



ANALISIS CYBER CRIME TERHADAP PENCURIAN DATA DALAM HUKUM POSITIF INDONESIA

Mimi Rahayu

Fakultas Hukum Universitas Muhammadiyah Sumatera Barat

Email: mimirahayu1979@gmail.com

Abstract

This article will answer how important it is to enact a special law to protect the personal data of every public and a firm and comprehensive policy in overcoming the theft of personal data that takes place through electronic media in Indonesia. This problem arises with the current development of information technology which has created new legal issues, namely regarding the security of personal data that takes place through electronic media. The large number of parties using the electronic media as a means of communication and transactions has resulted in the theft of personal data. However, so far Indonesia has not had a specific law to tackle the misuse of personal data. The research used in this study, a normative juridical namely a research method with a focus on the study of the application of norms in positive law. In Indonesia, the rules regarding this matter are contained in Article 26 of Law No. 19 of 2016, amendments to Law No. 11 of 2008 concerning Electronic Information and Transactions and Government Regulation No.71 of 2019 concerning the implementation of electronic systems and transactions. Even so, the Article and these efforts are still felt to be ineffective. It is deemed necessary to immediately enact a separate law relating to the protection of personal data so that it can guarantee the security and protection of personal data.

Keywords: *Cyber Crime, personal data; electronic media.*

Abstrak

Dalam Artikel ini akan menjawab seberapa pentingnya penetapan undang-undang khusus melindungi data pribadi setiap masyarakat dan kebijakan yang tegas dan komprehensif dalam menanggulangi pencurian data pribadi yang berlangsung melalui media elektronik di Indonesia. Permasalahan ini muncul dengan perkembangan teknologi informasi saat ini telah menimbulkan persoalan hukum baru, yaitu mengenai keamanan atas data pribadi yang berlangsung melalui media elektronik. Banyaknya pihak yang menggunakan media elektronik tersebut sebagai alat komunikasi dan transaksi mengakibatkan terjadinya pencurian data pribadi. Akan tetapi sampai sejauh ini Indonesia belum punya undang-undang khusus yang dalam menanggulangi penyalahgunaan data pribadi. Penelitian yang digunakan dalam penelitian ini adalah penelitian yang bersifat yuridis normatif yaitu metode penelitian dengan fokus kajian mengenai penerapan kaidah-kaidah atau norma-norma dalam hukum positif. Di Indonesia aturan mengenai hal tersebut terdapat dalam Pasal 26 Undang-Undang No 19 Tahun 2016 perubahan atas UU No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Peraturan Pemerintah No.71 Tahun 2019 tentang penyelenggaraan sistem dan transaksi elektronik. Meskipun demikian, Pasal tersebut serta upaya tersebut masih dirasakan kurang efektif. hal ini dipandang perlu segera disahkan undang-undang

tersendiri yang berkaitan dengan perlindungan data pribadi sehingga dapat memberikan jaminan keamanan dan perlindungan pada data pribadi.

Kata Kunci: *Cyber Crime, data pribadi, media elektronik.*

A. PENDAHULUAN

Kemajuan teknologi informasi terutama pada bidang komputer dan internet terbukti telah memberikan dampak positif bagi kemajuan kehidupan manusia. Perlu digaris bawahi, dibalik kelebihan dan kemudahan yang ditawarkan oleh komputer dan internet, ternyata memiliki sisi gelap yang dapat menghancurkan kehidupan dan budaya manusia itu sendiri.¹Perkembangan teknologi informasi mengubah pola pemikiran mengenai batas wilayah, waktu, nilai-nilai, wujud benda, logika berfikir, pola kerja, dan batas perilaku sosial dari yang bersifat manual menjadi komputerisasi/digital.²Informasi sudah dianggap sebagai “power” yang diartikan sebagai kekuatan dan kekuasaan yang sangat menentukan nasib manusia itu sendiri.Saat ini ketergantungan masyarakat akan teknologi informasi semakin tinggi sehingga semakin tinggi pula resiko yang dihadapi. Teknologi informasi saat ini menjadi “pedang bermata dua” karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum termasuk tindak pidana (kejahatan). Berbagai bentuk tindak pidana (kejahatan) inilah yang kemudian dikenal dengan istilah “cybercrime”.³

Tidak hanya itu suatu tindak pidana (*cybercrime*) yang berpotensi Berawal pada tahun 2003 banyak kejahatan-kejahatan (*cybercrime*) yang bermunculan dengan dengan memanfaatkan kemajuan dari teknologi informasi, seperti kejahatan *carding* (*credit card fraud*), *ATM/EDC skimming*, *hacking*, *cracking*, *phising* (*internet banking fraud*), *malware* (*virus/worm/trojan/bots*), *cybersquatting*, pornografi, perjudian online, transnasional crime (perdagangan narkoba, mafia, terorisme, *money laundering*, *human trafficking*, *underground economy*).Kesemua tindak pidana tersebut bisa dengan mudah dan efektif dilakukan dengan memanfaatkan kemajuan teknologi informasi itu sendiridilakukan dengan mudah dan efektif dengan memanfaatkan perkembangan teknologi dan informasi juga pada sektor pengelolaan data dan informasi khususnya pada pengelolaan data pribadi yang membutuhkan perlindungan data. Sebab dengan kemajuan teknologi informasi dan komunikasi tersebut membuat batas privasi makin tipis sehingga berbagai data-

Brisilia Tumulun, “Upaya Penanggulangan Kejahatan Komputer Dalam Sistem Elektronik Menurut Pasal 30 Undang-Undang Nomor 11 Tahun 2008,” *Jurnal Lex Et Societatis* 6, No. 2 (2018), Hlm 67.

¹Dian Ekawati, “Perlindungan Hukum Terhadap Nasabah Bank Yang Dirugikan Akibat Kejahatan Skimming Ditinjau Dari Perspektif Teknologi Informasi Dan Perbankan,” *Jurnal Unes Law Review* 1, No. 2 (2018), Hlm 158.

data pribadi semakin mudah untuk tersebar. Salah satu contoh kejahatan penyalahgunaan data pribadi yaitu pencurian data pribadi dengan modus operandi awalnya adalah penipuan: kasus yang terjadi di Indonesia pada tahun 2019 yaitu ajakan mengikuti try out simulasi *computer assisted test* (CAT). yang diselenggarakan oleh akun @cpnsindonesia.id di Instagram walaupun ajakan tersebut belum memunculkan korban. Namun ajakan simulasi try out CPNS berbasis “CAT” tersebut dianggap sebuah penipuan karena saat melakukan pendaftaran, setiap calon peserta diminta untuk melakukan pengisian data pribadi (*privacy date*) pada link yang disediakan. Sehingga data tersebut diduga akan disalahgunakan oleh para pihak yang tidak bertanggung jawab. Sehubungan dengan kejadian untungnya dengan cepat ditindaklanjuti oleh BKN kejadian tersebut dengan mengingatkan melalui akun resmi twitter dari BKN itu sendiri bahwa “BKN tidak pernah melakukan kerja sama dengan pihak lain dalam melakukan simulasi berbasis CAT walaupun ada maka akan ada pemberitahuan resmi melalui website dan media sosial resmi milik BKN”.⁴

Berkaitan dengan pencurian data pribadi seperti yang dilakukan oleh perusahaan besar seperti facebook yang pernah ditulis dalam artikel Rudi Natamiharja dalam jurnal Fiat Justisia yang berjudul “A Case Study on Facebook Data Theft in Indonesia” mengenai pencurian data yang dialami perusahaan media sosial facebook. Mekanisme pengumpulan data pribadi dapat dilakukan dengan sederhana. Sebagai contoh, konsumen memberikan data tanpa ada paksaan. Ia memberikan data pribadi kepada facebook dengan cara mengisi formulir pendaftaran. Hal ini dilakukan dengan penuh kesadaran memberikan persetujuan secara terang-terangan atau tersembunyi. Berkaitan dengan perlindungan terhadap permasalahan-permasalahan yang telah disampaikan diatas khususnya terkait dengan pencurian data pribadi milik orang sangatlah diperlukan. Saat ini perlindungan hukum sebagaimana dimaksud tersebar pada beberapa Peraturan perundang-undangan yang berlaku seperti pada Pasal 79. ayat (1) Undang-Undang Nomor 24 Tahun 2013 Tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan (UU Administrasi Kependudukan), Pasal 5815 Peraturan Pemerintah Nomor 37 Tahun 2007 tentang Pelaksanaan Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (PP Administrasi Kependudukan), dan Pasal 26 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Selanjutnya disebut UU ITE). Dengan dibentuknya regulasi tersebut tidak hanya memberikan perlindungan hukum kepada para korban tetapi juga secara otomatis mengharuskan adanya sebuah kepastian atas pengelolaan data dan informasi khususnya pada pengelolaan data pribadi karena tanpa dikelolanya data dengan baik dan tepat, maka akan berujung pada

Garry Gumelar Pratama Rosadi, Sinta Dewi, “PERLINDUNGAN PRIVASI DAN DATA PRIBADI DALAM ERA EKONOMI DIGITAL DI INDONESIA,” *VeJ* vo.4 no 1 (2018), Hlm 91.

penyalahgunaan dan serangan kejahatan siber atau *cybercrime*. Oleh karena itu, dibutuhkan analisis manajemen risiko dalam menghadapiserangan kejahatan siber *cybercrime*.

B. METODE PENELITIAN

Tulisan ini menggunakan Metode pendekatan yang digunakan dalam penelitian ini adalah metode yuridis normatif yaitu pengumpulan materi atau bahan penelitian yang ditujukan pada dokumen, Adapun teknik pengumpulan data yang digunakan yaitu penelitian kepustakaan (*library research*), Analisis data yang digunakan merupakan analisis secara kualitatif, yaitu dengan cara menginterpretasikan data dan memaparkan dalam bentuk kalimat untuk menjawab permasalahan.⁵ melalui pembahasan tersebut diharapkan permasalahan tersebut dapat terjawab sehingga memudahkan untuk ditarik kesimpulan dari permasalahan tersebut.⁶

C. HASIL DAN PEMBAHASAN

1. Pengaturan Perlindungan Data Pribadi

Dalam alinea ke-4 Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, menyebutkan Pemerintah Negara Indonesia mempunyai kewajiban konstitusional melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia dan untuk memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi, dan keadilan sosial. Dalam konteks perkembangan teknologi informasi dan komunikasi, tujuan bernegara tersebut diwujudkan dalam bentuk perlindungan data pribadi dari setiap penduduk atau warga negara Indonesia. Secara umum dapat diterima bahwa UUD NRI 1945 selaku Konstitusi memberikan kebijakan dalam menaggulangi pencurian data pribadi dengan cara melindungi kepemilikan pribadi dari para pihak yang mencoba melakukan pembobolan atau pencurian data pribadi milik seseorang dalam media elektronik. Undang-undang sebagai *legal policy* dalam suatu penyelenggaraan pemerintahan demi mencapai tujuan bernegara merupakan instrumen penting dalam negara hukum (*rule of law*). Keadaan yang demikian mengakibatkan munculnya konsekuensi bahwa suatu regulasi yang dibentuk oleh pemerintah merupakan suatu instrumen untuk memberikan perlindungan hukum dan penegakan hak asasi manusia (HAM) bagi warga negara. Sementara di sisi lain, sebagai *politico-legal document*, pembentukan undang-undang

⁵Peter Mahmud Marzuki, *Penelitian Hukum, Edisi Revisi* (Jakarta: Kencana, 2013), Hlm 35.

⁶Zainudin Ali. 2016, *Metode Penelitian Hukum*. Jakarta : Sinar Grafika, hlm 17.

sangat bergantung pada proses politik yang dinamis dan tidak mudah untuk diperkirakan dengan pasti (*unpredictable*) sehingga pembahasan undang-undang sering berjalan berlarut-larut bahkan pembahasannya terpaksa dihentikan karena pergantian jabatan pembentuk undang-undang. Meskipun hal tersebut terkesan bertolak belakang terhadap upaya pemenuhan hak asasi warga negara, tetapi hal tersebut sebetulnya wajar terjadi dalam praktik demokrasi.

Perkembangan terhadap pemanfaatan teknologi informasi pada era globalisasi saat ini mengalami kemajuan yang sangat pesat. Hal demikian berdampak kepada perkembangan pemanfaatan terhadap data pribadi pula. Perkembangan tersebut seperti penyelenggaraan *electronic commerce*(*e-commerce*) dalam sektor perdagangan/bisnis, *electronic education* (*e-education*) dalam bidang pendidikan, *electronic health* (*e-health*) dalam bidang kesehatan, *electronic government*(*e-government*) dalam bidang pemerintahan, *search engines*, *social networks*, *smartphone* dan *mobile internet* serta perkembangan industri komputasi awan atau *cloud computing*. Aktivitas-aktivitas masyarakat virtual dalam memanfaatkan teknologi informasi tersebut sangat bergantung pada ketersediaan (*availability*), keutuhan (*integrity*) dan kerahasiaan (*confidentiality*) informasi di ruang siber.⁷

Banyaknya masyarakat yang menggunakan media elektronik sebagai alat komunikasi memiliki potensi untuk terjadinya pelanggaran terhadap privasi khususnya adalah penyalahgunaan berupa pembobolan atau pencurian data pribadi. Hal tersebut dipengaruhi oleh perilaku atau budaya masyarakat yang senang membagi bagi data serta informasi. Contohnya dari media elektronik seperti telepon seluler yang mengharuskan mengisi data pribadi atau registrasi sebelum menggunakan kartu telepon seluler atau bahkan melalui media elektronik internet di setiap profil pada akun jejaring sosial (seperti *facebook*, *twitter*, *friendster*, *myspace*, dan lain-lain) individu yang bersangkutan selalu mencantumkan data-data pribadinya secara relatif lengkap dan jujur.⁸

Pelindungan terhadap data pribadi berkaitan dengan konsep privasi, konsep privasi sendiri adalah merupakan sebuah gagasan untuk memelihara integritas dan martabat setiap orang secara pribadi. Privasi adalah istilah lain yang kemudian digunakan oleh negara-negara maju yang berkaitan dengan data pribadi sebagai hak yang harus dilindungi, yaitu hak seseorang untuk tidak diganggu kehidupan pribadinya. membahas privasi berarti membahas tentang hak untuk menikmati hidup. Meskipun privasi diakui sebagai hak asasi manusia, sebagai sebuah konsep, sangat sulit untuk mendefinisikan dan bervariasi sesuai dengan konteks, bangsa, dan budaya. Hak privasi melalui pelindungan data merupakan elemen kunci bagi kebebasan dan

⁷Edmon Makarim. Kompilasi Hukum Telematika. Jakarta: PT. Raja Grafindo Perkasa, Hlm 89.

⁸Mohammad Ilham Agung, "HAM Dalam Perkembangan Rule of Law," *Humanitas: Jurnal Kajian dan Pendidikan HAM* vol 6, no. (2015), Hlm 117.

harga diri individu. Pelindungan data menjadi pendorong bagi terwujudnya kebebasan politik, spiritual, keagamaan bahkan kegiatan yang bersifat privat. Hak untuk menentukan nasib sendiri, kebebasan berekspresi dan privasi adalah hak-hak yang penting untuk menjadikan kita sebagai manusia. Potensi pelanggaran hak privasi atas data pribadi tidak saja ada dalam kegiatan online tetapi juga kegiatan offline.⁹ Potensi pelanggaran privasi atas data pribadi secara online misalnya terjadi dalam kegiatan pengumpulan data pribadi secara masal (digital dossier), pemasaran langsung (direct selling), media sosial, pelaksanaan program e-KTP, pelaksanaan program e-health dan kegiatan komputasi awan (cloud computing). Khususnya di era big data, pengumpulan data secara masif lazim dilakukan, tak hanya oleh pemerintah, namun juga oleh entitas bisnis atau korporasi. Jenis data yang dikumpulkan pun beragam, mulai dari personally identifiable information (PII) hingga sensitive personal information (SPI). Perusahaan sebagai pengendali data memiliki tanggung jawab untuk menjaga data konsumen dari kebocoran data. Bocornya data pribadi konsumen merupakan sebuah bentuk pelanggaran terhadap hak atas privasi. Oleh karenanya, diperlukan peraturan hukum yang komprehensif guna melindungi data pribadi konsumen yang dikumpulkan oleh korporasi.

Di Indonesia pelanggaran terhadap penggunaan data pribadi masih kerap terjadi. Semisal dalam dunia perbankan, pertukaran data pribadi dilakukan melalui sistem sharing yaitu bertukar informasi tentang data pribadi nasabah di antara sesama card center, mengungkapkan informasi termasuk transaksi yang berhubungan dengan pemegang kartu kredit kepada pihak ketiga atau diperjual belikan di antara bank sendiri ataupun melalui pihak ketiga, yaitu baik perorangan maupun perusahaan-perusahaan pengumpul data serta memperjualbelikan data pribadi nasabah. Saat ini di Indonesia belum memiliki peraturan perundang-undangan yang secara khusus mengatur mengenai pelindungan data pribadi. Berbagai macam permasalahan di atas menuntut pemerintah Indonesia untuk melindungi masyarakat dan mengatur masalah perlindungan atas data pribadi dan menyiapkan berbagai bentuk perlindungan hukum.¹⁰

Ketentuan hukum terkait pelindungan data pribadi masih bersifat parsial dan sektoral, tampaknya belum bisa memberikan perlindungan yang optimal dan efektif terhadap data pribadi, sebagai bagian dari privasi. Saat ini undang-undang yang digunakan untuk melindungi data pribadi yaitu Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan mengatur tentang rahasia kondisi pribadi pasien, Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan mengatur data pribadi mengenai

⁹Hidayat Chusnul Chotimah, *Tata Kelola Keamanan Siber Dan Diplomasi Siber Di Indonesia Dibawah Kelembagaan Badan Siber Dan Sandi Negara*, Jurnal Politica, vol. 10, N, 2019, Hlm 114

¹⁰Human Rights Committee General Comment No, *On the Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 1988, 17.

nasabah penyimpan dan simpanannya, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 24 Tahun 2013 Tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan, dan Peraturan Pemerintah Nomor 37 Tahun 2007 Tentang Pelaksanaan Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan.

2. Kebijakan Penanggulangan Pencurian Data Pribadi dalam media Elektronik Menurut UU di Indonesia.

Ketentuan mengenai kebijakan penanggulangan data pribadi dengan cara memberikan perlindungan hal ini merupakan amanah Pasal 28 G Undang-Undang Dasar Republik Indonesia Tahun 1945 (UUD) yang mengatur hak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya. Untuk dapat melihat ketentuan tersebut sebagai ketentuan mengenai privasi dan data pribadi, pendapat Warren dan Brandeis dalam karyanya yang berjudul *"The Right to Privacy"* menyatakan bahwa privasi adalah hak untuk menikmati kehidupan dan hak untuk dihargai perasaan dan pikirannya.

Hak privasi dan data pribadi menjadi hak yang memiliki karakter internasional dalam ketidakjelasan statusnya dalam perlindungan hukum nasional. Dalam perlindungan hukum nasional terdapat dua hal yang dapat diperdebatkan. Privasi di satu sisi merupakan hak yang membuat adanya jarak antara individu dan masyarakat. Undang Undang Republik Indonesia No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang Republik Indonesia Nomor 11 Tahun 2011. tentang Informasi dan Transaksi Elektronik (Selanjutnya disebut "UU ITE"), meliputi perlindungan dari penggunaan tanpa izin, perlindungan oleh penyelenggara sistem elektronik, dan perlindungan dari akses ilegal. Terkait penanggulangan pencurian data pribadi melalui sarana penal yaitu dengan memberikan perlindungan kepada data pribadi dari penggunaan atau pemanfaatan tanpa izin. Pasal 26 UU ITE mensyaratkan bahwa penggunaan setiap data pribadi dalam sebuah media elektronik harus terlebih dahulu mendapatkan persetujuan pemilik data bersangkutan. Setiap orang yang melanggar ketentuan ini dapat digugat atas kerugian yang ditimbulkan. Ketentuan Pasal 26 UU ITE adalah sebagai berikut :

- a. 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.
- b. Setiap orang yang melanggar haknya sebagaimana yang dimaksud pada ayat 1 dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan undang-undang ini.

- c. Setiap penyelenggara sistem elektronik wajib menghapus informasi elektronik dan/atau dokumen elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan orang yang bersangkutan berdasarkan penetapan pengadilan.
- d. Setiap penyelenggara sistem elektronik wajib menyediakan mekanisme penghapusan informasi elektronik dan/atau dokumen elektronik yang tidak relevan sesuai dengan ketentuan peraturan perundang-undangan.
- e. Ketentuan mengenai tata cara penghapusan informasi elektronik dan/atau dokumen elektronik sebagaimana dimaksud pada ayat (3) dan ayat (4) diatur dalam peraturan pemerintah.

Berdasarkan ketentuan dari Pasal 26 UU ITE yang berkaitan dengan data pribadi yang telah disampaikan diatas pemerintah melarang setiap penyelenggara sistem elektronik menggunakan atau menafatkan data milik orang lain tanpa persetujuan dari si pemilik data tersebut. Berdasarkan isi dari pasal tersebut artinya aktivitas-aktivitas seperti pengumpulan dan penyebarluasan data pribadi merupakan pelanggaran terhadap privasi seseorang karena hak privasi mencakup hak menentukan memberikan atau tidak memberikan data pribadi. Termasuk didalamnya pencurian data pribadi, ketika pihak penyelenggara elektronik menggunakan data pribadi milik orang lain, bentuk larangan tersebut tidak lain karena pandangan pemerintah menganggap bahwa data pribadi merupakan suatu aset atau komoditi bernilai ekonomi tinggi.

C. PENUTUP

Dari analisis yang disampaikan oleh penulis maka, kesimpulan yang dapat diambil adalah: Pengaturan perlindungan data pribadi merupakan hal yang penting saat ini karena berbagai permasalahan muncul sering dengan meningkatnya penggunaan terhadap data pribadi pada transaksi berbasis teknologi informasi di berbagai aspek kehidupan. Namun, sampai saat ini masih belum terdapat pengaturan yang secara khusus memberikan perlindungan bagi masyarakat atas berbagai persoalan-persoalan yang berkaitan dengan penyalahgunaan data pribadi dalam proses pemanfaatan teknologi informasi. Pengaturan terkait dengan perlindungan data pribadi yang tersebar dalam beberapa Undang-Undang di Indonesia seperti Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan mengatur tentang rahasia kondisi pribadi pasien, Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan mengatur data pribadi mengenai nasabah penyimpan dan simpanannya, Undang-Undang Nomor 19

Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 24 Tahun 2013 Tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan, dan Peraturan Pemerintah Nomor 37 Tahun 2007 Tentang Pelaksanaan Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan. Perlu untuk dilakukan kovergensi yaitu menyatukan beberapa undang-undang tersebut menjadi satu undang-undang yang secara khusus membahas tentang perlindungan hukum pada data pribadi.

DAFTAR PUSTAKA/DAFTAR REFERENSI

Buku:

Edmon Makarim. *Kompilasi Hukum Telematika*. Jakarta: PT. Raja Grafindo Perkasa.

Peter Mahmud Marzuki, *Penelitian Hukum, Edisi Revisi* (Jakarta: Kencana, 2013).

Zainudin Ali. *Metode Penelitian Hukum*. Jakarta : Sinar Grafika, 2016.

Jurnal:

Brisilia Tumulun, "Upaya Penanggulangan Kejahatan Komputer Dalam Sistem Elektronik Menurut Pasal 30 Undang-Undang Nomor 11 Tahun 2008," *Jurnal Lex Et Societatis* 6, No. 2 (2018).

Dian Ekawati, "Perlindungan Hukum Terhadap Nasabah Bank Yang Dirugikan Akibat Kejahatan Skimming Ditinjau Dari Perspektif Teknologi Informasi Dan Perbankan," *Jurnal Unes Law Review* 1, No. 2 (2018).

Garry Gumelar Pratama Rosadi, Sinta Dewi, "PERLINDUNGAN PRIVASI DAN DATA PRIBADI DALAM ERA EKONOMI DIGITAL DI INDONESIA," *VeJ* vo.4 no 1 (2018).

Hidayat Chusnul Chotimah, *Tata Kelola Keamanan Siber Dan Diplomasi Siber Di Indonesia Dibawah Kelembagaan Badan Siber Dan Sandi Negara*, *Jurnal Politica*, vol. 10, N, 2019.

Human Rights Committee General Comment No, *On the Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 1988

- Lauder Siagian, Arief Budiarto, Dan Simatupang, "Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional," *Jurnal Prodi Perang Asimetris*, Vol. 4, No (2018).
- Mohammad Ilham Agang, "HAM Dalam Perkembangan Rule of Law," *Humanitas: Jurnal Kajian dan Pendidikan HAM* vol 6, no. (2015)