



PERLINDUNGAN TERHADAP KORBAN PENCURIAN DATA PRIBADI MELALUI MEDIA DIGITAL

Muhammad Triadi

Fakultas Hukum Universitas Malikussaleh
muhammad.180510295@mhs.unimal.ac.id

Sumiadi, S.H., M.Hum

Fakultas Hukum Universitas Malikussaleh

Dr. Yusrizal, S.H., M.H

Fakultas Hukum Universitas Malikussaleh

Abstract

Theft of personal data is a crime that results in many victims experiencing material and psychological losses. However, legal protection for victims has not been clearly regulated in the current law regarding legal protection for victims of personal data theft. This study discusses two important issues, namely how legal protection for victims of personal data theft through digital media and how legal protection policies for victims of personal data theft through digital media. This study uses a normative juridical research method with a statutory and conceptual approach. The nature of this research is descriptive analytical. The collection of legal materials is carried out by literature study and data analysis techniques are carried out qualitatively. The policy of protection for victims of personal data theft in terms of the Personal Data Protection Bill (RUU PDP



DOI: [10.29103/REUSAM.VXII1.10178](https://doi.org/10.29103/REUSAM.VXII1.10178)

already contains protection for victims of personal data theft regarding the weaknesses in existing regulations.

Keywords: Protection, Law, Victims, Theft, Personal Data

1. PENDAHULUAN

Saat ini teknologi informasi sangat berkembang pesat tidak hanya dibidang internet tetapi juga dibidang komputer. Dengan berkembangnya teknologi informasi memberikan dampak yang positif dalam kehidupan manusia, yaitu memudahkan manusia saat ini dalam mengakses apapun itu melalui elektronik. Teknologi informasi memberikan beberapa hal yang bermanfaat yakni dibidang bisnis, telekomunikasi, pendidikan, dan juga peradaban pada masyarakat, selain itu dengan meningkatnya teknologi informasi dapat memberikan hal negatif juga yaitu sarana efektif perbuatan melawan hukum yaitu tindak pidana kejahatan. banyak bentuk kejahatan yang dilakukan dengan teknologi informasi sehingga dikenal dengan kata istilahnya yaitu *cybercrime*. Beraneka macam kejahatan yang dapat dilakukan melalui teknologi saat ini seperti kejahatan *hacking*, kejahatan *phising*, kejahatan *carding*, kejahatan *Ransomware*, penipuan online, dan masih banyak kejahatan lainnya.

Salah satu dampak negatif dari kemajuan teknologi adalah kejahatan pencurian data pribadi. Pencurian data pribadi merupakan kejahatan yang sangat berbahaya, dimana kejahatan ini merupakan awal dari kejahatan lainnya di dalam dunia *cyber*. Kejahatan *cyber* juga merupakan sebuah kejahatan yang susah diungkap dikarenakan media digital bersifat global atau luas. Sehingga membuat banyak korban susah untuk melaporkan dan juga mendapat hak-hak nya kembali, kerugian yang didapatkan oleh korban tidak hanya berbentuk uang atau kekayaan saja tetapi juga pelanggaran privasi.

Pengaturan data pribadi dalam sistem perundang-undangan di Indonesia diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Menteri Komunikasi dan Informatika Nomor 20 tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (PDPSE). Dan Undang-Undang 31 Tahun 2014 tentang Perlindungan Saksi dan Korban

Dengan adanya Undang-Undang 31 Tahun 2014 tentang Perlindungan Saksi dan Korban memiliki manfaat bagi saksi dan korban, akan tetapi dalam Undang-Undang 31 Tahun 2014 tentang Perlindungan Saksi dan Korban tidak menjelaskan secara spesifik atau menjamin terhadap korban pencurian data pribadi, mengingat juga Lembaga Perlindungan Saksi dan Korban (LPSK) juga hanya berada dikota-kota besar sehingga membuat masyarakat yang berada didaerah terpencil pun tidak dapat melaporkan atau mengklaim ganti kerugian, dikarenakan tidak adanya LPSK didaerah-daerah terpencil.

Dalam pasal 26 ayat 2 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 memang sudah mengatur tentang ganti kerugian, tetapi itu hanya berlaku untuk pelaku yang telah ditemukan, namun bagaimana apabila pelakunya pun korban tidak ketahui. Serta dalam Undang-Undang Nomor 31 Tahun 2014 tentang Perlindungan Saksi dan Korban pun belum mengatur atau menjelaskan secara spesifik bahwa korban dari pencurian data berhak mendapatkan hak



ganti kerugian, oleh karena itu perlu kita ketahui sudah sejauh mana korban pencurian data pribadi telah memperoleh perlindungan hukum yang seharusnya didapatkan. Adapun permasalahan dalam penelitian ini yakni Bagaimanakah perlindungan hukum terhadap korban pencurian data pribadi melalui media digital, Bagaimanakah kebijakan perlindungan hukum terhadap korban pencurian data pribadi melalui media digital dilihat dari RUU PDP.

2. METODE PENELITIAN

Jenis penelitian yang digunakan oleh penulis adalah penelitian normatif atau biasa disebut dengan penelitian doktrin. Penelitian yuridis normatif ini yaitu sebuah metode penelitian hukum yang dilakukan dengan menggunakan cara meneliti data kepustakaan, Penelitian yuridis normatif ini juga dilakukan dengan cara mengkaji sebuah norma dan peraturan perundang-undangan, dan pendapat para ahli hukum. Penelitian ini menggunakan pendekatan undang-undang (*statute Approach*). Dan pendekatan konseptual (*conceptual approach*). Sifat Pada Penelitian ini bersifat deskriptif analitis, Deskriptif analitis adalah sebuah jenis penelitian yang menggambarkan peraturan perundang-undangan yang berlaku serta dikaitkan dengan teori-teori hukum dan praktek pelaksanaan hukum yang menyangkut tentang permasalahan dalam penelitian ini. Penelitian ini menggunakan sumber data kepustakaan, yakni data yang penulis peroleh dari berbagai sumber literatur yang berhubungan dengan topik/permasalahan yang diangkat dengan perundang-undangan, buku, media cetak, jurnal serta berbagai pendapat para pakar hukum, dan dibedakan menjadi 3 (tiga), yaitu Bahan hukum primer yang terdiri dari Peraturan Perundang-Undangan yang berkaitan dengan permasalahan yang dibahas, Bahan hukum sekunder merupakan bahan yang memberikan penjelelasan bahan hukum primer seperti buku-buku, kamus-kamus hukum, dan jurnal-jurnal hukum, dan Bahan hukum tersier merupakan bahan hukum yang memberikan penjelasan bahan hukum primer dan bahan hukum sekunder seperti karya ilmiah, internet, dan lain-lain. Analisis data penelitian ini dilakukan secara kualitatif yakni dengan mengumpulkan bahan hukum primer, sekunder, dan bahan tersier yang relevan dengan permasalahan yang sedang diteliti. Setelah itu melakukan pemilahan terhadap bahan-bahan hukum yang relevan tersebut agar sesuai dengan permasalahan yang sedang di bahas oleh penulis.

3. HASIL PENELITIAN DAN PEMBAHASAN

A. Perlindungan Hukum Terhadap Korban Pencurian Data Pribadi Melalui Media Digital

1) Perlindungan Hukum Terhadap Korban Pencurian Data Pribadi Melalui Media Digital Menurut Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Perlindungan data pribadi merupakan salah satu dari hak pribadi dengan kata lain (*privacy rights*), adapun hak pribadi mengandung pengertian yaitu:

1. Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan
2. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan orang lain tanpa tindakan dimata-matai
3. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan Pribadi.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik merupakan Undang-Undang yang mengatur mengenai segala kejahatan yang dilakukan melalui digital/internet. Sayangnya untuk pengaturan mengenai pencurian data pribadi hanya sedikit diatur dalam Undang-Undang Nomor 19 Tahun 2016 (UU ITE) ini, dimana pengaturannya tersebut terdapat pada Pasal 26 Ayat 1 yang isinya: "Kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan, setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan."

Adapun untuk Pasal 26 Ayat 2 Undang-Undang Nomor 19 Tahun 2016 (UU ITE) "Setiap orang yang dilanggar haknya sebagaimana di maksud pada Ayat 1 dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini." Dalam Pasal 46 Ayat 2 dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) juga mengatur pelaku yang melanggar pencurian data, yang isinya "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 Ayat 2 dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah)." Melihat pengaturan pada Undang-Undang Nomor 19 Tahun 2016 (UU ITE) bahwa secara tegas UU ITE ini melarang mengakses data pribadi orang lain tanpa sepengetahuan sipemilik data, dikarenakan data pribadi adalah suatu privasi yang harus dijaga dengan baik, sayangnya pada UU ITE ini tidak adanya perlindungan hukum yang harus ditanggung oleh pihak penyelenggara yang tidak dapat melindungi data pribadi korban.

Berdasarkan uraian sebelumnya bahwa Undang-Undang No. 19 tahun 2016 (UU ITE) belum dapat memenuhi perlindungan hak bagi parakorban pencurian data pribadi, yang mengakibatkan kerugian signifikan bagi para korban yang seyogyanya di cegah dan ditanggulangi dengan di formulaskannya norma yang dapat menghukum pelaku tindak pidana sampai pada level pemidanaan (penjara) sesuai dengan kesalahannya dan menetapkan sanksinya dengan tegas sebagaimana yang dikehendaki oleh norma hukum pidana, serta dikarenakan kasus kasus pencurian data pribadi ini korban banyak mendapat kerugian materiil, sehingga perlunya formulasi sanksi pun harus sampai pada tahap korban mendapatkan ganti kerugian seperti yang dialaminya dengan tahapan tahapan semudah mungkin.



2) Perlindungan Hukum Terhadap Korban Pencurian Data Pribadi Melalui Media Digital Menurut Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik

Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (PDPSE) merupakan pengaturan yang bisa dikatakan cukup jelas dalam melindungi data pribadi dimedia digital. Inilah beberapa Pasal yang bisa dikatakan aspek penting dalam perlindungan data pribadi yaitu :

- a) Pasal 2 ayat 2 Mengenai Perlindungan Data Pribadi yaitu yang berisikan 10 Poin yaitu:
 1. Penghormatan terhadap Data Pribadi sebagai privasi
 2. Data Pribadi bersifat rahasia sesuai Persetujuan dan/atau berdasarkan ketentuan peraturan perundang-undangan
 3. Berdasarkan Persetujuan
 4. Relevansi dengan tujuan perolehan, pengumpulan, pengolahan, penganalisan, penyimpanan, penampilan, pengumuman, pengiriman, dan penyebarluasan
 5. Kelaikan Sistem Elektronik yang digunakan
 6. Iktikad baik untuk segera memberitahukan secara tertulis kepada Pemilik Data Pribadi atas setiap kegagalan perlindungan Data Pribadi
 7. Ketersediaan aturan internal pengelolaan perlindungan Data Pribadi
 8. Tanggung jawab atas Data Pribadi yang berada dalam penguasaan Pengguna
 9. Kemudahan akses dan koreksi terhadap Data Pribadi oleh Pemilik Data Pribadi
 10. Keutuhan, akurasi, dan keabsahan serta kemutakhiran Data Pribadi.
- b) Pasal 26 Mengenai Hak Pemilik Data Pribadi, bahwa pemilik data berhak:
 1. Atas kerahasiaan Data Pribadinya
 2. Mengajukan pengaduan dalam rangka penyelesaian sengketa data pribadi atas kegagalan perlindungan kerahasiaan data pribadinya oleh Penyelenggara Sistem Elektronik kepada Menteri
 3. Mendapatkan akses atau kesempatan untuk mengubah atau memperbaiki data pribadinya tanpa mengganggu sistem pengelolaan Data Pribadi, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan
 4. Mendapatkan akses atau kesempatan untuk memperoleh historis Data Pribadinya yang pernah diserahkan kepada Penyelenggara Sistem Elektronik sepanjang masih sesuai dengan ketentuan peraturan perundang-undangan
 5. Meminta pemusnahan Data Perseorangan Tertentu miliknya dalam Sistem Elektronik yang dikelola oleh Penyelenggara Sistem Elektronik, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan.
- c) Pasal 28 Mengenai Kewajiban Penyelenggara Sistem Elektronik, bahwa penyelenggara wajib:
 1. Melakukan sertifikasi Sistem Elektronik yang dikelolanya sesuai dengan ketentuan peraturan perundangundangan;
 2. Menjaga kebenaran, keabsahan, kerahasiaan, keakuratan dan relevansi serta kesesuaian dengan tujuan perolehan, pengumpulan, pengolahan, penganalisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan Data Pribadi
 3. Memberitahukan secara tertulis kepada Pemilik Data Pribadi jika terjadi kegagalan perlindungan rahasia Data Pribadi dalam Sistem Elektronik yang dikelolanya,

dengan ketentuan pemberitahuan sebagai berikut :

- a) Harus disertai alasan atau penyebab terjadinya kegagalan perlindungan rahasia Data Pribadi;
 - b) Dapat dilakukan secara elektronik jika Pemilik Data Pribadi telah memberikan Persetujuan untuk itu yang dinyatakan pada saat dilakukan perolehan dan pengumpulan Data Pribadinya;
 - c) Harus dipastikan telah diterima oleh Pemilik Data Pribadi jika kegagalan tersebut mengandung potensi kerugian bagi yang bersangkutan
 - d) Pemberitahuan tertulis dikirimkan kepada Pemilik Data Pribadi paling lambat 14 (empat belas) hari sejak diketahui adanya kegagalan
4. Memiliki aturan internal terkait perlindungan Data Pribadi yang sesuai dengan ketentuan peraturan perundang-undangan
 5. Menyediakan rekam jejak audit terhadap seluruh kegiatan penyelenggaraan Sistem Elektronik yang dikelolanya
 6. Memberikan opsi kepada Pemilik Data Pribadi mengenai Data Pribadi yang dikelolanya dapat/atau tidak dapat digunakan dan/atau ditampilkan oleh/pada pihak ketiga atas Persetujuan sepanjang masih terkait dengan tujuan perolehan dan pengumpulan Data Pribadi
 7. Memberikan akses atau kesempatan kepada Pemilik Data Pribadi untuk mengubah atau memperbarui Data Pribadinya tanpa mengganggu sistem pengelolaan Data Pribadi, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan
 8. Memusnahkan Data Pribadi sesuai dengan ketentuan dalam Peraturan Menteri ini atau ketentuan peraturan perundang-undangan lainnya yang secara khusus mengatur di masing-masing Instansi Pengawas dan Pengatur Sektor untuk itu
 9. Menyediakan narahubung (contact person) yang mudah dihubungi oleh Pemilik Data Pribadi terkait pengelolaan Data Pribadinya.

d) Pasal 29 Mengenai Penyelesaian Sengketa, yaitu:

1. Setiap Pemilik Data Pribadi dan Penyelenggara Sistem Elektronik dapat mengajukan pengaduan kepada Menteri atas kegagalan perlindungan kerahasiaan Data Pribadi.
2. Pengaduan sebagaimana dimaksud pada ayat (1) dimaksudkan sebagai upaya penyelesaian sengketa secara musyawarah atau melalui upaya penyelesaian alternatif lainnya.
3. Pengaduan sebagaimana dimaksud pada ayat (1) dilakukan berdasarkan alasan yaitu :
 - a) Tidak dilakukannya pemberitahuan secara tertulis atas kegagalan perlindungan rahasia Data Pribadi oleh Penyelenggara Sistem Elektronik kepada Pemilik Data Pribadi atau Penyelenggara Sistem Elektronik lainnya yang terkait dengan Data Pribadi tersebut, baik yang berpotensi maupun tidak berpotensi menimbulkan kerugian
 - b) Telah terjadinya kerugian bagi Pemilik Data Pribadi atau Penyelenggara Sistem Elektronik lainnya yang terkait dengan kegagalan perlindungan rahasia Data Pribadi tersebut, meskipun telah dilakukan pemberitahuan secara tertulis atas kegagalan perlindungan rahasia Data Pribadi namun waktu pemberitahuannya yang terlambat.
4. Menteri dapat berkoordinasi dengan pimpinan Instansi Pengawas dan Pengatur Sektor untuk menindaklanjuti pengaduan sebagaimana dimaksud pada ayat (1).



- e) Pasal 36 Mengenai Sanksi Administratif yang Diberikan Kepada Pelaku yang Melanggar Peraturan pada Pasal 36 ini, yaitu:
1. Setiap orang yang memperoleh, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, atau menyebarkan data pribadi tanpa hak atau tidak sesuai dengan ketentuan dalam Peraturan Menteri ini atau peraturan perundang-undangan lainnya dikenai sanksi administratif sesuai dengan ketentuan peraturan perundang-undangan berupa:
 - a) Peringatan lisan
 - b) Peringatan tertulis
 - c) Penghentian sementara kegiatan
 - d) Pengumuman di situs dalam jaringan (website online).

Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik memang sudah mengatur secara detail mengenai perlindungan data pribadi, mulai dari pengertian, batasan-batasan, tanggung jawab penyelenggara, proses perlindungan dan sanksi. Melihat permen Nomor 20 Tahun 2016 (PDP SE) sayangnya masih memiliki kelemahan yang mana tidak adanya perlindungan hukum terhadap korban untuk mendapatkan ganti kerugian yang dilakukan oleh pihak penyelenggara yang gagal melindungi data pribadi korban, serta tidak adanya sanksi pidana yang diberikan terhadap pelaku penyalahgunaan data pribadi hanya sanksi administrasi saja, dalam hal ini sanksi yang diberikan kurang cukup untuk memberikan efek jera terhadap pelaku sehingga perlunya formulasi sanksi yang sepadan yang harus diberikan sesuai dengan hukum pidana yang berlaku.

3) Perlindungan Hukum Terhadap Korban Pencurian Data Pribadi Melalui Media Digital Menurut Undang-Undang Nomor 31 Tahun 2014 Tentang Perubahan Atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban

Korban pencurian data pribadi yang pada dasarnya memiliki kebutuhan terhadap pemenuhan kerugian materil yang dialaminya, dalam Undang-Undang Nomor 31 Tahun 2014 Tentang Perubahan Atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban menyebutkan terdapat adanya perlindungan korban dan saksi tindak pidana yaitu dalam bentuk Kompensasi, Restitusi dan Bantuan.

Kerugian materil bagi korban tindak pidana pencurian data pribadi ini, Restitusi adalah metode yang tepat. Seperti dalam Pasal 1 Ayat 11 yang menyebutkan bahwa "Restitusi adalah ganti kerugian yang diberikan kepada Korban atau keluarganya oleh pelaku atau pihak ketiga." Untuk memperoleh perlindungan bagi korban tindak pidana melalui LPSK, harus melalui tahap pengajuan permohonan yang diajukan LPSK, dengan memperhatikan syarat-syarat yang tercantum dalam Pasal 21 Peraturan Pemerintah No. 7 Tahun 2018 tentang Pemberian Kompensasi, Restitusi dan Bantuan Kepada Saksi dan Korban.

Pada dasarnya pengajuan permohonan Restitusi kepada LPSK dapat diajukan sebelum perkara didakwakan, dan setelah perkara memperoleh putusan pengadilan. Dengan ditangani oleh LPSK, untuk mengajukan permohonan Restitusi dari pemohon ke

pihak terkait. Untuk perkara yang belum didakwakan, permohonan diajukan kepada penuntut umum agar dapat memuat permohonan kedalam tuntutan sekaligus, dan untuk perkara yang telah memperoleh putusan pengadilan diajukan kepada pengadilan agar dapat diberikan penetapan.

Dalam Pasal 7A ayat 1 Undang-Undang Nomor 31 Tahun 2014 Tentang Perubahan Atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban menyebutkan bahwa Korban tindak pidana berhak memperoleh Restitusi, berupa:

- a. Ganti kerugian atas kehilangan kekayaan atau penghasilan;
- b. Ganti kerugian yang ditimbulkan akibat penderitaan yang berkaitan langsung sebagai akibat tindak pidana
- c. Penggantian biaya perawatan medis dan/atau psikologis.

Dalam Peraturan Ketua LPSK Nomor 6 Tahun 2010 tentang Tata Cara Pemberian Perlindungan Saksi dan Korban, Pasal 16 Ayat 1 menyebutkan bahwa, Keputusan Rapat Paripurna anggota LPSK sebagaimana dimaksud dalam Pasal 15 Ayat 4 memuat:

- a. Klasifikasi kasus atau perkara: berat, sedang, atau ringan yang dihadapi oleh pemohon
- b. Bentuk perlindungan yang diberikan kepada pemohon
- c. Pemberian bantuan pemenuhan hak procedural.

Sehingga, kelanjutan pada tahap yang berikutnya hanya bergantung dari hasil Rapat Paripurna Anggota LPSK ini, kemudian selanjutnya jika dinyatakan diterima dapat dilimpahkan ke bidang perlindungan untuk masuk ke tahap pemberian perlindungan sebagaimana yang dimaksud dalam permohonan tersebut. Apabila, permohonan ditolak, LPSK tetap menyampaikan pemberitahuan tersebut kepada pihak pemohon secara tertulis. Akan tetapi, perlindungan hukum yang dimaksud menurut Undang-Undang Nomor 31 Tahun 2014 Tentang Perubahan Atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban ini ialah siapa saja yang mengajukan permohonan perlindungan yang dapat dilindungi ditinjau dari kerugian yang benar-benar dialami oleh korban.

Untuk kompensasi, kompensasi menurut Pasal 1 Ayat 10 Undang-Undang Nomor 31 Tahun 2014 Tentang Perlindungan Saksi dan Korban, "Kompensasi adalah ganti kerugian yang diberikan oleh negara karena pelaku tidak mampu memberikan ganti kerugian sepenuhnya yang menjadi tanggung jawabnya kepada Korban atau Keluarganya". Kompensasi hanya di berikan kepada korban pelanggaran hak asasi manusia yang berat dan terorisme, tidak ada pemberian kompensasi terhadap korban pencurian data.

Perlindungan hukum terhadap korban kejahatan yaitu terdapat dalam Undang-Undang Nomor 31 Tahun 2014 Tentang Perlindungan Saksi dan Korban, dalam undang-undang ini menjelaskan mengenai hak-hak korban dan perlindungan yang diberikan kepada korban, tetapi dalam Undang-Undang Nomor 31 Tahun 2014 Tentang Perlindungan Saksi dan Korban tidak memuat semua korban kejahatan yang mendapatkannya.

Dapat dipahami dari yang telah dijelaskan diatas bahwa terdapat beberapa peraturan yang mengatur tentang perlindungan pencurian data pribadi namun belum ada Undang Undang yang secara khusus membahas tentang perlindungan data pribadi, tidak

adanya kepastian hukum yang jelas terhadap pencurian data pribadi akan berdampak terhadap kesejahteraan privasi bagi para korban khususnya dan masyarakat pada umumnya karena semua warga negara berpotensi data pribadinya di curi serta disalahgunakan, oleh karena itu perlunya pemerintah untuk segera memberikan kepastian hukum yang jelas dan khusus mengenai data pribadi dengan mengedepankan dan mengikuti standar hukum internasional.

B. Perlindungan Hukum Terhadap Korban Pencurian Data Pribadi Melalui Media Digital Menurut Instrumen Hukum Internasional

Melihat perlindungan terhadap korban pencurian data di Indonesia masih belum memiliki Undang-Undang tersendiri atau khusus mengenai perlindungan data pribadi, ini membuat masyarakat susah untuk mendapat perlindungan. Dikarenakan kasus pencurian data menjadi masalah yang besar dan pelakunya juga susah untuk dapat dideteksi, sehingga hukum internasional pun ikut membahas dan mengatur struktur organisasi internasional salah satunya yang diatur yaitu perlindungan mengenai data pribadi. Adapun beberapa Instrumen hukum Internasional yang mengatur perlindungan data pribadi yaitu:

1. *Organization for Economic Co-operation and Development (OECD) Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data 1980*

OECD (*The Organization for Economic and Cooperation Development*) turut serta dengan mengeluarkan *guidelines*/pedoman prinsip dasar dalam perlindungan data pribadi yang dapat dijadikan suatu rujukan dalam membuat suatu aturan. Adapun prinsip-prinsip dasar tersebut yaitu:

- a. Prinsip pengumpulan batasan (*collection limitation principle*), untuk melakukan pengumpulan data pribadi secara sah dan adil, serta diikuti persetujuan dari subjek data dan dengan sepengetahuannya.
- b. Prinsip Kualitas (*Data Quality Principle*), pengambilan data pribadi harus cocok dengan tujuan pengguna serta data pribadi tersebut harus lengkap, akurat dan apabila terdapat perubahan harus segera diperbaharui
- c. Prinsip Tujuan Khusus (*Purpose Specification Principle*), tujuan pengumpulan data pribadi harus ditentukan paling lambat pada saat data pribadi dikumpulkan
- d. Prinsip Batasan Penggunaan (*Use Limitation Principle*), persetujuan pemilik data diperlukan untuk mengungkapkan, menyediakan atau menggunakan data tersebut untuk tujuan selain tujuan awal dikumpulkannya data tersebut
- e. Prinsip Perlindungan Keamanan (*Security Safeguard Principle*), data pribadi harus mendapatkan perlindungan dari resiko kehilangan data, perusakan terhadap data, penggunaan tanpa ijin, pengungkapan data maupun akses yang tidak sah.
- f. Prinsip Keterbukaan (*Openness Principle*) Tujuan utama penggunaan data, identitas serta pengontrol data harus dibangun, sebelumnya harus dibentuk kebijakan tentang keterbukaan terkait pengembangan atau pengelolaan yang berkaitan dengan data pribadi.
- g. Prinsip Partisipasi Individu (*Individual Participation Principle*) Tujuan dari prinsip ini adalah untuk mengontrol data atau mengkonfirmasi data yang terkait dengannya dengan memberikan akses untuk dapat dihapus, dirubah maupun diperbaiki.

h. Prinsip Akuntabilitas (*Accountability Principle*) Pengontrol data harus bertanggung jawab untuk mematuhi langkah-langkah yang berdampak pada prinsip-prinsip yang disebutkan di atas.

OECD telah mengatur tentang prinsip-prinsip dasar perlindungan data pribadi kemudian juga mengatur pedoman terkait tentang perlindungan data pribadi, namun OECD dalam hal perlindungan hukum terhadap korban belum sama sekali mengatur tentang aturan hukum terkait ganti kerugian yang harus diberikan kepada korban pencurian data pribadi sehingga membuat Instrumen Hukum Internasional yang termuat dalam OECD ini belum begitu optimal. OECD juga seharusnya bisa memfokuskan pada korban pencurian data pribadi yang telah dirugikan sehingga para korban dapat mendapatkan hak mereka yang telah di ambil oleh pelaku pencurian data pribadi.

2. European Union Data Protection Directive 1995

Mengenai aturan umum tentang prinsip-prinsip negara-negara anggota pada Pasal 6 Data Protection Directive 1995 menetapkan bahwa data pribadi harus:

- a. Diproses secara adil dan legal
- b. Dikumpulkan secara jelas dan legal sesuai dengan tujuan yang telah ditentukan, dan tidak akan diproses secara lanjut dengan cara yang tidak sesuai dengan tujuan
- c. Relevan dan tidak berlebihan dengan tujuan pengumpulan dan pemrosesan
- d. Data harus akurat, setiap data yang tidak akurat atau tidak lengkap harus di hapus atau diperbaiki
- e. Disimpan dalam bentuk yang memungkinkan untuk identifikasi subjek data. Dan negara-negara harus menetapkan perlindungan yang sesuai untuk data pribadi yang akan disimpan dalam priode yang lama.
- f. Diproses keamanan data pribadi dengan cara menjamin perlindungan terhadap pemrosesan, dan tidak melanggar hukum.

Upaya-upaya hukum mengenai tanggung jawab dan sanksi, dimana tentang kewajiban negara diatur dalam Pasal 23 ayat 1 dan 2 Data Protection Directive 1995 yaitu:

1. Negara-negara anggota harus menetapkan bahwa setiap orang yang telah menderita kerugian berhak untuk mendapatkan kompensasi dari pengolahan yang melanggar hukum.
2. Pengendali dapat dibebaskan dari kewajiban ini apabila terbukti bahwa ia tidak bertanggung jawab terhadap kerusakan yang terjadi

Selanjutnya mengenai otoritas pengawas dan perlindungan individu dalam pengelolaan data pribadi yang di atur dalam Pasal 28 Data Protection Directive 1995 dimana otoritas pengawasannya yaitu:

1. Setiap negara-negara anggota harus menetapkan bahwa satu atau lebih otoritas publik harus bertanggung jawab untuk memantu penerapan didalam wilayah dari ketentuan-ketentuan yang dipegang oleh negara-negara anggota



2. Setiap negara anggota harus menetapkan bahwa otoritas pengawas dikonsultasikan ketika menyusun tindakan atau peraturan administratif yang berkaitan dengan perlindungan hak serta kebebasan individu sesuai dengan pemrosesan data pribadi
3. Setiap otoritas secara khusus akan diberikan wewenang investigasi seperti wewenang untuk mengakses data, kekuatan intervensi yang efektif seperti memberikan pendapat sebelum operasi pemrosesan dilakukan, serta yang terakhir kekuasaan dapat terlibat dalam proses hukum
4. Setiap otoritas pengawas harus mendengarkan klaim yang di ajukan oleh setiap orang
5. Setiap otoritas pengawas harus membuat laporan kegiatannya secara berkala, serta laporan tersebut akan diumumkan kepada publik
6. Setiap otoritas pengawas berwenang, apapun hukum nasional yang berlaku untuk pemrosesan yang bersangkutan untuk melaksanakan di wilayah negara anggotanya sendiri
7. Setiap anggota dan staf otoritas setelah masa kerja mereka berakhir, mereka harus tunduk pada kewajiban kerahasiaan yang berkenaan dengan informasi rahasia yang telah mereka akses.

Melihat beberapa peraturan yang ada pada *European Union Data Protection Directive*, dapat kita simpulkan bahwa intruksi dari *European Union Data Protection Directive* ini dianggap sebagai peraturan mengenai perlindungan data pribadi yang paling kuat. Walaupun instruksi ini memang hanya berlaku untuk negara-negara di Eropa saja, tentu instruksi ini bisa menjadi rujukan atau pedoman untuk negara-negara lain termasuk Indonesia sendiri, dalam membuat peraturan mengenai perlindungan data pribadi melalui media digital agar jauh lebih aman dalam melindungi masyarakat dari kasus pencurian data pribadi.

3. Resolusi Majelis Umum Perserikatan Bangsa-Bangsa mengenai Hak Privasi di Era Digital atau disebut dengan (*The Rights of Privacy in Digital Age*)

Resolusi ini juga salah satu respon atas gerakan negara Jerman dan Brazil, sehingga resolusi ini pun didukung oleh tiga puluh lima negara termasuk Indonesia, adapun hal-hal yang memuat Resolusi Majelis Umum PBB tentang Hak Privasi Diera Digital ini yaitu:

- a. Resolusi ini meningkatkan kapasitas pemerintah atau perusahaan untuk melakukan pengawasan terhadap pengumpulan data yang melanggar hak privasi
- b. Menegaskan hak manusia untuk privasi agar tidak mengalami gangguan sewenang-wenang
- c. Menekankan tindakan yang melanggar hak privasi, adalah perbuatan mengganggu hak kebebasan dan bertentangan dengan prinsip-prinsip masyarakat demokratis
- d. Resolusi ini memperhatikan mengenai dampak negatif terhadap intersepsi komunikasi serta pengumpulan data pribadi khususnya dilakukan dalam skala massal
- e. Menegaskan bahwa hak yang dimiliki oleh seseorang secara offline maka harus juga dilindungi secara online, termasuk juga hak privasi
- f. Memberitahukan kepada seluruh negara-negara untuk:
 1. Menghormati dan melindungi hak privasi, termasuk komunikasi secara digital



2. Mengambil tindakan untuk mengakhiri pelanggaran terhadap hak-hak privasi agar menciptakan kondisi untuk mencegah pelanggaran
3. Meninjau prosedur, praktik, dan perundang-undangan mengenai pengawasan komunikasi, dan pengumpulan data, hal ini dengan maksud untuk menegakkan hak privasi pelaksanaannya berdasarkan hak asasi manusia dan hukum internasional
4. Membentuk independensi pengawasan yang mampu menjamin untuk pengawasan terhadap komunikasi, intersepsi dan pengumpulan data pribadi
5. Memberikan ganti kerugian yang sepadan terhadap individu yang hak atas privasinya dilanggar, sesuai dengan kewajiban hak asasi internasional.

Beberapa instrumen hukum internasional yang sudah dijelaskan sebelumnya membuktikan bahwa sangat penting untuk melindungi data pribadi warga negara, melihat mayoritas penduduk Indonesia saat ini sudah sangat banyak menggunakan teknologi, sudah sepantasnya negara Indonesia melindungi warga negaranya agar aman atas privasinya. Dapat kita lihat saat ini Indonesia belum memiliki Undang-Undang khusus yang mengatur mengenai perlindungan data pribadi, Indonesia sendiri baru memiliki peraturan khusus mengenai perlindungan data pribadi di media digital yang dimana dalam bentuk Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Hal ini juga menunjukkan kemajuan terhadap negara Indonesia yang sudah memiliki peraturan mengenai perlindungan data pribadi walaupun baru dalam bentuk Peraturan Pemerintah.

C. Perbedaan Perlindungan Hukum Terhadap Korban Pencurian Data Pribadi Melalui Media Digital Menurut Perundang-Undangan Indonesia dan Instrumen Hukum Internasional

Tabel. 1 Kelebihan dan Kekurangan Perundang Undangan Indonesia dan Instrumen

Hukum Internasional

	Kelebihan	Kekurangan
Perundang Undangan Indonesia	<ul style="list-style-type: none"> • Dalam UU No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik pada pasal 26 ayat 1 menyebutkan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan dan pada Ayat 2 nya dijelaskan pula bagi setiap orang yang dilanggar haknya sebagaimana yang dimaksud pada ayat 1 maka 	<ul style="list-style-type: none"> • Pada UU No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik tidak adanya perlindungan hukum terhadap pemilik data yang dilakukan oleh pihak yang terkait seperti penyelenggara data pribadi. • Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tidak mengatur mengenai bentuk ganti kerugian bagi korban yang harus ditanggung pihak



	<p>dapat mengajukan gugatan atas kerugian yang ditimbulkan.</p> <ul style="list-style-type: none"> • Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan data Pribadi dalam Sistem Elektronik sudah cukup jelas dalam melindungi data pribadi dimedi digital • Undang Undang Nomor 31 Tahun 2014 Tentang Perlindungan Saksi dan Korban mengatur tentang perlindungan saksi dan korban serta korban berhak mendapatkan kompensasi dan restitusi 	<p>ketiga.</p> <ul style="list-style-type: none"> • Undang Undang Nomor 31 Tahun 2014 Tentang Perlindungan Saksi dan Korban tidak memuat secara pasti bahwa korban pencurian data pribadi mendapat perlindungan.
<p>Instrumen Hukum Internasional</p>	<ul style="list-style-type: none"> • OECD membuat rujukan mengenai prinsip dasar dalam melindungi privasi atas data pribadi di internet ataupun media digital. • European Union Data Directive 1995 memberikan kewajiban secara langsung kepada pihak perorangan atau organisasi untuk menentukan tujuan dan langkah dalam mengolah data pribadi secara adil dan legal serta tidak melanggar hukum yang berlaku. • Pasal 23 ayat 1 data protection directive 1995 mengatur tentang negara anggota harus menetapkan bagi setiap orang yang telah menderita kerugian berhak mendapatkan kompensasi dari pengolahan data yang 	<ul style="list-style-type: none"> • OECD hanya mengatur tentang prinsip prinsip dasar perlindungan data pribadi namun tidak mengatur tentang perlindungan hukum terhadap korban • European Union Data Directive 1995 memang dianggap sebagai peraturan perlindungan data pribadi yang paling kuat, namun sayangnya instruksi ini hanya berlaku untuk negara negara di Eropa saja.



	<p>melanggar hukum.</p> <ul style="list-style-type: none">• Data protection directive 1995 juga mengatur tentang prinsip transfer data pribadi, otoritas pengawas dan perlindungan individu dalam pengolahan data pribadi.• Pembentukan Resolusi Majelis Umum PBB tentang Hak Privasi diEra Digital untuk dapat menghormati dan melindungi hak privasi setiap warganya, serta tanggung jawab negara terhadap ganti kerugian yang dialami setiap orang yang merasa dirugikan atas privasinya sesuai dengan kewajiban hak asasi manusia internasional.	
--	---	--

Dari tabel diatas dapat dipahami bahwa hukum Indonesia masih belum mengatur secara jelas mengenai perlindungan hukum terhadap korban pencurian data pribadi melalui media digital. Dalam pemberian restitusi dan kompensasi yang diatur dalam UU Nomor 31 tahun 2014 tentang perlindungan saksi dan korban, pemberian restitusi pada UU ini tidak menyebutkan secara pasti bahwa korban pencurian data pribadi dapat mengajukan restitusi, kemudian kompensasi juga hanya diberikan kepada korban pelanggaran Hak Asasi Manusia yang berat dan terorisme, tidak ada kompensasi bagi korban pencurian data. Dalam Instrumen hukum Internasional pembahasan mengenai perlindungan hukum terhadap pencurian data pribadi belum semua membahas tentang perlindungan hukum terhadap korban, seperti halnya OECD yang hanya membahas prinsip prinsip dasar tentang perlindungan data pribadi. Instrumen Hukum Internasional juga belum dapat mencakup seluruh negara yang mana hanya baru menyentuh Regional Uni Eropa saja, namun Indonesia bisa menjadikan European Union Data Directive 1995 dan Resolusi Majelis Umum PBB sebagai standar dalam membuat aturan mengenai perlindungan hukum terhadap korban pencurian data pribadi.

A. Kebijakan Perlindungan Hukum Terhadap Korban Pencurian Data Pribadi Melalui Media Digital Ditinjau Dari Rancangan Undang-Undang Perlindungan Data Pribadi

Rancangan Undang-Undang Perlindungan Data Pribadi mendefinisikan, data pribadi adalah “setiap data tentang seseorang baik yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau nonelektronik.” Serta dalam Rancangan Undang-Undang Perlindungan Data Pribadi pun menjelaskan, mana yang termasuk data yang bersifat umum dan spesifik. Adapun data pribadi yang bersifat umum yaitu nama lengkap, jenis kelamin, kewarganegaraan, agama, dan yang terakhir data pribadi yang dikombinasi untuk mengidentifikasi seseorang, adapun data pribadi yang bersifat spesifik yaitu data informasi kesehatan, data biometrik, data genetika, data orientasi seksual, pandangan politik, catatan kejahatan, data anak, data keuangan pribadi.

Dalam RUU Pelindungan Data Pribadi mengatur tentang pihak-pihak yang terlibat dalam pemrosesan data pribadi, yaitu pemilik data pribadi, pengendali data pribadi, dan prosesor data pribadi. Pemilik data pribadi selaku subyek data memiliki hak, antara lain hak untuk meminta informasi, hak untuk melengkapi, mengakses, memperbarui, dan/atau memperbaiki kesalahan dan/atau ketidakakuratan data pribadi miliknya, hak untuk mengakhiri pemrosesan, menghapus, dan/atau memusnahkan data pribadi miliknya (right to erasure), hak untuk menarik kembali persetujuan pemrosesan, hak untuk mengajukan keberatan atas tindakan profiling, hak terkait penundaan atau pembatasan pemrosesan, hak untuk menuntut dan menerima ganti rugi.

Pengendali data pribadi adalah pihak yang tujuannya untuk melakukan pemrosesan data pribadi. Dengan demikian, pengendali data pribadi wajib bertanggung jawab atas seluruh pemrosesan data pribadi. Sedangkan prosesor data pribadi adalah pihak yang melakukan pemrosesan data pribadi atas nama pengendali data pribadi. walaupun pengendali data pribadi dan prosesor data pribadi berbeda namun tetap memiliki kewajiban dasar yang sama, inilah 7 lingkup kewajiban dasar yang sama antara pengendali data pribadi dan prosesor data pribadi yaitu, menjaga kerahasiaan data pribadi, melindungi dan memastikan keamanan data pribadi, termasuk menjaga data pribadi diakses secara tidak sah, melakukan pengawasan terhadap seluruh aktivitas pemrosesan data pribadi, melakukan perekaman aktivitas pemrosesan data pribadi, menjamin akurasi, kelengkapan, perbaikan dan konsistensi data pribadi.

Untuk memastikan keefektifan penegakan hukum perlindungan data pribadi, Rancangan Undang-Undang ini juga mengatur sanksi administratif, sanksi pidana, ganti rugi dan sanksi pidana ditujukan terhadap penyalahgunaan data pribadi. Sanksi administratif dapat berupa peringatan tertulis, penghentian sementara kegiatan pemrosesan, penghapusan atau pemusnahan data pribadi, ganti rugi, dan denda administratif. Dalam RUU PDP terhadap pihak penyelenggara (Korporasi) yang tidak dapat melindungi data pribadi milik penggunanya maka dapat dikenakan pidana denda sesuai dengan pasal 66 ayat 2 sampai ayat 4 RUU ini yaitu : “(2) Pidana yang dapat dijatuhkan terhadap Korporasi hanya pidana denda. (3) Pidana denda yang dijatuhkan

kepada Korporasi paling banyak 3 (tiga) kali dari maksimal pidana denda yang diancamkan. (4) Selain dijatuhi pidana denda sebagaimana dimaksud pada ayat (2), Korporasi dapat dijatuhi pidana tambahan berupa:

- a) perampasan keuntungan dan/atau harta kekayaan yang diperoleh atau hasil dari tindak pidana;
- b) pembekuan seluruh atau sebagian usaha Korporasi;
- c) pelarangan permanen melakukan perbuatan tertentu;
- d) penutupan seluruh atau sebagian tempat usaha dan/atau kegiatan Korporasi;
- e) melaksanakan kewajiban yang telah dilalaikan; dan
- f) pembayaran ganti kerugian, serta tidak adanya sanksi pidana yang diberikan kepada pihak penyelenggara data pribadi yang melanggar.

Rancangan Undang Undang Perlindungan data pribadi juga mengatur ganti rugi bagi para korban dengan pengajuan penyelesaian sengketa melalui gugatan perdata. Terkait pengajuan ganti kerugian bagi para korban akan lebih mudah apabila langsung dimasukkan kedalam dakwaan pada perkara pidana yang bersangkutan, dikarenakan jika para korban harus melakukan gugatan ganti kerugian dalam perkara perdata itu akan sangat menyulitkan para korban. Korban yang telah dirugikan dan direnggut hak nya oleh pelaku sebaiknya harus diberi jalan yang semudah mudahnya oleh pemerintah untuk mendapatkan ganti kerugian materiil maupun immateriil yang diakibatkan oleh pelaku kejahatan, khususnya pencurian data pribadi.

Adapun ketentuan yang melanggar Pasal 51 Ayat 1 Rancangan Undang-Undang Perlindungan Data Pribadi yaitu "Setiap Orang dilarang memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum atau dapat mengakibatkan kerugian Pemilik Data Pribadi". Akan di kenakan sanksi pada Pasal 61 Ayat 1 Rancangan Undang-Undang Perlindungan Data Pribadi yaitu "Setiap Orang yang dengan sengaja memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum atau dapat mengakibatkan kerugian Pemilik Data Pribadi sebagaimana dimaksud dalam Pasal 51 ayat 1 dipidana dengan pidana penjara paling lama 5 (lima) tahun atau pidana denda paling banyak Rp50.000.000.000,00 (lima puluh miliar rupiah)". Pasal 65 RUU PDP Menyatakan Selain dijatuhi pidana penjara lima 5 (lima) Tahun dan denda paling banyak Rp. 50.000.000.000,00 (lima puluh miliar rupiah) terdakwa juga dapat dijatuhi pidana tambahan berupa perampasan keuntungan atau harta kekayaan yang diperoleh dan hasil dari tindak pidana dan pembayaran ganti kerugian.

Melihat beberapa peraturan yang di atur dalam Rancangan Undang-Undang Perlindungan Data Pribadi pastinya ada kekurangan yang dimana kekurangan tersebut yaitu seperti pada pemrosesan data pribadi, dimana Rancangan Undang-Undang Perlindungan Data Pribadi tersebut tidak menyebutkan secara jelas tugas dan tanggung jawab Kominfo dalam perannya sebagai otoritas perlindungan data pribadi. Serta tidak adanya komisi indenpenden khusus untuk mengawasi pengelolaan data pribadi, Ardi Khawatir selaku coordinator riset imparisial mengatakan "jika pengelolaan data pribadi sepenuhnya diserahkan kepada pemerintah, katakanlah Kominfo, maka kerentanan



terjadinya penyalahgunaan data pribadi makin besar”. Oleh dari itu sudah sepatutnya Indonesia memiliki badan khusus yang mengawasi pengelolaan data pribadi. Sedangkan dalam General Data Protection Regulation (GDPR) otoritas perlindungan data pribadinya telah independen dan memiliki cakupan tanggung jawab yang jelas untuk memastikan badan tersebut bisa menegakkan hukum dan memberikan sanksi kepada pihak-pihak kepentingan seperti pemerintah dan perusahaan.

Selanjutnya kelemahan pada Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) yaitu, tidak adanya sanksi pidana terhadap pihak penyelenggara data pribadi, bila melakukan pelanggaran, hanya ada sanksi administratif yang dikenakan, hal ini dirasa kurang cukup dalam memberikan efek jera terhadap pihak penyelenggara yang melakukan pelanggaran terhadap data pribadi korban.

Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) memang belum mencakup standar Internasional, dengan hal ini diharapkan negara Indonesia harus segera merevisi RUU PDP agar sesuai dengan standar internasional dalam melindungi data pribadi semua warga negaranya, serta mengesahkan secepat mungkin agar masyarakat dapat terlindungi dari kejahatan pencurian data pribadi dan mendapatkan kepastian hukum yang maksimal. Kehadiran RUU PDP diharapkan dapat memberi perlindungan sistem elektronik dari serangan keamanan siber, dan perlindungan data pribadi masyarakat dalam platform digital. pemerintah terus melakukan upaya untuk melindungi data pribadi masyarakat, guna menghindari penyalahgunaan atau kebocoran data yang dilakukan pihak-pihak yang tidak bertanggung jawab. Dalam menanggulangi masalah kebocoran data pribadi pemerintah melalui lembaga kominformo ikut turun tangan memberikan penguatan regulasi dan mengajak seluruh masyarakat untuk terus meningkatkan literasi khususnya terkait perlindungan data pribadi. Termasuk mengikuti berbagai pelatihan literasi digital yang disediakan, di mana target Kemenkominformo per tahunnya mencapai 12,5 juta masyarakat melek literasi digital.

Melihat pemerintah dalam menanggulangi korban pencurian data pribadi hanya memberikan sosialisasi serta pelatihan literasi digital (himbauan) dirasa kurang cukup dalam melindungi korban, yang seharusnya pemerintah harus menjamin perlindungan terhadap korban yang mendapatkan kerugian dengan memberikan atau memperbaharui UU PSK agar di tambahkan dapatnya di berikan kompensasi terhadap korban pencurian data pribadi dikarenakan perlindungan terhadap korban pencurian data pribadi ini adalah salah satu tanggung jawab negara untuk melindungi setiap warga negaranya, dapat dilihat dalam Pasal 28 G ayat 1 Undang-Undang Dasar 1945 yang menyatakan bahwa “setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi manusia”.

4. KESIMPULAN

A. Pengaturan mengenai perlindungan data pribadi dalam hukum Indonesia yaitu diatur dalam Pasal 26 Ayat 1 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

namun UU ini belum mengatur tentang perlindungan hukum terhadap pemilik data yang dilakukan oleh pihak yang terkait seperti penyelenggara data pribadi. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik namun Permen ini tidak mengatur mengenai bentuk ganti kerugian bagi korban yang harus ditanggung pihak ketiga. Undang Undang Nomor 14 Tahun 2016 Tentang Perlindungan Saksi dan Korban hanya mengatur pemberian restitusi dan kompensasi bagi korban pelanggaran HAM berat. Pengaturan mengenai perlindungan data pribadi dalam instrumen hukum internasional diatur dalam Organization for Economic Co- operation and Development (OECCD) Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data 19880, namun OECD belum membahas tentang perlindungan hukum terhadap korban, selanjutnya European Union Data Protection Directive 1995 Instrumen hukum ini dianggap sebagai peraturan perlindungan data pribadi yang paling kuat dalam melindungi data pribadi dan juga korban, namun sayangnya instruksi ini hanya berlaku untuk negara negara di Eropa saja, selanjutnya Resolusi Majelis Umum Perserikatan Bangsa- Bangsa mengenai Hak Privasi di Era Digital atau disebut dengan (The Rights of Privacy in Digital Age) telah optimal dalam mengatur perlindungan korban dan data pribadi serta Instrumen Hukum ini dapat dijadikan pedoman bagi Negara Indonesia dalam membuat aturan hukum perlindungan data pribadi dan korban.

B. Kebijakan Rancangan Undang-Undang Perlindungan Data Pribadi sudah dikatakan optimal dalam melindungi korban dari pencurian data pribadi, RUU PDP telah mengatur tentang definisi data pribadi, jenis, hak kepemilikan, pemrosesan, pengecualian, pengendali dan prosesor, pengiriman, lembaga berwenang yang mengatur data pribadi, serta penyelesaian sengketa. Selain itu, RUU PDP juga akan mengatur kerja sama internasional hingga sanksi yang dikenakan atas penyalahgunaan data pribadi. RUU PDP sudah lebih fokus membahas dan mengatur secara khusus tentang perlindungan hukum terhadap korban yang dirugikan dan juga terhadap perlindungan privasi dari data data pribadi. RUU PDP juga memiliki kelemahan yaitu tidak menyebutkan secara jelas tugas dan tanggung jawab Kominfo dalam perannya sebagai otoritas pelindungan data pribadi. Serta tidak adanya komisi indenpenden khusus untuk mengawasi pengelolaan data pribadi.

5. DAFTAR PUSTAKA

Abdul Salam Siku. Perlindungan Hak Asasi Saksi Dan Korban Dalam Proses Peradilan Pidana, Indonesia Prime, Indonesia, 2016.

Amira Paripurna, dkk. Viktimologi Dan Sistem Peradilan Pidana. Deepublish, Yogyakarta, 2021.

Marli Candra dan Imron Rosyadi. Victim Precipitation Dalam Tindak Pidana Pencurian (Sebuah Pendekatan Viktimologi), Duta Media Publishing, Indonesia, 2020.



M. Arief Mansur dan Elistaris Gultom. *Cyber Law Aspek Hukum Teknologi Informasi*. Refika Aditama, Bandung, 2005.

Muhadar. *Perlindungan Saksi Dan Korban Dalam Sistem Peradilan Pidana*, Putra Media Nusantara, Surabaya, 2010.

Republik Indonesia "Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan Atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi Dan Korban,".

Republik Indonesia, "Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik".

Republik Indonesia. "Peraturan Menteri Komunikasi Dan Informatika Republik Indonesia Nomor 5 Tahun 2015 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik,".

Joshefin Mareta. "Analisis Kebijakan Perlindungan Saksi Dan Korban." *Balitbangham.Go.Id* Vol 10, No. 1, 2016, hlm.1-29. [https://www.balitbangham.go.id/po-content/po-upload/jikh volume 10 No 1 tahun 2016](https://www.balitbangham.go.id/po-content/po-upload/jikh%20volume%2010%20No%201%20tahun%202016).

Kominfo. "Kementerian Komunikasi Dan Informatika." *Kominfo.Go.Id*. Last modified 2020. Accessed January 28, 2022. <https://www.kominfo.go.id/content/detail/28343/bersama-lindungi-data-pribadi-di-platform-digital/0/artikel>.

Catatan :

Nomor ponsel yang dapat dihubungi : 085326864776