JURNAL HUKUM PIDANA
& KRIMINOLOGI
Volume 2 No 2 Oktober 2021

Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi

Adik Nur Luthiya[1] Benny Irawan[2] Rena Yulia[3]
[1] *Fakultas Hukum Universitas Sultan Ageng Tirtayasa, E-mail: adik.nurluthiya2@gmail.com*
[2]*Dosen Fakultas Hukum Universitas Sultan Ageng Tirtayasa, E-mail: benny.irawan@untirta.ac.id*
[3]*Dosen Fakultas Hukum Universitas Sultan Ageng Tirtayasa, E-mail: rena.yulia@gmail.com*

INFO ARTIKEL

Kata Kunci:
Kebijakan Hukum Pidana, Cyber Crime, Pencurian Data Pribadi

Cara pengutipan:
Adik Nur Luthiya, Benny Irawan, & Rena Yulia. Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi dan Informasi. JURNAL HUKUM PIDANA & KRIMINOLOGI, Vol 02 No 02 Edisi Oktober 2021 (hlm. 14-29)

Riwayat Artikel:
Dikirim: 25 Juli 2021
Direview: 29 Juli 2021
Direvisi: 08 Agt 2021
Diterima: 16 Agt 2021

ABSTRAK

Pencurian data yang dahulu dilakukan secara konvensional kini dapat dilakukan dengan lebih mudah melalui bantuan medium komputer dan internet dalam melakukan aksi kejahatannya, namun hingga saat ini belum ada pengaturan khusus untuk menanggulangi penyalahgunaan data pribadi sehingga menimbulkan persoalan hukum baru. Oleh karena itu, penelitian ini difokusan kepada bagaimana kebijakan hukum pidana terhadap pencurian data pribadi sebagai penyalahgunaan teknologi komunikasi dan informasi. Adapun hasil dari penelitian ini, yang merupakan penelitian secara konseptual, kebijakan hukum pidana yang saat ini digunakan untuk menanggulangi kasus pencurian data pribadi dilihat dari Pasal 362 dan pasal 363 ayat (1) ke 5 Kitab Undang-Undang Hukum Pidana (KUHP) dan Pasal 30 Jo. Pasal 46 dan pasal 32 Jo. Pasal 48 Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Sedangkan kebijakan hukum pidana terhadap pencurian data pribadi sebagai penyalahgunaan teknologi komunikasi dan informasi di masa yang akan datang dapat ditemukan dalam RUU KUHP 2019 dan RUU PDP 2020.

DOI: 10.51370/jhpk.v2i2.43

1. Pendahuluan

Manusia pada abad XXI sangat tidak dapat dilepaskan dari internet, semua aktifitas dan kebutuhannya sangat bergantung dengan internet, yang kemudian ditambah dengan adanya pandemi *Coronavirus Disease* 2019 (COVID-19) yang menyebar

dengan sangat masif sehingga banyak masyarakat melakukan kegiatannya dirumah seperti bekerja dari rumah, belajar dari rumah, berbelanja dari rumah, menjadikan dunia teknologi informasi dan komunikasi adalah suatu kebutuhan yang tidak bisa ditinggalkan.

Teknologi komunikasi dan informasi membawa dampak bagi masyarakat secara luas, baik dampak positif maupun negatif. Dampak positifnya adalah dapat memperoleh berbagai informasi, baik dari dalam maupun luar negeri, transaksi jarak jauh. Sedangkan dampak negatifnya adalah memberikan peluang untuk melakukan berbagai kejahatan, seperti penipuan, pencurian, pencemaran nama baik, keasusilaan, perjudian, pengancaman, perusakan dan teror yang seluruhnya dikenal dengan *cyber crime*.

Kemudian ditambah dengan keadaan yang semakin banyak perusahaan dan lembaga pemerintah yang mengalihkan kegiatan menuju digital, artinya semakin besar kemungkinan serangan siber meningkat. Berdasarkan data *Honeynet Map* Badan Siber dan Sandi Negara (BSSN), dalam jangka waktu 1 Januari 2020 sampai dengan 4 Juni 2021 Indonesia menjadi peringkat tertinggi serangan siber kedua setelah India sebanyak 58,124,687 serangan.[1]

Insiden siber merupakan kejadian yang mengganggu berjalannya sistem elektronik misalnya serangan virus, pencurian data, informasi pribadi, hak kekayaan intelektual perusahaan, *web defacement* dan gangguan akses terhadap layanan elektronik. Mekanisme *work from home* semakin memperbesar potensi risiko karena pekerjaan harus dilakukan melalui jaringan. Hal tersebut harus disikapi oleh organisasi sebagai momentum untuk membenahi kebijakan keamanan informasi untuk mengantisipasi insiden serangan siber. Persiapan yang baik akan memperkecil kerugian akibat pencurian informasi atau gangguan pada layanan dan insiden siber berkembang menjadi lebih luas.[2]

Perhatian terhadap pemberian perlindungan kepada data pribadi (*privacy data protection*) yang dicuri semakin mendapat perhatian dari masyarakat ketika salah satu perusahaan (*company*) media sosial terbesar di dunia mengalami pencurian data pribadi oleh beberapa pihak. Sebuah berita pencurian data pribadi tersebut sudah tersebar dengan cepat di berbagai media elektronik yang kemudian dengan mendapat pengakuan dari perusahaan tersebut bahwa telah terjadi pencurian data pribadi atau pengambilan data pribadi milik orang lain tanpa izin yang kemudian dikenal dengan sebutan informatik "pencurian data atau pembobolan data". Keadaan ini terjadi disebabkan karena adanya kelemahan pada sistem yang digunakan untuk menyimpanan data yang dimiliki oleh perusahaan sehingga data pribadi milik orang lain dapat dicuri oleh pihak yang tidak bertanggung jawab.[3]

Pada bulan Mei 2020 beberapa *E-Commerce* Indonesia diserang dengan upaya pencurian data pribadi. Pada tanggal 1 Mei muncul berita mengenai kebocoran data pengguna Tokopedia. Sebanyak 91 juta data yang dilaporkan sebagai data pengguna Tokopedia ditawarkan seharga US$5.000 di forum hacker. Dalam rilis resminya, Tokopedia menyatakan bahwa mereka "menemukan adanya upaya pencurian data

---

1 https://bssn.go.id/rekap-serangan-siber-januari-april-2020/ diakses 18 Maret 2021.

2 *Ibid.*

3 Natamiharja, Rudi (2018). A Case Study On Facebook Data Theft In Indonesia. *Flat Justisia*, 12(3), 206-223. doi: https://doi.org/10.25041/fiatjustisia.v12no3.1312

terhadap pengguna Tokopedia." Kemudian, Pada tanggal 6 Mei, sebanyak 12,9 juta data pengguna Bukalapak kembali diperjualbelikan. Data ini diduga merupakan data yang bocor pada Maret 2019. Sementara Bukalapak mengakui adanya akses tidak sah terhadap *cold storage* mereka (rilis Bukalapak). Pada 10 Mei, sebanyak 1,2 juta data yang diduga data pengguna toko online Bhinneka diketahui bocor dan ditawarkan untuk dijual di forum pasar gelap online (*dark web*). Bhinneka menyatakan masih melakukan investigasi terhadap dugaan kebocoran tersebut.[4]

Satu tahun kemudian pada 12 Mei 2021, 279 juta data pribadi penduduk dilaporkan bocor dan dijual di *Raid Forums*, sebuah forum *hacker*, oleh akun bernama kotz. Data tersebut berisi nama lengkap, KTP, nomor telepon, email, NID, alamat dan gaji. Lebih dari itu, 20 juta data pribadi diantaranya, dilengkapi dengan foto pribadi penduduk. Kotz juga memberikan sampel data sebanyak satu juta secara cuma-cuma dengan memberikan tiga tautan link beserta kata sandi yang diperlukan.[5]

Dengan adanya berbagai kasus pencurian data pribadi yang terjadi, seharusnya Indonesia mengantisipasi hal tersebut tidak terjadi atau diminimalisir, dengan membuat perlindungan hukum yang jelas untuk segera keluar dari masalah tersebut, tetapi hal tersebut belum dilakukan oleh Indonesia.[6]

Penyalahgunaan data pribadi dapat sangat mengakibatkan kerugian yang sangat besar kepada korbannya baik secara materil maupun immateril. Apabila melihat definisi korban menurut Van Boven, korban kejahatan dan penyalahgunaan kekuasaan adalah orang yang secara individual maupun kelompok telah menderita kerugian, termasuk cedera fisik maupun mental, penderitaan emosional, kerugian ekonomi atau perampasan yang nyata terhadap hak-hak dasarnya, baik karena tindakan maupun kelalaian.[7]

Dari pendapat Van Boven tersebut dikaitkan dengan korban pencurian data pribadi sangat dimungkinkan terjadinya korban berantai, yaitu tidak hanya pengunjung situs atau sistem elektronik saja namun juga perusahaan pemilik sistem elekronik serta pihak perbankan yang menjadi mitra transaksi pembayaran tersebut juga berpotensi dicuri datanya hal ini mengartikan bahwa korban tidak lagi mengacu kepada perseorangan namun juga mencakup kelompok dan masyarakat.

Pengaturan perlindungan data pribadi belum diatur ketentuannya dalam hukum Indonesia secara khusus artinya peraturan tentang data pribadi masih bersifat parsial atau sektoral dan masih tumpang tindih dan termuat secara terpisah dibeberapa perundang-undangan dan hanya mencerminkan aspek perlindungan data pribadi secara umum. Khususnya pada peraturan dalam sistem elektronik seperti pada Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik hingga Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaran Sistem dan Transaksi

---

4 Nafi'ah, Rahmawati (2020). Pelanggaran Data Dan Pencurian Identitas Pada E-Commerce. *Jurnal CyberSecurity Dan Forensik Digital*, 3(1), 7-14. doi: https://doi.org/10.14421/csecurity.2020.3.1.1980

5 https://elsam.or.id/dugaan-kebocoran-279-juta-data-pribadi-penduduk-makin-pentingnya-akselerasi-pengesahan-ruu-pelindungan-data-pribadi/#:~:text=Pada%2012%20Mei%202021%2C%20279,dilengkapi%20dengan%20foto%20pribadi%20penduduk . Diakses pada tanggal 10 Juni 2021

6 Natamiharja, Rudi, h. 215.

7 Yulia, Rena. (2021). *Viktimologi; Perlindungan Hukum Terhadap Korban Kejahatan Edisi 2*. Yogyakarta: Graha Ilmu, h. 51.

Elektronik, Peraturan Menteri Komunikasi Dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

Terlihat bahwa peraturan yang masih bersifat parsial dan sektoral pengaturan pelindungan data pribadi yang saat ini berlaku di Indonesia dari berbagai legislasi sektoral sehingga belum adanya kesamaan rumusan definisi data pribadi dan jenis data pribadi yang memadai. Termasuk juga materinya yang belum selaras dengan prinsip-prinsip dalam perlindungan data secara internasional; ketidakjelasan dasar hukum pemrosesan data; ketidaksatuan pengaturan pemrosesan data; ketidakjelasan pengaturan perihal kewajiban pengendali dan pemroses data; kekosongan jaminan perlindungan hak-hak subjek data; dan ketiadaan lembaga yang secara khusus berfungsi sebagai regulator, pengendali dan pengawas, termasuk penyelesaian permasalahan hukum pemilik data pribadi.

Artikel ini tidak membahas semua lingkup kebijakan hukum pidana, namun lebih difokuskan pada kebijakan pada formulasi hukum pidana. Artikel ini akan menjelaskan kebijakan hukum pidana terhadap pengaturan pencurian data pribadi yang saat ini digunakan untuk menanggulangi tindak pidana pencurian data pribadi dilihat dari KUHP dan Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Kebijakan hukum pidana terhadap pengaturan pencurian data pribadi yang digunakan untuk menanggulangi tindak pidana pencurian data pribadi di masa yang akan datang dilihat dari pidana untuk itu penulis melihat dari Rancangan Undang-Undang Kitab Undang-Undang Hukum Pidana Tahun 2019 (RUU KUHP 2019) dan Rancangan Undang-Undang Perlindungan Data Pribadi Tahun 2020 (RUU PDP 2020).

Oleh karena itu, artikel ini membahas pertanyaan penelitian berikut; Bagaimana kebijakan hukum pidana terhadap pengaturan pencurian data pribadi sebagai penyalahgunaan teknologi komunikasi dan informasi dan bagaimana sebaiknya pengaturan kedepannya?

2. Pembahasan

2.1 Kebijakan Hukum Pidana terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi

Membicarakan pencurian data pribadi tidak dapat dilepaskan dari pembahasan akan hal perkembangan teknologi komunikasi dan informasi yang menyebabkan munculnya tindak pidana baru yang memiliki karakteristik yang berbeda dengan tindak pidana konvensional. Penyalahgunaan komputer sebagai salah satu dampak dari perkembangan teknologi tersebut itu tidak terlepas dari sifatnya yang khas sehingga membawa persoalan yang rumit dipecahkan berkenaan dengan masalah penanggulangannya (penyelidikan, penyidikan hingga dengan penuntutan).[8] Salah satu kejahatan yang ditimbulkan oleh perkembangan dan kemajuan teknologi informasi atau telekomunikasi adalah kejahatan yang berkaitan dengan aplikasi internet. Kejahatan ini dalam istilah asing sering disebut dengan *cybercrime.*

Menurut Kepolisian Inggris, *cybercrime* adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan/atau kriminal berteknologi tinggi dengan

[8] Makarim, Edmon. (2005). *Pengantar Hukum Telematika Suatu Kajian Kompilasi*. Jakarta: Raja Grafindo Persada, h. 42.

menyalahgunakan kemudahan teknologi digital.[9] Kualifikasi kejahatan dunia maya (*cybercrime*), sebagaimana dikutip Barda Nawawi Arief, adalah kualifikasi *Cybercrime* menurut *Convention on Cybercrime* 2001 di Budapest Hongaria, yaitu:[10]

1. *Illegal access*
2. *Illegal interception*
3. *Data interference*
4. *System interference*
5. *Misuse of Devices*
6. *Computer related Forgery*
7. *Computer related Fraud*
8. *Content-Related Offences*: *(child pornography).*
9. *Offences related to infringements of copyright and related rights.*

Istilah *cybercrime* saat ini merujuk pada suatu tindakan kejahatan yang berhubungan dengan dunia maya (*cyberspace*) dan tindakan kejahatan yang menggunakan komputer. Ada ahli yang menyamakan antara tindak kejahatan *cyber* (*cybercrime*) dengan tindak kejahatan komputer, dan ada ahli yang membedakan di antara keduanya. Meskipun belum ada kesepahaman mengenai definisi kejahatan Teknologi Informasi, namun ada kesamaan pengertian universal mengenai kejahatan komputer.[11] Hal diungkapkan serupa oleh Agus Raharjo bahwa istilah *cyber crime* sampai saat ini belum ada kesatuan pendapat bahkan tidak ada pengakuan internasional mengenai istilah baku, tetapi ada yang menyamakan istilah *cyber crime* dengan *computer crime*.[12]

Pencurian data pribadi telah berkorelasi dengan penyalahgunaan komputer, kejahatan komputer dan kejahatan terkait komputer karena Internet memfasilitasi mereka, itu disebut pencurian identitas *online*, misalnya adalah kasus peretas yang mencuri informasi pribadi seseorang melalui pelanggaran data online. Pencurian data pribadi sangat mempengaruhi konsumen dan organisasi.[13]

Pencurian data pribadi menurut peneliti termasuk kedalam *cybercrime* atau tindak pidana siber. Pencurian data pribadi ini sebenarnya bisa dikatakan dengan pelanggaran akses dengan membobol atau menembus suatu sistem elektronik untuk langsung meraih data pribadi seseorang yang terdapat didalam sistem tersebut yang kemudian data pribadi tersebut digunakan untuk kejahatan lainnya seperti penipuan.

---

[9] Wahid, Abdul & Labib, Mohammad. (2010). *Kejahatan Mayantara (Cyber Crime).* Jakarta:Refika Aditama, h. 40.

[10] Nawawi Arief, Barda. (2007). *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*. Jakarta: Kencana Prenada Media Group, h. 24.

[11] Arief Mansyur, Dikdik & Gultom, Elisatris. (2009). *Cyber Law: Aspek Hukum Teknologi Informasi*. Bandung: Refika Aditama, h. 8.

[12] Raharjo, Agus. (2002). *Cybercrime, Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi*. Bandung: Citra Aditya Bhakti, h. 227.

[13] Rahmawati Nafi'ah, *Op,Cit.*, h. 8.

Tindak pidana pencurian data melalui internet merupakan tindak pidana berupa perbuatan mengambil data milik orang lain yang tersimpan di dalam internet atau sistem elektronik tanpa seizin dari pemilik data tersebut.

Data theft atau mencuri data adalah kegiatan memperoleh data komputer secara tidak sah, baik untuk digunakan sendiri ataupun untuk diberikan kepada orang lain. *Identity theft* merupakan salah satu dari jenis kejahatan ini yang sering diikuti dengan kejahatan penipuan (*fraud*). Selain itu, kejahatan ini juga sering diikuti dengan kejahatan *data leakage*.[14]

Menurut Teguh Prasetyo, data pribadi adalah informasi tunggal ataupun sekumpulan informasi baik yang bersifat rahasia maupun yang tidak diberikan oleh pemilik data pribadi atau konsumen dan dihimpun ke dalam sistem elektronik yang diproses oleh penyelenggara sistem elektronik untuk dipergunakan sesuai dengan tujuan dan kegunaannya serta apabila disalahgunakan maka pemilik data pribadi atau konsumen dapat menyelesaikannya melalui media hukum administrasi negara dan atau atau media hukum perdata dan/atau media hukum pidana.[15]

Pengertian data pribadi jika mengacu pada Pasal 4 ayat (1) EU General Data Protection Regulation (GDPR) adalah Setiap informasi terkait seseorang (subjek data) yang dapat mengenali atau dapat dikenali; mengenali secara langsung atau tidak langsung seseorang tersebut, terutama dengan merujuk pada sebuah tanda pengenal seperti nama, nomor identitas, data lokasi, data pengenal daring atau pada satu faktor atau lebih tentang identitas fisik, psikologis, genetik, mental, ekonomi, atau sosial orang tersebut.

Pengertian kebijakan atau politik hukum pidana dapat dilihat dari politik hukum maupun dari politik kriminal. Menurut Sudarto, politik hukum adalah:[16]

a. Usaha untuk mewujudkan peraturan-peraturan yang baik sesuai dengan keadaan dan situasi pada suatu saat;

b. Kebijakan dari Negara melalui badan-badan yang berwenang untuk menetapkan peraturan-peraturan yang dikehendaki yang diperkirakan bisa digunakan untuk mengekspresikan apa yang terkandung dalam masyarakat dan untuk mencapai apa yang dicita-citakan.

Menurut Barda Nawawi Arief Kebijakan legislatif atau tahap formulasi merupakan kebijakan yang sangat penting dalam kebijakan hukum pidana. Kebijakan legislatif adalah suatu perencanaan atau program dari pembuat undang-undang mengenai apa yang akan dilakukan dalam menghadapi problema tertentu dan cara bagaimana melakukan atau melaksanakan sesuatu yang telah direncanakan atau diprogramkan.[17]

Hingga saat ini Indonesia tidak mempunyai pengaturant entang perlindungan data pribadi secara khusus, sejauh ini masih termuat secara terpisah di beberapa peraturan perundang-undangan, sehingga diperlukan adanya satu undang-undang yang mengatur secara komprehensif, jelas dan tegas terkait atas penyalahgunaan data

---

[14] Munir, Nudirman. (2017). *Pengantar Hukum Siber Indonesia.* Depok: Rajagrafindo Persada, h. 231.

[15] P.P.Karo Karo, Rizky, & Prasetyo, Teguh. (2020). *Pengaturan Perlindungan Data Pribadi Di Indonesia; Perspektif Teori Keadilan Bermartabat*. Bandung: Nusa Media, h. 50.

[16] Nawawi Arief, Barda. (2017). *Bunga Rampai Kebijakan Hukum Pidana:Perkembangan Penyusunan Konsep KUHP Baru*. Jakarta: Kencana Prenada Grup. h. 26.

[17] Nawawi Arief, Barda. (2010). *Kebijakan Legislatif Dalam Penanggulangan Kejahatan Dengan Pidana Penjara*. Yogyakarta: Genta Publishing, h. 59.

pribadi. Saat ini perlindungan data pribadi termuat di beberapa peraturan perundang-undangan, antara lain Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (UU ITE).

Kitab Undang-Undang Hukum Pidana (KUHP) masih dijadikan sebagai dasar hukum untuk menjaring tindak pidana siber, khususnya jenis tindak pidana siber yang memenuhi unsur-unsur dalam pasal-pasal KUHP. Ketika produk ini dinilai belum cukup memadai untuk menjaring beberapa jenis tindak pidana siber, maka disamping mencoba menggunakan dasar hukum di luar KUHP, juga menggunakan penafsiran hukum. Dasar hukum dalam KUHP yang digunakan oleh aparat penegak hukum dalam menanggulangi pencurian data, dalam hal ini diinterpretasikan sebagai tindak kejahatan konvensional pada umumnya yaitu pencurian,[18] sebagaimana diatur dalam Pasal 362 KUHP, yang menyebutkan bahwa:

"*Barang siapa mengambil barang sesuatu, yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk dimiliki secara melawan hukum, diancam karena pencurian, dengan pidana penjara paling lama lima tahun atau pidana denda paling banyak sembilan ratus rupiah*."

Jadi, kasus pengambilan data pribadi yang tersimpan dalam komputer dengan cara melawan hukum diinterpretasikan memenuhi salah satu unsur kejahatan pencurian. Ketentuan Pasal 362 KUHP mengatur tentang pencurian pada pokoknya dan ketentuan ini dapat diterapkan terhadap tindak pidana *carding*, yaitu pencurian data berupa *credit card number* yang didahului dengan *unauthorized access* atau pencurian password untuk memasuki sistem komputer orang lain atau pencurian informasi milik orang lain atau *unauthorised fund transfer*, dan lain sebagainya.

Permasalahan dalam KUHP ini adalah pencurian tradisional atau konvensional sebagaimana dimaksud dalam Pasal 362 KUHP secara konseptual menjadi berbeda dengan pencurian yang terjadi pada internet atau sistem elektronik. Dalam konsep pencurian tradisional barang yang diambil tidak lagi berada dalam penguasaan si pemilik dan beralih kepada pelaku pencurian, sedangkan pencurian data atau informasi pribadi di internet masih dalam penguasaan pemilik data, namun data atau informasi tersebut juga berada dalam penguasaan si pencuri. Dalam pembuktian unsur-unsur tindak pidana pencurian yaitu "mengambil" dan "barang" perlu dilakukan penafsiran ekstensif, karena kata "mengambil" dalam pencurian data pribadi tidak lagi dapat diartikan secara fisik memindahkan sesuatu dengan tangan tetapi termasuk memindahkan dengan menggunakan komputer atau teknologi informasi dan komunikasi lainnya. Di samping itu, data atau informasi pribadi yang dicuri tidak harus hilang sebagaimana pencurian secara tradisional atau fisik.

Kata "barang" juga harus ditafsirkan tidak hanya benda bergerak dan berwujud tetapi juga benda benda tidak bergerak dan tidak berwujud. Seperti pada putusan Hoge Raad mengenai *electriciteits arrest* dan putusan terhadap pelaku pembobolan Bank BNI cabang New York menjadi sumber hukum yang baik dalam penegakan hukum dan perkembangan hukum pidana. Hoge Raad telah menerima penafsiran kata "mengambil" termasuk didalamnya "mengalirkan aliran listrik dengan kawat dan memakainya" dan kata "barang" tidak hanya benda berwujud tetapi juga benda tidak

[18] Wahid, Abdul & Labib, Mohammad. *Op.Cit.*, h. 149

berwujud.[19] Oleh sebab itu, sebagai bukti pembaharuan terhadap hukum, Hoge Raad telah membuat keputusan dalam *arrest*nya bahwa benda yang tidak berwujud itu dapat dijadikan objek pencurian dan pelakunya dapat dipidana berdasarkan Pasal 362 Kitab Undang-Undang Hukum Pidana (KUHP). Putusan Hoge Raad itu dikenal dengan *Electriciteits-arrets* atau *arrest* listrik.

Kemudian terdapat beberapa tindak pidana pencurian data pribadi yang dijerat dengan Pasal 363 ayat (1) ke 5 KUHP, yaitu diancam dengan pidana penjara paling lama tujuh tahun terhadap pencurian yang masuk ke tempat melakukan kejahatan, atau untuk sampai pada barang yang diambil, dilakukan dengan merusak, memotong atau memanjat, atau dengan memakai anak kunci palsu, perintah palsu atau pakaian jabatan palsu.

Dalam Pasal 363 ada unsur pemberatan yaitu dengan ancaman hukuman lebih berat yaitu penjara selama-lamanya tujuh tahun. Unsur pemberat yang dicantumkan dalam Pasal 363 ayat (1) ke 5 KUHP yaitu jika pencurian itu dilakukan ke tempat kejahatan atau untuk mengambul barang yang akan dicuri itu, dengan jalan membongkar, memecah, memanjat atau memakai anak kunci palsu dan perintah palsu.

Penggunaan Pasal 363 ayat (1) ke 5 KUHP bagi kejahatan pencurian data dengan teknik *skimming*. *Skimming* adalah aktivitas yang berkaitan dengan upaya pelaku untuk mencuri data dari pita magnetik kartu ATM atau debit secara ilegal untuk memiliki kendali atas rekening korban. Perbuatan *skimming* termasuk perbuatan mengakses komputer dan atau sistem informasi milik orang lain dengan cara ilegal dengan maksud mengambil atau mencuri secara ilegal data-data pribadi yang terdapat dalam komputer dan atau sistem informasi tersebut dengan modusnya adalah menempelkan alat skimmer pada slot untuk memasukan kartu ATM pada mesin ATM.[20]

Sedangkan situasi saat ini, pencurian data pribadi dengan teknik *skimming* ini tidak lagi hanya menyerang ATM seseorang tetapi sudah menyerang sistem elektronik khususnya adalah *E-Commerce*, yang dimana *E-Commerce* memiliki banyak sekali data pribadi termasuk juga didalamnya terdapat data keuangan dalam sistem pembayarannya. *JS Sniffer* adalah termasuk dalam katagori *Web/Online Skimming* yaitu suatu bentuk kejahatan siber dimana sebuah *malware* diinjeksikan kepada sebuah *website* untuk menjalankan aktifitas intersep data perbankan atau transaksi keuangan yang dimasukkan oleh pengguna *website* tersebut. *Malware* ini dirancang untuk mencuri data pembayaran pelanggan dari toko online atau *E-Commerce*.[21]

Apabila ketentuan 362 dan 363 ayat (1) ke 5 KUHP diterapkan terhadap kejahatan pencurian data pribadi dan dikaitkan dengan pasal 1 KUHP maka terjadilah dua kemungkinan analogi atau penafsiran ekstensif. Hal ini tergantung pada hakim, apakah hakim akan menerapkan penafsiran ekstensif atau tidak, mengingat analogi tidak diperbolehkan, yang perlu diperhatikan adalah jika hakim dalam menafsirkan terlalu ekstensif maka dapat dipernyatakan apakah asas legalitas tidak dirusak oleh penerapan undang-undang didasarkan pada analogi terselubung. Dengan demikian

---

[19] Suseno, Sigid. (2012). *Yuridiksi Tindak Pidana Sibe.* Bandung*:* Refika Aditama, h. 183.

[20] Ekawati, Dian. (2018). Perlindungan Hukum Terhadap Nasabah Bank Yang Dirugikan Akibat Kejahatan Skimming Ditinjau Dari Perspektif Teknologi Informasi Dan Perbankan*, Unes Law Review*, 1(2), 157-171.

[21] https://forensics.uii.ac.id/js-sniffer-attack/ diakses pada tanggal 30 Maret 2021

menurut peneliti, dalam penerapan aturan terhadap delik sangat bergantung kepada hakim dalam memberikan pertimbangan. Dalam kaitannya dengan pencurian data pribadi, maka tergantung apakah hakim tersebut membedakan analogi dengan tafsiran ekstensif atau tidak, hal ini dapat menimbulkan ketidakpastian dan keadilan hukum.

Keseluruhan uraian kebijakan yang diprogramkan dari pembuat undang-undang mengenai apa yang akan dilakukan dalam menghadapi problema pencurian data pribadi dengan menggunakan pasal 362 dan 363 KUHP dapat disimpulkan apabila melihat unsurnya maka tidak lagi dapat dikenakan atau dapat menjerat pelaku dengan hukum pidana, karena pencurian data pribadi adalah kejahatan yang relatif baru. Oleh karena itu, penerapan Pasal-Pasal KUHP peneliti rasa sudah tidak relevan dalam penanggulangan tindak pidana teknologi informasi karena pasal tersebut berlaku untuk pencurian secara umum dan tidak khusus kepada tindak pidana pencurian data pribadi. Kebijakan pengaturan tindak pidana siber dalam KUHP dapat dilakukan dengan merumuskan tindak pidana baru apabila memang perumusan yang sudah ada tidak cukup memadai untuk mengatur tindak pidana siber atau dapat juga dengan merumuskan kembali (memodifikasi) perumusan tindak pidana yang sudah ada sehingga dapat mencakup berbagai perkembangan baru di bidang teknologi informasi.

Berbeda dengan KUHP, Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dibuat sebagai dalam rangka mengatur *cyber space* dan tindak pidana yang merupakan respon perkembangan teknologi informasi di bidang hukum. Respon ini didasarkan atas perkembangan suatu era hukum baru yang dikenal dengan hukum siber atau hukum telematika. Hukum siber (*cyberlaw*) secara internasional digunakan untuk istilah hukum yang terakit dengan pemanfaatan teknologi informasi dan komunikasi. Demikian pula dengan hukum telematika yang merupakan perwujudan dari konvergensi hukum telekomunikasi, hukum media dan hukum informatika.[22]

UU ITE ini adalah undang-undang pertama di bidang teknologi informasi dan transaksi elektronik sebagai produk legislasi yang sangat dibutuhkan dan menjadi pionir yang meletakan dasar pengetahuan dibidang pemanfaatan teknologi informasi dan transaksi elektronik. Kebijakan lahirnya UU ITE merupakan upaya penanggulangan kejahatan melalui hukum pidana itu sendiri. Kebijakan dibidang transaksi elektronik di Indonesia diatur dalam UU ITE yang bersifat khusus atau *lex specialist*. Kebijakan hukum mengenai perbuatan pencurian ataupun pembocoran data pribadi pada dasarnya dapat mengoptimalkan ketentuan Pasal 30 Jo. Pasal 46 dan pasal 32 Jo. Pasal 48 Pasal dalam UU ITE mengenai akses ilegal dan data inferensi.

Ketentuan pasal 30 Jo. Pasal 46 mengatur perbuatan akses ilegal atau memasuki komputer atau sistem elektronik secara tanpa hak. Dalam kententuan tersebut diatur 3 bentuk akses ilegal, yaitu:

1. Akses ilegal pada pokoknya yang diancam dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah) yang dirumuskan dalam pasal 30 ayat (1) Jo. Pasal 46 Ayat (1).
2. Akses ilegal dalam pengertian khusus yaitu akses ilegal dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik yang diancam

[22] Hardinanto, Aris. (2019). *Akses Ilegal Dalam Perspektif Hukum Pidana,* Malang*:* Setara Press, h. 63.

dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah) yang dirumuskan dalam pasal 30 ayat (2) Jo. Pasal 46 Ayat (2).

3. Akses ilegal dalam pengertian khusus yaitu akses ilegal dengan melanggar, menerobos, melampaui atau menjebol sistem pengamanan yang diancam dengan pidana pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah) yang dirumuskan dalam pasal 30 ayat (3) Jo. Pasal 46 Ayat (3)

Ketentuan pasal 32 Jo. Pasal 48 mengatur tentang perbuatan data inferensi yang terdiri dari 3 ayat mengatur tentang tiga perbuatan, yaitu:

1. Mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik yang diancam dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah) yang dirumuskan dalam pasal 32 ayat (1) Jo. Pasal 48 Ayat (1)
2. Memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak yang diancam dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah) yang dirumuskan dalam pasal 32 ayat (2) Jo. Pasal 48 Ayat (2).
4. Mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya yang diancam dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah) yang dirumuskan dalam pasal 32 ayat (3) Jo. Pasal 48 Ayat (3).

Permasalahan dalam UU ITE ini adalah penempatan unsur sifat melawan hukumnya adalah pada Pasal 30 Jo. Pasal 46 mengakses dengan cara apapun, tetapi permasalahannya adalah tidak ditentukan oleh perumus undang-undang apa yang membedakan antara akses tanpa hak dengan berhak terhadap komputer dan/atau sistem elektronik. Konsekuensi dari perumusan tersebut adalah jika seseorang menggunakan komputer dan/atau sistem elektronik milik orang lain dapat dipidana, lain halnya jika ditambahkan unsur "otorisasi", dengan kata lain seseorang dapat dipidana jika melakukan akses ilegal dengan sengaja dan tanpa hak terhadap komputer dan/atau sistem elektronik milik orang lain "tanpa persetujuannya" atau "tanpa kewenangannya".[23]

Unsur persetujuan ini penting karena dalam hal pembuktiaan. Penuntut umum tidak hanya harus membuktikan unsur akses komputer dan/atau sistem elektronik milik orang lain saja, tetapi harus juga membuktikan bahwa akses terhadap komputer dan/atau sistem elektronik tersebut tanpa persetujuan pemilik.

---

[23] Hardinanto, Aris. *Ibid,* h. 72.

Meskipun UU ITE ini sering digunakan untuk menjerat pelaku tindak pidana siber terlebih khusus menjerat pelaku penyalahgunaan data pribadi dalam sistem elektornik namun dalam kenyataannya pengaturan terkait dengan data pribadi yang ada dalam UU ITE tersebut masihlah belum komprehensif mengatur data pribadi pemilik data, seperti data yang harus dilindungi, ruang lingkup terkait data pribadi, perbedaan data pribadi data sensitif dan umum.

Kemudian dalam pelaksanaaannya tindak pidana siber sering kali dilakukan tidak hanya dengan satu jenis tindak pidana tetapi dilakukan dengan dua langkah atau lebih jenis tindak pidana. Dalam tindak pidana pencurian data pribadi pelaku tindak pidana terlebih dahulu melakukan akses ilegal terhadap sistem elektronik orang lain dan kemudian melakukan pencurian atau melakukan *identity theft* seseorang untuk itu dikenakan pasal 30 Jo. Pasal 46 UU ITE, dengan data yang didapatkan demikian pelaku dapat melakukan kejahatan lainnya.

Karakteristik dari tindak pidana pencurian data pribadi seharusnya menjadi dasar pertimbangan perumusan tindak pidana siber terutama berkaitan dengan jenis tindak pidana, delik formil atau materil dan penerapan ajaran *concursus* atau perbarengan. Apakah akan diberlakukan perbarengan realis atau perbuatan berlanjut. Pasal 362 KUHP misalnya yang mengatur pencurian dapat menjadi bagian dari tindak pidana pencurian data pribadi yang merugikan orang lain begitupun dengan Pasal 30 Jo. Pasal 46 UU ITE. Pencurian data pribadi tanpa ditindaklanjuti dengan tindakan melawan hukum lainnya sesungguhnya belum menimbulkan bahaya atau kerugian pada pihak lain sehingga tidak perlu dipidana.

Selain itu, salah satu alasan yang sering dikemukakan menjadi penyebab tidak tuntasnya kasus-kasus kebocoran data pribadi di Indonesia adalah tidak adanya pengaturan yang secara komprehensif mengatur perlindungan data pribadi. Ini karena tidak ada harmonisasi pengaturan diantara berbagai lembaga pemerintahan, sehingga menimbulkan penegak hukum dalam menegakkan hukum yang berwenang sering ragu-ragu dalam menerapkan sanksi terhadap pelanggaran aturan pribadi karena belum adanya mekanisme dan tanggung jawab dari pengelola data pribadi yang jelas. Hal ini menimbulkan ketidakpastian hukum dan kesulitan bagi pihak yang dirugikan untuk mengajukan tuntutan.

Sampai saat ini hukum positif di Indonesia belum mengatur perbuatan mendapatkan data identitas diri menggunakan teknik *phising* atau pencurian data pribadi baik dalam KUHP Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik sehingga terjadi kekosongan hukum yang memungkinkan menimbulkan kekacauan di masyarakat. Oleh karena itu, diperlukan pembaharuan pengaturan hukum di masa yang akan datang untuk menyelesaikan permasalahan yang dihadapi masyarakat digital atau mayantara saat ini.[24]

Dalam kenyataannya, peneliti melihat sebuah fakta bahwa meskipun terdapat ada peraturan perundang-undangan yang mengatur secara eksplisit mengenai tindak pidana siber, pelaku kejahatan tindak pidana siber masih sulit untuk dijerat. Hal ini dikarenakan sifat dari kejahatan tersebut yang bersifat transnasional dan memiliki

[24] Arya Utamayasa, I. G., Surya Dharma Jaya, I. D., & Dike Widhiyaastuti, I. G. A. (2016) Kriminalisasi Terhadap Perbuatan Memperoleh Data Identitas Diri Dengan Menggunakan Teknik Phising. *Kertha Wicara: Journal Ilmu Hukum*, 5(1), 1-5. doi: 10.24843

karakter-karakter tersendiri yang rumit. Sehingga diperlukan pembaharuan hukum di masa yang akan datang untuk menyelesaikan permasalahan dunia siber terutama terhadap kejahatan yang menyangkut ketidakamanan data pribadi yang disimpan dalam sistem elektronik saat ini.

2.2. Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi Di Masa Yang Akan Datang

Pengaturan perbuatan pencurian data pribadi perumusan tindak pidana pencurian data pribadi sebagai penyalahgunaan teknologi komunikasi dan informasi di masa yang akan datang dapat ditemukan dalam RUU KUHP 2019 yaitu pada Pasal 482 dan Pasal 483. Pasal 482 menentukan bahwa:

"Setiap Orang yang mengambil suatu Barang yang sebagian atau seluruhnya milik orang lain, dengan maksud untuk dimiliki secara melawan hukum dipidana karena pencurian, dengan pidana penjara paling lama 5 (lima) tahun atau pidana denda paling banyak kategori V."

Aturan ini memang tidak mengatur secara spesifik tentang pencurian data pribadi namun apabila unsur-unsur diidentifikasikan maka tindak pidana pencurian adalah mengambil suatu barang, sebagian atau seluruhnya milik orang lain, dengan maksud untuk memiliki atau menguasai, melawan hukum. Menurut penjelasan Pasal 482, yang dimaksud dengan "mengambil" dalam ketentuan ini adalah tidak hanya diartikan secara fisik, tetapi juga meliputi bentuk-bentuk perbuatan "mengambil" lainnya secara fungsional (non-fisik) mengarah pada maksud "memiliki barang orang lain secara melawan hukum". Misalnya pencurian uang dengan cara mentransfer, atau menggunakan tenaga listrik tanpa hak. Kemudian yang dimaksud "memiliki" adalah mempunyai hak atas barang tersebut.

Berdasarkan penjelasan tersebut, pembuktian pada unsur-unsur tindak pidana pencurian data pribadi dapat terpenuhi karena kata "mengambil" tidak perlu lagi secara fisik berpindah tangan, artinya pencurian data atau informasi pribadi di internet walaupun masih dalam penguasaan pemilik data dan data atau informasi tersebut juga berada dalam penguasaan si pencuri tetap dikatakan perbuatan mengambil, selain itu, kata "barang" sesuai dengan Pasal 152 pembatasan benda tidak lagi hanya untuk yang berwujud tetapi juga digunakan untuk benda yang tidak berwujud seperti data. Dan dalam sanksi yang akan dihadapi oleh pelaku tindakan tersebut yaitu akan mendapatkan sanksi pidana penjara paling lama 5 tahun atau pidana denda kategori V. Pidana denda kategori V adalah sebesar Rp500.000.000,00 (lima ratus juta rupiah).

Pada Pasal 483 Ayat (1) huruf f, menentukan bahwa:

"*Pencurian dengan cara merusak, membongkar, memotong, memecah, memanjat, memakai Anak Kunci Palsu, menggunakan perintah palsu, atau memakai pakaian jabatan palsu, untuk Masuk ke tempat melakukan Tindak Pidana atau sampai pada barang yang diambil.*"

Pada Pasal 483 Ayat (1) huruf f disebutkan sebelumnya anak kunci palsu pada pengertian istilah yang terdapat pada Bab V RUU KUHP 2019, anak kunci palsu adalah anak kunci duplikat atau alat yang digunakan untuk membuka kunci seperti kunci masuk komputer yang dapat digunakan untuk membuka sistem pengamanan suatu sistem elektronik. Dan terdapat unsur delik berupa kata "masuk" yang dalam

pengertian istilah Pasal 169 ditetapkan bahwa masuk adalah termasuk mengakses komputer atau masuk ke dalam sistem komputer, ini artinya Pasal 483 Ayat (1) huruf f RUU KUHP juga dapat menjerat pelaku pencurian data pribadi dalam sistem elektronik karena pelaku pencurian data dalam sistem elektronik langkah awalnya pasti dilakukan dengan anak kunci palsu berupa *malware* untuk menerobos masuk kedalam sistem pengamanan untuk mengambil data pribadi pemilik atau penggunya suatu sistem elektronik tersebut.

Delik pencurian dalam Pasal 482 dan Pasal 483 Ayat (1) huruf f RUU KUHP 2019 ini dapat digunakan untuk menjangkau pencurian data pribadi, karena dalam rumusan tindak pidana dirumuskan bahwa barang-barang pencurian tersebut dapat berupa benda tidak berwujud berupa data dalam sistem elektronik atau komputer, mengambil tidak lagi harus berpindah tangan dalam arti menjadi dalam penguasaan pencuri tetapi bisa juga masih didalam penguasaan pemilik, anak kunci palsu diartikan sebagai kunci yang lain yang digunakan untuk membuka atau kunci masuk kedalam suatu sistem elektronik, dan masuk diartikan sebagai mengakses komputer atau masuk ke dalam sistem komputer.

Hanya saja RUU KUHP 2019 belum mencantumkan definisi terkait data pribadi atau informasi pribadi, sehingga menimbulkan belum adanya batasan terkait data pribadi. Pada pasal 159 RUU KUHP 2019 dijelaskan bahwa data termasuk bagian dari pengertian barang, namun belum ada pengertian data pribadi, perbedaan data umum dan data sensitif. Sehingga belum ada pengaturan tentang pencurian data pribadi dan bagaimana cara pembuktian apabila terindikasi adanya pencurian data pribadi.

Pemerintah saat ini telah merancang Undang-Undang tentang Perlindungan Data Pribadi per Tahun 2020 (RUU PDP). Terdapat dua norma dalam RUU PDP terkait pencurian data pribadi yaitu norma tentang larangan memalsukan data pribadi dengan maksud menguntungkan diri sendiri atau orang lain atau yang mengakibatkan kerugian bagi orang lain dan norma yang kedua adalah norma larangan untuk menjual atau membeli data pribadi.

Berkaitan dengan penelitian ini, peneliti tidak dapat menemukan pasal yang secara spesifik mengatur pencurian data pribadi namun terdapat pasal 61 dan 64 yang dapat digunakan berkaitan dengan penyalahgunaan data pribadi karena dalam pelaksanaaannya tindak pidana siber sering kali dilakukan tidak hanya dengan satu jenis tindak pidana tetapi dilakukan dengan dua langkah atau lebih jenis tindak pidana. Alasan pasal-pasal ini dapat digunakan untuk menjerat pelaku pencurian data pribadi adalah karena dilihat dari berbagai resiko-resiko kejahatan lainnya, antara lain:[25]

1. Informasi atau data pribadi yang dicuri lalu dijual ke *dark web*, *dark web* adalah bagian tersembunyi dari internet yang hanya bisa diakses menggunakan aplikasi khusus.
2. Modus penipuan dengan iming-iming hadiah atau dapat diganggu oleh telemarketer yang mencoba memasarkan usaha mereka

Dalam ketentuan RUU PDP masih terdapat banyak kekurangan jika dibandingkan dengan standar perlindungan data pribadi internasional. Seperti belum adanya kejelasan dalam pembagian ruang lingkup hukum di antara perorangan dan lembaga, hal ini berpotensi mengakibatkan penetapan kewajiban perlindungan data pribadi

[25] P.P.Karo Karo, Rizky, & Prasetyo, Teguh. *Op.Cit.*, h. 27.

yang tidak sesuai dengan kapasitas pihak yang berbeda-beda. Hal ini dapat membuat penegak hukum menafsirkan bahwa seorang individu memiliki kewajiban yang sama dengan suatu lembaga yang mengendalikan memproses data. RUU PDP harus memberikan kejelasan yang lebih mendetail untuk membedakan kegiatan pengolahan data rumah tangga dan aktivitas pemrosesan data komersial. Kemudian ketidakjelasan dasar hukum RUU PDP yang belum menawarkan kejelasan tentang keabsahan dan dasar hukum pemrosesan data. RUU PDP mengatur bahwa pengendali data bisa memproses data untuk memenuhi kewajiban hukum untuk kepentingan publik. Tetapi, tidak ada penjelasan lebih lanjut mengenai "kepentingan publik". Ada potensi pengendali data bisa menafsirkan sendiri apa yang dimaksud dengan "kepentingan publik" dan memproses data sesuai dengan kepentingan pengendali data belaka.

Melihat dari rumusan RUU PDP pada pasal yang memuat ketentuan pidana yaitu pasal 61 sampai dengan pasal 68 dirumuskan "dengan sengaja" artinya RUU PDP ini hanya memasukkan unsur kesengajaan. Dalam pertanggungjawaban pidana dengan mendasarkan pada asas kesalahan, kesalahan terdapat dua bentuk yaitu kesengajaan (*Dolus/Opzet*) dan kealpaan (*Culpa/Alpa*). Sesuai yang dikemukakan oleh Ridwan selaku Dosen bidang pidana FH UNTIRTA sebaiknya RUU PDP pada ketentuan pidananya mencantumkan unsur kealpaan, untuk menghindari kerugian karena kelalaian pihak pengelola data dalam menjaga dan mengelola kerahasiaan, keutuhan dan ketersediaan data komputer dan sistem komputer.[26]

Kelemahan berikutnya adalah penempatan warga negara di posisi yang lemah, RUU PDP mengatur tentang hak-hak pemilik data seperti hak untuk diberitahukan, hak untuk diperbaiki, hak untuk pemulihan, dan hak-hak lainnya. Namun, RUU PDP menuntut pemilik data yang harus aktif menuntut hak-hak mereka sebagai pemilik data kepada pengendali data bukan membebankan pertanggungjawaban terkait hak-hak tersebut kepada pengendali data sedari awal. Ini membuka kemungkinan pihak pemilik data di Indonesia baru mengetahui hak-hak mereka sebagai pemilik data sesudah data mereka diproses.

Melihat Di Singapura, terdapat perkembangan yang menarik terhadap pengaturan kejahatan teknologi informasi terkhusus pada pencurian data pribadi atau identitas (*identity theft*) yaitu terdapat pada *Penal Code Chapter 224* dan terkait perlindungan data pribadi diatur dalam *Personal Data Protection Act 2012* (PDPA 2012) yang mulai berlaku secara bertahap dimulai dengan ketentuan terkait dengan pembentukan PDPC (*Personal Data Protection Commission*) pada 2 Januari 2013 serta *Public Sector Governance Act 2018* (PSGA). Maka perlu adanya pengaturan pencurian data pribadi dalam hukum positif di Indonesia dengan metode perbandingan yaitu membandingkan dengan negara singapura melihat singapura telah mengatur tindak pidana pencurian identitas sebaiknya Badan Legislatif agar segera melakukan pengkajian ulang khususnya di bidang teknologi dan informatika dalam RUU KUHP 2019 dan perlindungan data pribadi dalam RUU PDP 2020 sehingga ketika disahkan di masa yang akan datang tidak ada lagi kekosongan norma terhadap perbuatan mendapatkan data identitas diri atau pencurian data pribadi.

---

[26] Ridwan. "*Perlindungan Hukum Pidana Terhadap Kepentingan Hukum",* Dalam Diskusi Publik Urgensi Pembentukan Undang-Undang Tentang Perlindungan Data Pribadi, Dilaksanakan Di UNTIRTA, 22 Oktober 2020.

3. Kesimpulan

Berdasarkan uraian tersebut dapat disimpulkan bahwa Kebijakan hukum pidana terhadap pengaturan pencurian data pribadi sebagai penyalahgunaan teknologi komunikasi dan informasi pengaturan tentang kejahatan pencurian data pribadi tidak diatur dalam berbagai hukum positif di Indonesia, baik dalam undang-undang yang dan mengatur tentang pencurian biasa dalam KUHP dan *cyber law* seperti UU ITE. Dengan belum diaturnya kejelasan tentang penyalahgunaan terhdap data pribadi maka hal tersebut akan berpengaruh kepada kebijakan aplikasi dan eksekusinya. Pengaturan perbuatan pencurian data pribadi Perumusan tindak pidana pencurian data pribadi sebagai penyalahgunaan teknologi komunikasi dan informasi di masa yang akan datang dapat ditemukan dalam RUU KUHP 2019 dan RUU PDP 2020. Namun perlu dilakukan pengkajian ulang dalam RUU KUHP dan RUU PDP dikarenakan masih tidak ada pengaturan tentang pencurian data identitas diri agar kedepannya tidak ada lagi kekosongan hukum. Badan legislatif Indonesia harus melakukan perbandingan kepada Negara Singapura Serikat dimana Negara Singapura mengatahui potensi-potensi yang timbul akibat dari perbuatan pencurian data pribadi itu sendiri.

Referensi

Buku:

Mansyur, D.A. & Gultom, E. (2009). *Cyber Law: Aspek Hukum Teknologi Informasi*. Bandung: Refika Aditama.

Hardinanto, A. (2019). *Akses Ilegal Dalam Perspektif Hukum Pidana*, Malang: Setara Press.

Makarim, E. (2005). *Pengantar Hukum Telematika Suatu Kajian Kompilasi*. Jakarta: Raja Grafindo Persada.

Munir, N. (2017). *Pengantar Hukum Siber Indonesia*. Depok: Rajagrafindo Persada.

Arief, BN. (2017). *Bunga Rampai Kebijakan Hukum Pidana:Perkembangan Penyusunan Konsep KUHP Baru*. Jakarta: Kencana Prenada Grup

Arief, BN. (2010). *Kebijakan Legislatif Dalam Penanggulangan Kejahatan Dengan Pidana Penjara*. Yogyakarta: Genta Publishing

Arief, BN. (2007). *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*. Jakarta: Kencana Prenada Media Group.

P.P.Karo Karo, Rizky, & Prasetyo, Teguh. (2020). *Pengaturan Perlindungan Data Pribadi Di Indonesia; Perspektif Teori Keadilan Bermartabat*. Bandung: Nusa Media.

Raharjo, A. (2002). *Cybercrime, Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi*. Bandung: Citra Aditya Bhakti.

Suseno, S. (2012). *Yuridiksi Tindak Pidana Siber*. Bandung: Refika Aditama

Yulia, R. (2021). *Viktimologi; Perlindungan Hukum Terhadap Korban Kejahatan Edisi 2*. Yogyakarta: Graha Ilmu.

Wahid, A. & Labib, M. (2010). *Kejahatan Mayantara (Cyber Crime).* Jakarta: Refika Aditama.

Jurnal Ilmiah:

Arya Utamayasa, I. G., Surya Dharma Jaya, I. D., & Dike Widhiyaastuti, I. G. A. (2016) Kriminalisasi Terhadap Perbuatan Memperoleh Data Identitas Diri Dengan Menggunakan Teknik Phising. *Kertha Wicara: Journal Ilmu Hukum*, 5(1), 1-5. doi: 10.24843

Ekawati, D. (2018). Perlindungan Hukum Terhadap Nasabah Bank Yang Dirugikan Akibat Kejahatan Skimming Ditinjau Dari Perspektif Teknologi Informasi Dan Perbankan, *Unes Law Review*, 1(2), 157-171.

Nafi'ah, R. (2020). Pelanggaran Data Dan Pencurian Identitas Pada E-Commerce. *Jurnal CyberSecurity Dan Forensik Digital*, 3(1), 7-14. doi: https://doi.org/10.14421/csecurity.2020.3.1.1980

Natamiharja, R. (2018). A Case Study On Facebook Data Theft In Indonesia. Flat Justisia, 12(3), 206-223. doi: https://doi.org/10.25041/fiatjustisia.v12no3.1312

Peraturan Perundang-Undangan

Kitab Undang-Undang Hukum Pidana (KUHP)

Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

Rancangan Undang-Undang Kitab Undang-Undang Hukum Pidana Tahun 2019 (RUU KUHP 2019)

Rancangan Undang-Undang Perlindungan Data Pribadi Tahun 2020 (RUU PDP 2020).

Internet:

Ridwan. "Perlindungan Hukum Pidana Terhadap Kepentingan Hukum", Sumber [Dalam Diskusi Publik Urgensi Pembentukan Undang-Undang Tentang Perlindungan Data Pribadi, Dilaksanakan Di UNTIRTA] pada tanggal 22 Oktober 2020.

"Rekap Serangan Siber (Januari – April 2020)", Sumber [Online]: https://bssn.go.id/rekap-serangan-siber-januari-april-2020/ , diakses pada tanggal 18 Maret 2021.

"Dugaan Kebocoran 279 Juta Data Pribadi Penduduk: Makin Pentingnya Akselerasi Pengesahan RUU Pelindungan Data Pribadi", Sumber [Online]: https://elsam.or.id/dugaan-kebocoran-279-juta-data-pribadi-penduduk-makin-pentingnya-akselerasi-pengesahan-ruu-pelindungan-data-pribadi/, diakses pada tanggal 10 Juni 2021.

"JS Sniffer Attack", Sumber [Online]: https://forensics.uii.ac.id/js-sniffer-attack/, diakses pada tanggal 30 Maret 2021.