya, yaitu negara harus mengatur ruang hukum dan menentukan undang-undang tentang bagaimana sanksi pidana dapat dijatuhkan bagi peretas data. Sehingga orang yang memiliki data pribadi terlindungi secara hukum dan tidak menjadi korban peretasan peretasan data pribadi yang dicuri dan ditransaksikan. Kebocoran data pribadi sangat meresahkan dan sangat merugikan negara dan pemilik data pribadi dimana para pelaku pencurian data harus ditindak secara hukum agar ada perlindungan hukum bagi pemilik data pribadi.

Kata Kunci : Data Pribadi, Perlindungan Hukum, Kebijakan Hukum Pidana

Abstract

The existence of personal data is privacy data that must be protected by law. The progress of the times and the advancement of information technology have made everything accessible so widely. Likewise, the existence of personal data must be stored firmly so that no one steals personal data and is not hacked by personal data thieves with the aim of being transacted. The breach of personal data of BPJS Health participants by "Kotz Accounts" which are buyers and sellers of personal data is a separate record for the state to be present to protect the owner of personal data from being hacked and transacted. Criminal law policy is the solution, namely the state must regulate the legal space and determine the law on how criminal sanctions can be imposed for data hackers.

So that people who own personal data are legally protected and do not become victims of hackers hacking personal data that is stolen and transacted. Leakage of personal data is very disturbing and very detrimental to the state and the owner of personal data in which the perpetrators of data theft must be punished by law so that there is legal protection for owners of personal data

***Keywords**: Personal Data, Legal Protection, Criminal Law Policy*.

PENDAHULUAN

A. Latar Belakang

Bocornya data peserta BPJS Kesehatan yang dibobol oleh *hacker* menjadikan catatan tersendiri dalam perlindungan data peserta BPJS Kesehatan dalam keikutsertaan para anggotanya. Kementerian Komunikasi dan Informatika (Kominfo) membenarkan bahwa data peserta BPJS Kesehatan dibobol oleh *hacker*. Data yang seharusnya rahasia itu dijual di forum internet *Raid Forum* oleh akun bernama Kotz. Akun Kotz menawarkan 279 juta data penduduk Indonesia dengan tanggal posting 12 Mei 2021. Kotz juga mengklaim akan menyediakan 1 juta data yang bisa diunduh gratis sebagai sampel. Dari *link* yang diunduh Jawa Pos, data yang disimpan dalam format Microsoft Excel itu memuat informasi seperti nama, nomor kepesertaan, nomor telepon dan sebagainya. Kabar itu sebenarnya telah mencuat pada tanggal 20 Mei 2021. Kominfo juga melakukan investigasi dan mengonfirmasi bahwa data peserta BPJS Kesehatan benar-benar bocor dan dimiliki oleh Kotz. "Akun Kotz sendiri merupakan pembeli dan penjual data pribadi (*reseller*)" kata Jubir Kominfo Dedy Permadi[1]

Peristiwa yang demikian menimbulkan gejolak kegelisahan bagi negara dan juga bagi para peserta BPJS Kesehatan. Karena data- data yang demikian adalah data pribadi yang kerahasiaan datanya tentunya harus menjadi perlindungan bagi negara untuk melindunginya. Negara juga mempunyai kewajiban bahwa ada proteksi perlindungan hukum bagi peserta BPJS Kesehatan agar data-data tersebut terlindungi secara informasi data dan juga tentunya

[1] Surat Kabar Harian Jawa Pos, Sabtu, 22 Mei 2021

terlindungi dari sisi hukum. Dalam arti harus ada perlindungan hukum yang nyata dan utuh bagi kerahasiaan data tersebut agar tidak bocor dan disalah gunakan oleh pihak lain dalam segala hal transaksi yang dampaknya nantinya adalah adanya kerugian bagi negara dan kerugian bagi para peserta BPJS Kesehatan.

Harus ada sinergi kesinambungan antar pihak agar perlindungan data BPJS Kesehatan utuh dan tidak ter*hack* oleh pihak lain yang ujung-ujungnya adalah ditransaksikan. Menteri kesehatan harus proaktif melakukan pemantauan data-data yang bocor tersebut juga Kementerian Komunikasi dan Informatika (Kemenkominfo), Badan Siber dan Sandi Negara (BSSN), *Cybercrime* Mabes Polri, Pusat Pertahanan Siber Kementerian Pertahanan, Kementerian Koordinator Bidang Politik, Hukum, dan Keamanan (Kemenko Polhukam), Kementerian Koordinator Bidang Pembangunan Manusia dan Kebudayaan (Kemenko PMK) serta pihak-pihak lainnya.

Bahkan peretasan juga terhadap data Covid 19 yang setelah dideteksi *hacker* Kotz juga adalah pelakunya dan ternyata melibatkan warga negara lain yakni terdeteksi warga Afghanistan. Ini tentunya merupakan kejahatan lintas negara bukan lintas dalam negeri saja. Tentunya hal yang demikian merupakan globalisasi kejahatan ekonomi yang sangat berdampak luas bagi antar negara. Globalisasi kejahatan ekonomi saat ini adalah sangat sistemik yang berakar pada hubungan bebasnya ruang gerak tingkat komunikasi yang semakin maju dan sangat mudah ditransaksikan secara kejahatan dalam dilakukannya kejahatan. Kejahatan ini adalah merupakan kejahatan lintas negara yang sangat menjadi ancaman serius bagi peradaban kemajuan bangsa terutama dalam sisi keamanan dan kemakmuran global yang mengingat sifatnya melibatkan berbagai negara.

Peretasan atau *hacking* terhadap data-data pelanggan BPJS Kesehatan dan juga data Covid 19 adalah sifatnya transaksional karena sudah ada penawaran transaksi yang dijual di forum internet *Raid Forum* yang dilakukan oleh akun bernama Kotz. Ini jelas merupakan globalisasi kejahatan ekonomi yang memanfaatkan situasi untuk dilakukan hacker dan peretasan secara tersistem. Semuanya tidak lepas dari era globalisasi yang semakin hari semakin menyeruak sebagai era keterbukaan dan era industri. Kejahatan yang demikian adalah merupakan bentuk kejahatan dengan modus operandi *cyber crime* yang

merupakan kejahatan tanpa batas dan juga melibatkan lintas negara dalam melakukan transaksi kejahatannya. Kejahatan ekonomi *cybercrime* ini tidak lepas dari pengaruh globalisasi dan juga pengaruh globalisasi kejahatan ekonomi yang semakin canggih.

Inilah hanyalah sebagai contoh terhadap lemahnya perlindungan data pribadi sehingga data pribadi mudah dibobol dan mudah di *hack,* dicuri dan ditransaksikan. Para pencuri data memanfaatkan lemahnya hukum dan perlindungan hukum terhadap keberadaan data pribadi. Negara mempunyai tanggung jawab untuk hadir melindungi pemilik data pribadi agar terlindungi secara hukum. Kebijakan hukum pidana negara harus mengatur dan menentukan perbuatan apa saja yang bisa dipidana dan sanksi hukum apa yang bisa diberikan kepada *hacker* dan pencuri data pribadi yang ditransaksikan.

B. Perumusan Masalah

Kebijakan hukum pidana dalam mengatur perlindungan data pribadi adalah kebutuhan pokok yang menuntut negara harus mengatur apa saja dan perbuatan apa saja yang dilarang dalam taksasi terhadap data-data pribadi. Karena kebijakan hukum pidana pada dasarnya adalah keseluruhan peraturan dari negara yang menentukan perbuatan apa saja yang dilarang dan termasuk ke dalam tindak pidana, serta bagaimana sanksi yang dijatuhkan terhadap pelakunya dengan tujuan untuk menanggulangi adanya kejahatan.

C. Metode Penelitian

Tulisan ini menggunakan metode tinjauan hukum, yakni metode hukum normatif yang arahnya untuk mengetahui apakah dan/atau bagaimanakah hukum positif mengatur atau kebijakan hukum pidana yang mengatur perlindungan terhadap data pribadi, dalam kaitannya terhadap kebijakan hukum pidana. Adakah hukum pidana yang mengatur proteksi perlindungan hukum terhadap data pribadi. Sehingga nantinya akan ditemukan kebijakan hukum pidana yang tepat dalam alur pemidanaan bagi pelaku yang mengakibatkan bocornya data pribadi yang telah di *hack* dan/atau telah dicuri. Hukum normatif yang mengatur keberadaan data pribadi sejauh mana menjangkau hukum terhadap perlindungan

data–data pribadi. Metode normatif hukum sebagai acuan untuk ditemukannya kebijakan hukum pidana dalam pemidanaan nantinya.

PEMBAHASAN

Pentingnya Perlindungan Data pribadi Dalam Era Globalisasi

Perkembangan zaman yang semakin maju, yang semakin berkembang tidak lepas dari era globalisasi sebagai arah kemajuan suatu bangsa di setiap bangsa. Hal ini sebagai arah dan tuntutan zaman yang semakin maju dan semakin berkembang sesuai arah modern yang tidak bisa terhindarkan. Bagaimanapun bangsa akan maju mana kala sejalan dengan bangsa lain dalam kemajuannya dengan prinsip globalisasi yang menjadi ukuran peradaban kemajuannya.

Globalisasi ditandai dengan adanya keterbukaan dan kebebasan dalam berbagai bidang kehidupan yang mengakibatkan perubahan dalam berbagai aspek kehidupan yang berlangsung secara cepat[2]**.** Melalui globalisasi serta keterbukaan teknologi informasi maka kegiatan di segala bidang menjadi bersifat terbuka sehingga mengakibatkan komunikasi dan informasi dapat diakses dan dilakukan dimana saja dan kapan saja. Bentuk informasi secara elektronik bukanlah merupakan suatu hal yang baru lagi, dimana dengan informasi elektronik, maka segala yang berkaitan dengan informasi yang ingin diketahui dengan cara akses yang sangat mudah dan murah, yakni melalui media elektronik yang menyediakan secara lengkap mengenai informasi yang diinginkan.[3]

Sebagai konsekuensi dari globalisasi juga membawa pengaruh terhadap perkembangan hukum di berbagai bidang, hal itu sebagai akibat berkembangnya pranata-pranata teknologi informasi yang mau tidak mau juga melahirkan suatu pranata hukum baru yang bersifat mengimpor hukum asing khususnya hukum yang berasal dari tradisi hukum *Anglo Saxon* dengan sistem hukum *Common Law*.[4]

Dengan kemajuan teknologi maka telah berkembang bentuk-bentuk informasi dan komunikasi yang merupakan bentuk informasi serta hubungan hukum yang

[2] Hikmahanto Juwana, *Hukum Ekonomi dan Hukum Internasional*, (Jakarta: Lentera Hati, 2002), hlm.25.
[3] Sampara Lukman, *Manajemen Kualaitas Pelayanan*. (Jakarta: STIA LAN Press, 2000), hlm.74
[4] T. Mulya Lubis (Ed), *Peranan Hukum Dalam Prekonomian di Negara Berkembang,* (Jakarta: Yayasan Obor Indonesia, 1986), hlm.72.

ramai dibicarakan sebagai online. Yaitu Informasi yang dilakukan secara elektronik dengan memadukan jaringan (*networking*) dari sistem informasi berbasis komputer dengan sistem komunikasi yang berbasis jaringan dan jasa telekomunikasi.[5]

Perkembangan globalisasi kejahatan ekonomi adalah selalu mengikuti dinamika globalisasi. Dimana dalam era globalisasi semakin diikuti dengan kejahatan lainnya yang sangat berdampak pada keamanan dalam era globalisasi. Munculnya berbagai bentuk kejahatan dalam dimensi baru, akhir-akhir ini, menunjukkan kejahatan itu berkembang sesuai dengan perkembangan masyarakatnya. Selanjutnya, sebagaimana ditulis oleh Benedict S. Alper[6] bahwa kejahatan itu sebenarnya merupakan problem sosial yang paling tua dan sehubungan dengan masalah tersebut sudah tercatat lebih dari 80 kali konferensi internasional yang dimulai tahun 1825 hingga tahun 1970 yang membahas upaya-upaya untuk mengatasi persoalan kejahatan.

Globalisasi kejahatan ekonomi semakin nyata masuk di segala sisi dengan atribut yang bisa ditransaksikan secara ekonomi maka disitu selalu ada kejahatan. Tidak lepas juga dengan data-data pengguna BPJS Kesehatan sudah ditransaksikan dan dijual dengan akun Kotz. Seharusnya ada perlindungan keamanan data yang ada terlindungi oleh negara. Bobolnya data pengguna BPJS Kesehatan oleh akun Kotz hal ini menandakan tidak ada proteksi hukum dan perlindungan hukum bagi data-data yang ada. Untuk memastikan keamanan data BPJS kesehatan harus mengimplementasikan sistem keamanan data yang sesuai dengan standar ISO 27001 (*certified*), *Control Objectives for Information Technologies* (COBIT) serta mengoperasikan *Security Operation Center* (SOC) yang bekerja 24 jam 7 hari. BPJS Kesehatan harus melakukan hubungan dan atau kerjasama yang menyeluruh dengan Badan Siber dan Sandi Negara (BSSN) untuk mengungkap kejahatan bobol data yang ada di BPJS Kesehatan.

Bobolnya data BPJS Kesehatan yang ditransaksikan oleh peretasan *hacker* menjadi problem hukum negara. Bagaimana negara harus hadir dan menjadi

[5] Gunarto Suhardi, *Peranan Hukum dalam Pembangunan Ekonomi*, (Yogyakarta; Universitas Atma Jaya, 2002), hlm 26.
[6] Benedict S. Alper, *Changing Concept of Crime and Criminal Plicy*. Dalam *Resource Material Series* No.6 UNAPEL, (Fuchu, Tokyo, Japan, Oktober 1993), hlm. 65

penyelamat terhadap data-data pengguna BPJS Kesehatan yang diretas dan diperjual belikan dan ditransaksikan. Peretasan oleh *hacker* data BPJS Kesehatan ini merupakan kejahatan ekonomi serius yang harus disikapi dengan alur penegakan hukum bagi pelakunya. Kejahatan ekonomi ini dalam peretasan data-data BPJS Kesehatan adalah merupakan globalisasi kejahatan yang tidak lepas dari global ekonomic yang semakin menantang kedepannya.

Menurut Mardjono Reksodiputro.[7] Bahwa yang dimaksud dengan kejahatan ekonomi adalah setiap perbuatan yang melanggar peraturan perundang-undangan dalam bidang perekonomian dan bidang keuangan serta mempunyai sanksi pidana. Data BPJS Kesehatan yang dijual melalui peretasan *hacker* oleh Kotz termasuk dalam klasifikasi kejahatan ekonomi global dan atau merupakan globalisasi kejahatan ekonomi. Karena sasaran peretasan *hacker* pada ujungnya adalah menjual data dan menjual informasi data yang ada di data peserta BPJS Kesehatan. Ini adalah globalisasi kejahatan yang semakin canggih dan terarah dengan memanfaatkan teknologi kekinian yakni melalui akun-akun yang mudah dibuat dan mudah juga disalahgunakan untuk kejahatan. Globalisasi kejahatan ekonomi di dalam peretasan data peserta BPJS kesehatan adalah data kejahatan yang memerlukan kecerdikan hukum dalam meranjau pelakunya untuk bisa dijerat dengan hukum pidana.

Data yang seharusnya rahasia itu dijual di forum internet *Raid Forum* oleh akun bernama Kotz. Akun Kotz menawarkan 279 juta data penduduk Indonesia dengan tanggal posting 12 Mei 2021. Kotz juga mengklaim akan menyediakan 1 juta data yang bisa diunduh gratis sebagai sampel. Bahkan data pasien covid 19 juga diretas dan di hack dan dijual datanya. Data data peserta BPJS kesehatan data-data yang telah di hacker bisa dijual dan ditransaksikan dengan globalisasi kejahatan ekonomi data yang demikian sangat potensial dimanfaatkan untuk melakukan tindakan kejahatan global. Diantaranya, *fraud* atau penipuan dan judi *online* yang pembelinya adalah tentu adalah penjahat juga. Apabila data tersebut dibeli untuk keperluan kejahatan, sudah pasti rakyat Indonesia sedang dalam ancaman menjadi

[7] Mardjono Reksodiputro, *Hukum Positif Mengenai Kejahatan Ekonomi dan Perkembangannya di Indonesia*. Dalam Rangkuman Seminar Ihtisar dan Kumpulan Makalah tentang Kejahatan Ekonomi di Bidang Perbankan, (Jakarta: Bank Indonesia, 4-7 Januari 1993), hlm. 326

korban. Jumlah data yang dijual mencapai 279 juta orang atau sebanyak jumlah warga negara Indonesia.

BPJS Kesehatan telah bertindak cekatan dengan melihat kejadian yang demikian langsung melaporkan ke Kepolisian Republik Indonesia untuk melacak keberadaan transaksi alih akun *hacker* Kotz yang telah mentransaksikan data–data BPJS Kesehatan dan juga data-data pasien Covid 19. Hasil pelacakan awal yang dilakukan oleh Mabes Polri diketahui bahwa *hacker* tersebut seorang warga negara Afghanistan dan selanjutnya terlacak lagi dia tidak tinggal di negara asalnya tapi telah berada di Qatar, yang terlacak terhadap keocoran data pasien Covid 19. Ini jelas membuktikan bahwa *cybercrime* itu *borderless* (tanpa batas) dan lintas negara. *Hacker* luar negara atau hacker luar negeri telah menyasar Indonesia. Ini menuntut sebuah kerja polisi untuk bekerjasama dengan interpol untuk mengajukan permintaan *red notice* ke Interpol pusat di Lyon, Prancis

Kebijakan Hukum Pidana terhadap *Cyber Crime Hacking* Data Pribadi

Terhadap data BPJS yang dihack, Tim Bareskrim Mabes Polri menemukan beberapa bukti bahwa Kotz diduga berusia 19 tahun dan tinggal di luar Jawa. Hal ini setelah Bareskrim berkoordinasi dengan negara lain, yaitu dengan negara Rusia dan Singapura. Koordinasi ini dilakukan dan terjadi karena akun *anonymous* itu menggunakan *IP addres* dari negara tersebut. Koordinasi lintas negara ini dilakukan pelaku menggunakan Telegram yang berasal dari negara tersebut. Ternyata setelah diselidiki lebih jauh *hacker* tersebut tinggal di Indonesia dan berada di luar pulau Jawa.

Bagaimana kejahatan *hacking* peserta BPJS Kesehatan ini memanfaatkan celah-celah ruang untuk melakukan kejahatan. Tentu ini tidak lepas dari semakin globalnya transaksi ekonomi dengan alat yang serbah canggih pula dengan data elektronik. Kejahatan yang demikian harus bisa ditinjau dengan hukum pidana yang ada sebagai alur pemidanaan agar pelakunya bisa dipidana dan bisa mempertanggungjawabkan perbuatannya. Negara tidak bisa hanya membiarkan kejahatan ekonomi yang demikian. Semuanya itu tidak bisa lepas dengan kejahatan lintas negara , karena kejahatan dengan *cyber crime* sudah melampaui batas negara.

Berdasarkan catatan dari *National Criminal Intelligence Services* (NCIS) di Inggris terdapat 13 macam bentuk-bentuk *cybercrime*. *Pertama*, *Recreational Hackers*, kejahatan ini dilakukan oleh *netter* tingkat pemula untuk iseng-iseng mencoba kekurangandalan dari sistem sekuritas atau keamanan data suatu perusahaan. Tujuan iseng-iseng ini oleh pelaku dimaksudkan sekedar hiburan akan tetapi mempunyai dampak pada kejahatan maya yang secara langsung maupun tidak langsung merugikan pihak lain. *Kedua*, *Crackers* atau *Criminal Minded Hackers*, yaitu pelaku kejahatan ini biasanya memiliki motivasi untuk mendapatkan keuntungan finansial, sabotase, dan penghancuran data pihak korban. Sebagai contoh pada tahun 1994 Citibank AS di Inggris mengalami kebobolan senilai US $ 400.000 oleh *cracker* dari Rusia. Pelaku akhirnya dapat ditangkap dan dijatuhi pidana penjara selama tiga tahun serta harus mengembalikan sejumlah uang yang dijarah. Tipe kejahatan ini dapat terjadi dengan bantuan orang dalam yakni biasanya adalah staf karyawan yang "sakit hati" atau datang dari kompetitor dalam kegiatan bisnis sejenis.

Ketiga, *Political Hackers*, yakni aktivis politik atau *hackactivist* melakukan perusakan terhadap ratusan situs web untuk mengkampanyekan program-program tertentu bahkan tidak jarang digunakan untuk menempelkan pesan untuk mendiskreditkan lawan politiknya. Usaha tersebut pernah dilakukan secara aktif dalam upaya kampanye anti Indonesia pada masalah Timor Timur yang dipelopori oleh Ramos Horta dan kawan-kawannya, sehingga situs Departemen Luar Negeri Republik Indonesia sempat mendapat serangan yang diduga keras dari kelompok anti integrasi sebelum dan setelah jajak pendapat tentang Referendum Timor Timur tahun 1999 lalu.

Keempat, *Denial of Service Attack*. Serangan tujuan ini adalah untuk memacetkan sistem dengan mengganggu akses dari pengguna jasa internet yang sah. Taktik yang digunakan adalah dengan mengirim atau membanjiri situs web dengan data sampah yang tidak perlu bagi orang yang dituju. Pemilik situs web menderita kerugian, karena untuk mengendalikan atau mengontrol kembali situs web tersebut dapat memakan waktu tidak sedikit yang menguras tenaga dan energi. *Kelima*, *Insiders (Internal) Hackers* yang biasanya dilakukan oleh orang dalam perusahaan sendiri. Modus operandinya adalah karyawan yang kecewa atau bermasalah dengan pimpinan korporasi dengan merusak data atau akses data dalam transaksi bisnis.

Contoh Departemen Perdagangan dan Perindustrian Inggris pernah mengumumkan bahwa tahun 1998 perusahaan di negeri itu menderita kerugian senilai 1,5 miliar poundsterling, akibat kelakuan musuh dalam "selimut" ini.

Keenam, *viruses*. Program pengganggu (*malicious*) perangkat lunak dengan melakukan penyebaran virus yang dapat menular melalui aplikasi internet, ketika akan diakses oleh pemakai. Sebelum ditemukan internet, pola penularan virus oleh *hackers* hanya bisa melalui *floppy disk*. Akan tetapi dengan berkembangnya internet dewasa ini, virus dapat bersembunyi di dalam *file* dan *downloaded* oleh *user* (pemakai) bahkan menyebar pula melalui kiriman *e-mail*. Seperti "dunia kedokteran", maka pada "dunia komputer" memang telah menciptakan jurus anti virus seperti Melissa 1999 atau Lovebug 2000 dan sebagainya, namun masih belum dapat berbuat banyak untuk membasmi semua jenis virus komputer yang terus berkembang dengan pesat.

Ketujuh, *piracy*. Pembajakan *software* atau perangkat lunak komputer merupakan *trend* atau kecenderungan yang terjadi dewasa ini, karena dianggap lebih mudah dan murah untuk dilakukan para pembajak dengan meraup keuntungan berlipat ganda. Pihak produsen *software* yang memproduksi piranti induk (master) dari permainan (*games*), film dan lagu dapat kehilangan *profit* atau keuntungan karena karyanya dibajak melalui *download* dari internet dan dikopi ke dalam bentuk CD-ROM yang selanjutnya diperbanyak secara ilegal atau tanpa seizin penciptanya melalui *video caset decoder* (VCD), *compact disc* (CD), *playstation* dan *cassette recorder*.

Kedelapan, *fraud* adalah sejenis manipulasi informasi keuangan dengan tujuan untuk mengeruk keuntungan sebesar-besarnya. Sebagai contoh adalah harga tukar saham yang menyesatkan melalui rumor yang disebarkan dari mulut ke mulut atau tulisan. Begitu juga dengan situs lelang fiktif dengan mengeruk uang masuk dari para peserta lelang karena barang yang dipesan tidak dikirim bahkan identitas para pelakunya tidak dapat dilacak dengan mudah. *Kesembilan*, *gambling*. Perjudian di dunia maya semakin global sulit dijerat sebagai pelanggaran hukum apabila hanya memakai hukum nasional suatu negara berdasarkan pada *locus delicti* atau tempat kejadian perkara, karena para pelaku dengan mudah dapat memindahkan tempat permainan judi dengan sarana komputer yang dimilikinya secara mobil. Dari kegiatan

gambling ini (juga kejahatan-kejahatan lainnya seperti pengedaran narkoba, perdagangan senjata gelap, dll.), uang yang dihasilkan dapat diputar kembali di negara yang merupakan *the tax heaven*, seperti Cayman Island yang juga merupakan surga bagi para pelaku *money laundrying*. Indonesia sering pula dijadikan oleh pelaku sebagai negara tujuan pencucian uang yang diperoleh dari hasil kejahatan berskala internasional. Upaya mengantisipasinya adalah diterbitkannya UU No. 15 Tahun 2002 tentang Pencucian Uang.

Kesepuluh, *pornography* and *paeddophilia*. Perkembangan dunia maya selain mendatangkan berbagai kemaslahatan bagi umat manusia dengan mengatasi kendala ruang dan waktu, juga telah melahirkan dampak negatif berupa "dunia pornografi" yang mengkhawatirkan berbagai kalangan terhadap nilai-nilai etika, moral dan estetika. Melalui *newsgroup*, *chat rooms* bahkan mengeksploitasi pornografi anak anak di bawah umur, kegiatan *hacker* ini amat meresahkan bagi kalangan orang tua, agamawan dan masyarakat beradab. *Kesebelas*, *cyber stalking* adalah segala bentuk kiriman *e-mail* yang tidak dikehendaki oleh user atau *junk e-mail* yang sering memakai *folder* serta tidak jarang dengan pemaksaan. Walaupun *e-mail* "sampah" ini tidak dikehendaki oleh para user bahkan secara paksa memperoleh identitas personal secara detail tentang calon para korbannya, akan tetapi kiriman ini sangat merepotkan dan menghabiskan waktu *user* untuk membersihkan halaman komputernya dari "sampah" tidak diundang ini. Para pemakai komputer hanya bisa menggerutu terhadap pelakunya.

Dua belas, *hate sites*. Situs ini sering digunakan oleh *hacker* untuk saling menyerang dan melontarkan komentar-komentar yang tidak sopan dan vulgar yang dikelola oleh para "ekstrimis" untuk menyerang pihak-pihak yang tidak disenanginya. Penyerangan terhadap lawan atau *opponent* ini sering mengangkat pada isu-isu rasial, perang program dan promosi kebijakan ataupun suatu pandangan (isme) yang dianut oleh seseorang/kelompok, bangsa dan negara untuk bisa dibaca serta dipahami orang atau pihak lain sebagai "pesan" yang disampaikan. *Ketiga belas*, *criminal communications*. NCIS telah mendeteksi bahwa internet dijadikan sebagai alat yang andal dan modern untuk melakukan kegiatan komunikasi antar *gangster*, anggota sindikat obat bius dan bahkan komunikasi antar "*hooligan*" di dunia sepakbola Inggris. Komunikasi lewat internet merupakan alat atau sarana yang cukup

ampuh untuk melakukan kejahatan terorganisir. Bagaimanakah dengan kasus kriminalitas atau modus operandi yang berbasiskan pada teknologi digital di Indonesia?. Beberapa kasus kejahatan maya yang terjadi dan ditangani oleh penegak hukum kepolisian lebih banyak bermotifkan pada masalah ekonomi antara lain pembobolan rekening bank yang dialami BNI Cabang New York (1987) dengan kerugian Rp. 30 miliar, Bank Danamon Jakarta (1990) sebanyak Rp. 372 miliar, Bank Panin Cabang Senayan, Jakarta (1995) sebanyak Rp. 4,2 miliar, Hongkong Bank di Jakarta (1996) sebanyak Rp. 96 miliar. Kasus penyadapan *credit card* pada beberapa daerah sempat marak pada tahun 2001 lalu.

Pada tahun 2010, *Conference of States Parties* (CoSP) UNTOC yang kelima telah mengidentifikasi beberapa kejahatan lintas negara baru dan berkembang (*New and Emerging Crimes*), antara lain *cyber crime, identity-related crimes*, perdagangan gelap benda cagar budaya, kejahatan lingkungan, pembajakan di atas laut, dan perdagangan gelap organ tubuh. Kejahatan Lintas Negara Baru telah menjadi perhatian dari dunia Internasional mengingat jumlahnya yang semakin meningkat dan cara yang semakin beragam. Begitu juga dengan kerugian yang ditimbulkan dari kejahatan jenis ini adalah sangat besar.

Lalu bagaimana untuk melindungi para peserta BPJS Kesehatan yang datanya telah ditransaksikan secara elektronik yang diduga dilakukan oleh akun Kotz. Serta bagaimana jerat hukum pidana yang harus ditimpakan kepada pelaku yang telah melakukan tindak pidana dalam globalisasi kejahatan ekonomi dengan memanfaatkan ruang media akun sebagai transaksinya. Ini adalah merupakan tantangan bagaimana sistem hukum kita bisa menjangkau agar benar-benar ada perlindungan hukum bagi data peserta BPJS Kesehatan.

Pada dasarnya perlindungan terhadap data pribadi tidak hanya terkait dengan bocornya data pribadi para peserta BPJS Kesehatan, akan tetapi bagaimana hukum negara mengatur terhadap data-data pribadi terlindungi dan tidak dijadikan bancakan hukum dalam transaksi melalui *hacking data*. Kejahatan dalam transaksi data-data pribadi adalah sangat tertata dengan rapi, karena *hacking data* tidak hanya mengandalkan teknologi informasi akan tetapi juga merupakan keahlian yang dimiliki oleh pencuri data telah tertata dengan kemampuan keahlian yang dimilikinya, sehingga sangat mudah meng*hack* data pribadi.

Kebijakan Hukum Pidana dan Sanksi Hukum Terhadap Hacker Data Pribadi

Kejahatan atau tindakan kriminal merupakan salah satu bentuk dari prilaku menyimpang.[8] Prof. Sudarto, berpendapat bahwa dalam menghadapi masalah kejahatan atau kriminal harus diperhatikan hal - hal yang pada intinya sebagai berikut.

a. Tujuan penggunaan hukum pidana harus memperhatikan tujuan pembangunan nasional yaitu mewujudkan masyarakat adil dan makmur yang merata materiil dan spirituil berdasarkan Pancasila. Sehubungan dengan ini penggunaan hukum pidana bertujuan untuk menanggulangi kejahatan dan mengadakan penyegaran terhadap tindakan penanggulangan itu sendiri, demi kesejahteraan dan pengayoman kepada masyarakat.
b. Perbuatan yang diusahakan untuk mencegah atau menanggulangi dengan hukum pidana harus merupakan "perbuatan yang tidak dikehendaki" yaitu perbuatan yang mendatangkan kerugian (materiil dan spirituil) atas warga masyarakat.
c. Penggunaan hukum pidana harus pula memperhitungkan prinsip"biaya dan hasil"
d. Penggunaan hukum pidana harus pula memperhatikan kapasitas atau kemampuan daya kerja dari badan-badan penegak hukum, yaitu jangan sampai ada kelampauan beban tugas (*overbelasting*) [9]

Sedangkan menurut pendapat Prof. Dr. Wirjono Prodjodikoro, SH, tujuan dari hukum pidana ialah untuk memenuhi rasa keadilan. Kemudian beliau menambahkan pula bahwa diantara para Sarjana Hukum diutarakan, tujuan hukum pidana, ialah :

a. Untuk menakut-nakuti orang jangan sampai melakukan kejahatan, baik secara menakut-nakuti orang banyak (*generale preventie*), maupun secara menakut-nakuti orang tertentu yang sudah menjalankan kejahatan lagi (*speciale preventie*), atau
b. Untuk mendidik atau memperbaiki orang-orang yang sudah menandakan suka melakukan kejahatan, agar menjadi orang yang baik taibiatnya, sehingga bermanfaat bagi masyarakat.

[8] Saparinah Sadli, *Persepdi Sosial Mengenai Prilaku Menyimpang*, (Jakarta: Bulan Bintang, 1976), hlm. 8
[9] Sudarto, *Hukum dan Hukum Pidana*, (Bandung: Alumni, 1981), hlm. 44

Pandangan-pandangan ini dapat saja beliau diterima sebagai tujuan sekunder atau tujuan tambahan, dan tujuan ini, meskipun bersifat tambahan, mungkin ada peranan besar sekali dalam meluruskan neraca kemasyarakatan, yang bagi saya tetap merupakan tujuan primer dari sanksi pidana, seperti juga tujuan dari sanksi administrasi dan sanksi perdata .

Barda Nawawi Arief, memandang bahwa istilah "Kebijakan" diambil dari istilah "*policy*" (Inggris) dan " *politiek*" (Belanda), sehingga "Kebijakan Hukum Pidana" dapat pula disebut dengan istilah "Politik Hukum Pidana" dan yang sering dikenal dengan istilah "*penal policy*", "*criminal law policy*" atau " *strafrechspolitiek*".[10]

Perlindungan data pribadi seharusnya mempunyai perlindungan hukum yang nyata dan konkrit agar data pribadi terlindungi secara hukum. Karena bagaimanapun data pribadi adalah sebuah privasi yang harus terlindungi datanya. Hal ini agar data pribadi tidak disalahgunakan dan dimanfaatkan oleh orang lain. Sehingga kebutuhan perlindungan data pribadi adalah harus ada dan negara hadir untuk melindunginya. Indonesia sendiri belum memiliki aturan soal perlindungan data pribadi karena draft RUU Perlindungan Data Pribadi belum disahkan oleh DPR. Perlindungan hukum yang dipakai dan/atau payung hukum yang dipakai saat ini hanya melalui Peraturan Pemerintah Nomor 71 Tahun 2019 tentang penyelenggaraan Sistem dan Transaksi Elektronik dan Peraturan Menteri Kominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik. Dalam aturan tersebut Penyelenggara Sistem Elektronik (PSE) yang sistem elektroniknya mengalami gangguan serius akibat kegagalan perlindungan data pribadi wajib melaporkan dalam kesempatan pertama kepada Kementerian Kominfo dan pihak berwenang lain. Selain itu Penyelenggara Sistem Elektronik wajib menyampaikan pemberitahuan secara tertulis kepada pemilik data pribadi jika diketahui terjadi kegagalan perlindungan data pribadi.

Pasal 36 dalam Peraturan Menteri Komunikasi dan Informatika Nomor 20 tahun 2016 yakni pihak yang menyebarluaskan data pribadi dikenai sanksi berupa peringatan lisan dan tertulis, penghentian kegiatan, atau pengumuman di situs *online*.

[10] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana Perkembangan Konsep Baru*, Cetakan Ke-1, (Jakarta: Kencana Prenadamedia Grup, 2008), hlm 26

Aturan yang demikian adalah merupakan aturan turunan dari pasal 26 ayat (1) dari Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, yang menyatakan bahwa penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan yang bersangkutan.

Data pribadi adalah wajib dilindungi. Semua pihak, baik badan publik maupun pihak swasta yang memiliki dan menyimpan data pribadi seseorang harus melindungi kerahasiaanya. Hal ini sejalan dengan dengan Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, serta Undang-Undang Nomor 24 tahun 2013 tentang Perubahan atau Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan. Tentunya saat ini adalah sudah darurat perlindungan data pribadi. Sebab jaminan hukum atas perlindungan data pribadi masih sangat lemah. Tidak cukup perlindungan data pribadi hanya diatur dengan adanya sebuah Peraturan Pemerintah tapi harus diatur dengan sebuah undang-undang agar perlindungan hukum terhadap data pribadi menjadi kenyamanan bagi masyarakat dan negara. Kebijakan hukum pidana negara harus hadir melindungi hukum pemilik data pribadi sebagai arah negara melindungi data-data pribadi yang dimiliki warga masyarakat negara. Pemidanaannya juga harus jelas dan terukur bagi peretas data pribadi yang merusak tatanan perlindungan data pribadi. Kejelasan pemidanaan akan sangat berdampak pada penegakan hukum yang konkrit apabila ada peretasan data atau *hacking data* terhadap data pribadi. Ketidakjelasan sanksi hukum dan embivalensi hukum terhadap pencuri data pribadi akan menyebabkan peretasan data selalu memanfaatkan ruang celah lemahnya hukum terhadap perlindungan hukum terhadap data-data pribadi.

Lemahnya kebijakan pemerintah dalam kebijakan hukum pidana terhadap lemahnya sanksi hukum akan menyebabkan kerugian yang sangat besar sekali bagi negara karena tidak bisa melindungi pemilik data pribadi. Kejahatan lintas negara yang semakin komplek dengan sistem informasi yang serba digital membuka ruang transaksional bagi pemanfaatan transaksi dengan menggunakan hacker data sebagai alur transaksinya. Globalisasi kejahatan ekonomi tidak akan ada kalau tidak ada peluang untuk melakukan kejahatan. Untuk itu diperlukan hukum yang kuat yang melindungi data-data pribadi agar tidak diperdagangkan dan diperjual belikan. Jual

beli dan atau perdagangan data pribadi yang di*hack* terutama yang telah terdeteksi yakni data peserta BPJS Kesehatan adalah jelas merupakan merupakan dampak dari globalisasi ekonomi yang berdampak pada kejahatan globalisasi ekonomi. Ini tidak terhindari karena lintas negara dan arus informasi publik semakin terbuka ruangnya. Sementara perlidungan terhadap data pribadi itu sendiri sangat lemah.

Bagaimanapun hukum harus menjadi panglima agar retas data atau *hacking* bisa dijerat dan ditinjau secara hukum. Apabila hukum lemah dan tidak bisa menjangkau kejahatan akibat globalisasi kejahatan ekonomi yang multi dimensi maka tentunya adalah masyarakat yang dirugikan dan negara juga dirugikan. Lemahnya hukum dalam melindungi kejahatan dalam hacker akan menghancurkan peradaban bangsa. Bangsa akan lemah dan tidak akan bermartabat karena hukumnya lemah. Salah satu cara adalah adanya giat hukum terus dilakukan agar kejahatan transaksi data dan penjualan data tidak terjadi.

Untuk itu dalam kasus bobolnya data peserta BPJS Kesehatan harus memanfaatkan ruang hukum yang ada sebagai perlindungan hukum bagi data pribadi. Ranjau hukum yang bisa digunakan sebagai alur hukum dalam penegakan hukumnya yakni :

a. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang penyelenggaraan Sistem dan Transaksi Elektronik
b. Peraturan Menteri Kominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.
c. Undang-Undang Nomor 24 tahun 2013 tentang Perubahan atau Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan
d. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik
e. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik

Negara Indonesia harus terus mendorong di forum-forum internasional agar kejahatan lintas negara menjadi sinergi hukum dalam penanggulangannya dan pemberantasannya. Seperti pemeliharaan keamanan siber. Hal ini dilakukan karena kejahatan lintas negara belum banyak menjadi perhatian khususnya dari dunia internasional, serta belum juga memiliki studi, definisi dan kriminalisasi yang

mencukupi. Kerja sama internasional adalah sudah tidak terelakkan lagi harus dilakukan karena globalisasi kejahatan ekonomi dalam menanggulanginya harus lebih ditingkatkan dan lebih disinergikan.

Indonesia memiliki kepentingan besar agar kejahatan lintas negara diatur secara lebih komprehensif mengingat kerugian besar dari kejahatan tersebut, termasuk dengan cara melakukan kerjasama-kerjasama dalam rangka peningkatan kapasitas penegak hukum dan pertukaran informasi. Semuanya itu adalah untuk melindungi negara dan melindungi masyarakatnya agar terhindar dari segala bentuk kejahatan , baik kejahatan pada umumnya maupun kejahatan dalam konteks globalisasi kejahatan ekonomi yang sudah semakin canggih dan tidak terhindari lagi. Hukum harus menjadi pelindungnya.

KESIMPULAN

Dari pemaparan yang telah terurai diatas sangat penting bagaimana perlindungan data pribadi menjadi perhatian pemerintah dan negara. Bagaimanapun data pribadi adalah sangat krusial apabila bocor dan dibocorkan dan atau ada yang menghack untuk diperjual belikan. Hacker data pribadi menjadi persoalan manakala hukum tidak bisa menjangkau dan meranjau para pelaku hacker. Hukum harus hadir menjadi penyelamat terhadap data-data pribadi yang dimiliki.

Negara harus hadir menjadi penyelamat terhadap *hacking* data pribadi. Pada intinya data pribadi harus mendapatkan proteksi hukum dan perlindungan hukum agar keberadaannya tidak di hacker dan aman data. Dalam artian data-data pribadi harus aman dari hacker dan harus aman dari transaksi data yang dicuri demi dan untuk kepentingan bisnis finansial semata. Hukum pidana melalui kebijakan hukum pidana pemerintah harus melindungi data pribadi. serta negara harus menghukum para pelaku hacker data pribadi. Berilah sanksi hukum yang jelas yang mempunyai efek jera agar data pribadi tidak dicuri.

Kehadiran hukum pidana akan memberikan proteksi perlindungan hukum bagi tegaknya hukum terhadap hacking data pribadi. Melalui politik hukum pidana yang dipunyai negara, negara harus mampu menjerat pelaku hacking data yang diretas dan atau dicuri. Perlindungan data pribadi tidak akan ada dan tidak akan nyaman manakala hukum pidana atau kebijakan hukum pidana tidak mengaturnya

untuk memberikan sanksi hukum bagi tegaknya perlindungan data pribadi. Hukum pidana dan atau kebijakan hukum pidana harus menjadi penyelamat bagi tegaknya perlindungan data pribadi dengan pola kebijakan hukum pidana yang teratur dan terukur. Sehingga hukum benar benar tegak dan mampu menangkap transaksi data pribadi yang di *hacking*.

DAFTAR PUSTAKA

Alper, Benedict S., *Changing Concept of Crime and Criminal Plicy*. Dalam *Resource Material Series* No.6 UNAPEL, Fuchu, Tokyo, Japan, Oktober 1993.

Arief, Barda Nawawi, *Bunga Rampai Kebijakan Hukum Pidana Perkembangan Konsep Baru*, Cetakan Ke-1, Jakarta: Kencana Prenadamedia Grup, 2008.

Juwana, Hikmahanto, *Hukum Ekonomi dan Hukum Internasional*, Jakarta: Lentera Hati, 2002.

Lubis, T. Mulya (Ed), *Peranan Hukum Dalam Prekonomian di Negara Berkembang,* Jakarta: Yayasan Obor Indonesia, 1986.

Lukman, Sampara, *Manajemen Kualaitas Pelayanan*. Jakarta: STIA LAN Press, 2000.

Peraturan Menteri Kominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang penyelenggaraan Sistem dan Transaksi Elektronik

Reksodiputro, Mardjono, *Hukum Positif Mengenai Kejahatan Ekonomi dan Perkembangannya di Indonesia*. Dalam Rangkuman Seminar Ihtisar dan Kumpulan Makalah tentang Kejahatan Ekonomi di Bidang Perbankan, Jakarta: Bank Indonesia, 4-7 Januari 1993.

Sadli, Saparinah, *Persepdi Sosial Mengenai Prilaku Menyimpang*, Jakarta: Bulan Bintang, 1976.

Sudarto, *Hukum dan Hukum Pidana*, Bandung: Alumni, 1981

Suhardi, Gunarto, *Peranan Hukum dalam Pembangunan Ekonomi*, Yogyakarta; Universitas Atma Jaya, 2002.

Surat Kabar Harian Jawa Pos, Edisi Sabtu, 22 Mei 2021

Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik

Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 24 tahun 2013 tentang Perubahan atau Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan.