

**PERLINDUNGAN DATA DAN INFORMASI PRIBADI MELALUI
INDONESIAN DATA PROTECTION SYSTEM (IDPS)****Ririn Aswandi¹, Putri Rofifah Nabilah Muchsin², Muhammad Sultan³**¹ *Fakultas Hukum Universitas Hasanuddin. E-mail: ririnaswandi20@gmail.com*² *Fakultas Hukum Universitas Hasanuddin. E-mail:
putrimuchsin1311@gmail.com*³ *Fakultas Hukum Universitas Hasanuddin. E-mail: muhammdsultn@gmail.com***Abstract**

The presence of cybercrime has been a threat to human life, making it difficult for governments to keep up with computer technology, particularly the internet. This is the result of rapid developments in information technology, so each development essentially has both a positive and negative impact. One negative effect is the misuse of data and personal information. The human world's weaknesses are not notwithstanding the lack of regulation or no regulation on cybersecurity and personal data protection, resulting in confusion among members of society. Therefore, a system that addresses this problem requires, the Indonesian Data Protection System (IPDS) I a system that guarantees and provides personal data and information management security/ it aims to know how to manage personal information data in Indonesia today, and to learn how formulations for data management and personal information via Indonesian Data Protection System (IPDS) as a cyber surveillance and data protection effort, the study adopted a normative juridical method with the State Approach. To this issue, the authors concluded, first, that it would require a rule relating to cybercrime as well as protection data and personal information in Indonesia. Second, there is a system that will address the problem of cybercrime especially in the field of data management and personal information of the Indonesian Data Protection System (IPDS).

Keywords: *Indonesian Data Protection System (IPDS); Cyber Crime; Personal Information and Data Protection;*

Abstrak

Adanya Kejahatan Siber (*cybercrime*) telah menjadi ancaman diberbagai kehidupan manusia, sehingga pemerintah sulit mengimbangi teknik kejahatan yang dilakukan dengan teknologi komputer, khususnya jaringan internet. Hal ini merupakan akibat dari pesatnya perkembangan teknologi informasi, sehingga setiap perkembangan pada hakikatnya membawa dampak yang positif maupun negatif. Salah satu dampak negatifnya adalah adanya penyalahgunaan data dan informasi pribadi. Kelemahan dunia siber tidak terlepas dari kurangnya pengaturan atau belum adanya regulasi mengenai keamanan siber dan perlindungan data pribadi, sehingga menimbulkan kerancuan ditengah-tengah anggota masyarakat. Oleh karena itu, dibutuhkan sebuah sistem yang mampu mengatasi

masalah tersebut, sistem Indonesia *Data Protection System* (IDPS) adalah sebuah sistem yang menjamin serta memberikan keamanan pengelolaan data dan informasi pribadi. Penelitian ini bertujuan untuk mengetahui bagaimana Problematika Pengelolaan data informasi pribadi di Indonesia saat ini, dan untuk mengetahui bagaimana formulasi pengelolaan data dan informasi pribadi melalui *Indonesian Data Protection System* (IDPS) Sebagai Upaya *Cyber Surveillance and Data Protection*. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan peraturan perundang-undangan (*Statute Approach*). Terhadap isu ini, penulis menyimpulkan, Pertama, dibutuhkan sebuah peraturan yang berkaitan dengan kejahatan dunia maya (*cybercrime*) dan juga perlindungan data dan informasi pribadi di Indonesia. Kedua, dibutuhkan sebuah sistem yang mampu mengatasi permasalahan kejahatan dunia maya khususnya dibidang pengelolaan data dan informasi pribadi yaitu *Indonesian Data Protection System* (IDPS).

Kata Kunci: *Indonesian Data Protection System; Kejahatan Sibern (Cybercrime); Perlindungan Data dan Informasi Pribadi;*

1. 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.¹ Perkembangan 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.² 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.³ Informasi sudah dianggap sebagai “*power*” yang diartikan sebagai kekuatan dan kekuasaan yang sangat menentukan nasib manusia

¹Brisilia Tumulun, 2018, Upaya Penanggulangan Kejahatan Komputer Dalam Sistem Elektronik Menurut Pasal 30 Undang-Undang Nomor 11 Tahun 2008, *Jurnal Lex Et Societatis* Vol. 6, No. 2, Halaman 24.

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

³A. Aco Agus dan Riskawati, 2016, Penanganan Kasus Cybercrime di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar), *Jurnal Supremasi*, Vol. 10, No. 1, Halaman 20.

itu sendiri.⁴ Saat ini ketergantungan masyarakat akan teknologi informasi semakin tinggi sehingga semakin tinggi pula resiko yang dihadapi.⁵

Seiring perkembangan teknologi internet, mengakibatkan munculnya kejahatan baru yang disebut dengan *new cybercrime* melalui jaringan internet. Munculnya beberapa kasus *cybercrime* di Indonesia, seperti penipuan, *hacking*, penyadapan data orang lain, *spamming email*, dan manipulasi data dengan program komputer untuk mengakses data milik orang lain.

Meningkatnya kejahatan dengan menggunakan teknologi informasi teridentifikasi sejak tahun 2003, sebagai contoh 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*).⁶ Selain itu salah satu potensi kejahatan pada perkembangan teknologi dan informasi juga pada sektor pengelolaan data dan informasi khususnya pada pengelolaan data pribadi yang membutuhkan perlindungan data. Kemajuan teknologi informasi dan komunikasi membuat batas privasi makin tipis. Berbagai data-data pribadi semakin mudah tersebar.⁷

Perlindungan data secara umum pengertiannya mengacu pada praktik, perlindungan, dan aturan mengikat yang diberlakukan untuk melindungi informasi pribadi dan memastikan bahwa subjek data tetap mengendalikan informasinya. Singkatnya, pemilik data harus dapat memutuskan apabila ingin membagikan

⁴ Lauder Siagian, Arief Budiarto, Dan Simatupang, 2018, Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional, *Jurnal Prodi Perang Asimetris*, Vol. 4, No. 3, Halaman 2.

⁵ Darmawan Napitupulu, 2017 Kajian Peran Cyber Law Dalam Memperkuat Keamanan Sistem Informasi Nasional, *Deviance Jurnal Kriminologi*, Vol. 1 No. 1, halaman 102

⁶ Maulia Jayantina Islami, 2017, Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index, *Jurnal Masyarakat Telematika Dan Informasi*, Vol. 8 No. 2, Halaman 137.

⁷ Normand Edwin Elnizar, 2019, *Perlindungan Data Pribadi Tersebar di 32 UU, Indonesia Perlu Regulasi Khusus*, [online] tersedia di: <https://www.hukumonline.com/berita/baca/lt5d1c3962e01a4/perlindungan-data-pribadi-tersebar-di-32-uu--indonesia-perlu-regulasi-khusus/> (Diakses Pada 22 November 2019).

beberapa informasi atau tidak, siapa yang memiliki akses, untuk berapa lama, untuk alasan apa.⁸

Berdasarkan Pasal 79⁹ Ayat (1) Undang-Undang Nomor 24 Tahun 2013 Tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan (selanjutnya disebut UU Administrasi Kependudukan), Pasal 58¹⁰ Peraturan Pemerintah Nomor 37 Tahun 2007 Tentang Pelaksanaan Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan (selanjutnya disebut PP Administrasi Kependudukan), dan Pasal 26 ayat (1)¹¹ Undang-Undang No. 19 tahun 2016 Tentang Perubahan Atas Undang Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Selanjutnya disebut UU ITE).

Adanya regulasi tersebut 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 penyalahgunaan dan serangan kejahatan siber atau *cybercrime*. Oleh karena itu, dibutuhkan analisis manajemen risiko dalam menghadapi serangan kejahatan siber *cybercrime*.¹² resiko kejahatan siber (*cybercrime*) berpotensi terhadap kehilangan sistem informasi data,¹³ dan menyebabkan sulitnya seseorang dalam mengatasi masalah tersebut. Hal ini disebabkan belum adanya lembaga atau penegak hukum yang bisa memproses itu.¹⁴ Kejahatan terhadap penyalahgunaan data pribadi seseorang sering kali ditemukan pada sebuah perusahaan, karena tidak mengetahui bagaimana data tersebut dikelola dan diamankan secara tepat.

⁸ Wahyudi Djafar, 2019, *Hukum Perlindungan Data Pribadi Di Indonesia: Lanskap, Urgensi, Dan Kebutuhan Pembaharuan*, Halaman 5.

⁹ Pasal 79 ayat (1) UU Administrasi Kependudukan, (1) Data Perseorangan dan dokumen kependudukan wajib disimpan dan dilindungi kerahasiaannya oleh Negara.

¹⁰ Pasal 58 PP Administrasi Kependudukan, Instansi pemerintah dan swasta sebagai pengguna data pribadi penduduk, dilarang menjadikan data pribadi penduduk sebagai bahan informasi publik.

¹¹ Pasal 26 Ayat (1) UU ITE, (1) kecuali ditentukan lain oleh peraturan perundang undangan setiap informasi melalui media elektronik yang menyangkit data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan

¹² Ineu Rahmawati, 2017, Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cybercrime) Dalam Peningkatan Cyber Defense, *Jurnal Pertahanan & Bela Negara*, Vol. 7, No. 2, Halaman 53.

¹³ *Ibid.*, Halaman 56.

¹⁴ Murti Ali Lingga, 2019, *Penyalahgunaan Data Pribadi Konsumen Sudah Masuk Kategori Gawat Darurat*, [online] tersedia di: <https://money.kompas.com/read/2019/07/27/201200426/penyalahgunaan-data-pribadi-konsumen-sudah-masuk-kategori-gawat-darurat?page=all> (Diakses Pada 22 November 2019).

Perusahaan perlu memahami regulasi, prinsip-prinsip, serta praktik perlindungan data pribadi.¹⁵ Sehingga data dan informasi seseorang tidak disalahgunakan oleh pihak yang tidak bertanggung jawab. Belum adanya sebuah regulasi mengenai perlindungan data pribadi sehingga menyebabkan banyaknya kejahatan penyalahgunaan sistem informasi dan data pribadi, maka dari itu dibutuhkan sebuah sistem yang mampu mengatasi hal tersebut.

Secara khusus penulisan ini diharapkan dapat menjadi rekomendasi bagi pemerintah dalam hal melindungi data dan informasi pribadi melalui *Indonesian Data Protection System (IDPS)* sebagai *Upaya Cyber Surveillance and Data Protection*.

Tujuan objektif dari penulisan ini adalah: *pertama*, untuk mengetahui bagaimana Problematika Pengelolaan data informasi pribadi di Indonesia saat ini. *Kedua*, bagaimana formulasi perlindungan data dan informasi pribadi melalui *Indonesian Data Protection System (IDPS)* Sebagai *Upaya Cyber Surveillance and Data Protection*.

2. Analisis

2.1 Pengelolaan Data dan Informasi Pribadi di Indonesia

Perkembangan teknologi informasi komunikasi berbasis komputer telah berkembang sangat pesat di masyarakat. Masyarakat kemudian dimudahkan dengan perkembangan teknologi tersebut.¹⁶ Salah satu kemudahan teknologi yang dirasakan masyarakat adalah dengan adanya internet. Penggunaan internet dalam berbagai bidang kehidupan tidak saja membuat segala sesuatunya menjadi lebih mudah, namun juga memunculkan sejumlah permasalahan termasuk dalam bidang hukum. Salah satu masalah hukum yang dapat muncul yakni berkaitan dengan perlindungan data pribadi (*the protection of privacy rights*).

¹⁵ Lembaga Studi dan Advokasi masyarakat, Pentingnya Melindungi Data Pribadi bagi Perusahaan [online] tersedia di: <https://elsam.or.id/pentingnya-melindungi-data-pribadi-bagi-perusahaan/> (Diakses Pada 22 November 2019).

¹⁶ Nani widya sari, 2018, kejahatan cyber dalam perkembangan teknologi informasi berbasis komputer, *jurnal surya kencana dua: dinamika masalah hukum dan keadilan*, Vol. 5, No. 2, Halaman 578.

Interaksi masyarakat digital dalam menggunakan internet sangat bergantung pada ketersediaan (*availability*), keutuhan (*integrity*) dan kerahasiaan (*confidentiality*) informasi di ruang siber,¹⁷ sebagai contoh apabila seseorang melakukan transaksi atau pendaftaran di suatu organisasi atau *mailing list* di internet, maka yang bersangkutan harus mengirimkan data-data pribadi tertentu.¹⁸ Adapun kasus-kasus pencurian data di Indonesia adalah sebagai berikut:

1. Kasus Pembobolan atau Pencurian Data Pribadi

Kasus pembobolan dan kebocoran data dan informasi merupakan problematika yang sedang terjadi di Indonesia, berikut beberapa contoh kasusnya:

Tabel 1. Beberapa Kasus Pembobolan atau Pencurian Data Pribadi

No.	Kasus	Jumlah Penyalahgunaan data	Tahun
1.	Kasus pembobolan <i>Sony Corp</i> ,	Kelompok hacker membobol jaringan playstation <i>Sony</i> dan mencuri data lebih dari 77 juta <i>account</i> .	2011 ¹⁹
2.	Kasus pembobolan data pribadi Telkomsel.	Diperkirakan 25 juta pelanggan Telkomsel	2011 ²⁰
3.	Kasus pencurian data pribadi	Pencurian data sebanyak 945 kasus	2018 ²¹
4.	Kasus pencurian data pribadi	Mencapai 1.162 kasus	2017 ²²

¹⁷ Hidayat Chusnul Chotimah, 2019, Tata Kelola Keamanan Siber Dan Diplomasi Siber Di Indonesia Dibawah Kelembagaan Badan Siber Dan Sandi Negara, *Jurnal politica*, Vol. 10, No. 2, Halaman 114.

¹⁸ Rosalinda Elsina Latumahina, 2014, *Aspek Hukum Perlindungan Data Pribadi Di Dunia Maya*, *Jurnal Gema Aktualita*, Vol. 3 No. 2, Halaman 14.

¹⁹ *Ibid.*

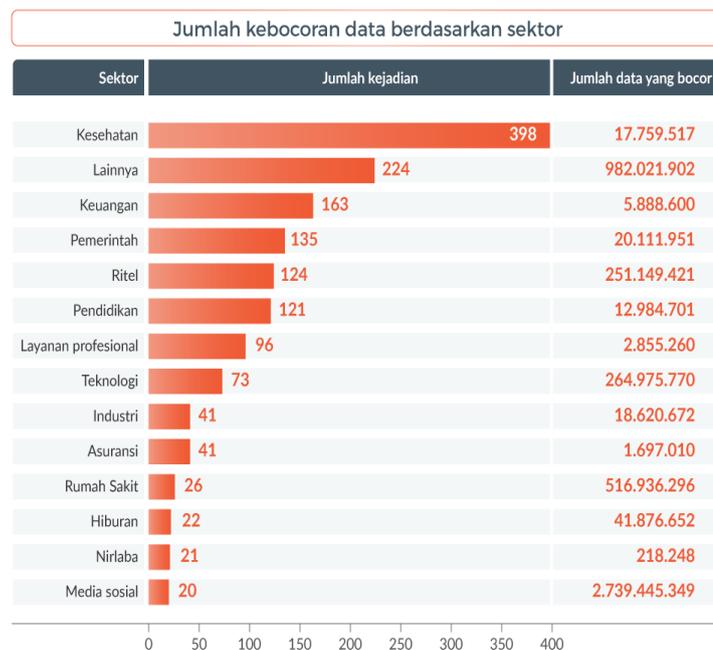
²⁰ *Ibid.*

²¹ Liputan6.com, 2018, *4,5 Miliar Data Dicuri Selama 6 Bulan Pertama 2018*, [online] tersedia di: <https://www.liputan6.com/tekno/read/3665291/45-miliar-data-dicuri-selama-6-bulan-pertama-2018> (Diakses Pada 13 Desember 2019).

²² *Ibid.*

5.	Lion Air Group	Diperkirakan 7,8 juta Data Penumpang	2018 ²³
----	----------------	--------------------------------------	--------------------

Selain itu, Gemalto melaporkan, jumlah data yang dibobol perharinya mencapai 6,9 juta data. Hal ini berdasarkan laporan pencurian data sejak 2013 hingga 2018 yang jumlahnya sebanyak 14,6 miliar, dan hanya 4 persen dari jumlah tersebut yang dilindungi enkripsi oleh pemiliknya. Jika dihitung secara statistik, jumlah data yang hilang paling banyak berasal dari perusahaan media sosial sebanyak 56,11 persen diikuti dengan data milik instansi pemerintah dengan persentasi 26,62 persen dari keseluruhan data yang dibobol.²⁴ Selain itu jumlah kebocoran data berdasarkan sektor pada 2018 sebagai berikut:



Tabel 2. Jumlah Kebocoran Data di Berbagai Sektor Tahun 2018

Sistem keamanan data pribadi pengakses dunia maya pernah menjadi sorotan. *Digital Forensic Indonesia* (DFI) menduga ada sekitar 7.5 miliar

²³ Agustin Setyo Wardani, 2019, Malindo: *Kebocoran Data Gara-Gara Mantan Staf Perusahaan Kontraktor*, <https://www.liputan6.com/teknologi/read/4069498/malindo-kebocoran-data-gara-gara-mantan-staf-perusahaan-kontraktor> (Diakses Pada 13 Desember 2019).

²⁴ Liputan6.com, *Op. Cit.*

data pribadi pengguna internet di seluruh dunia diretas pihak ketiga dalam 15 tahun terakhir. Ratusan juta di antaranya milik pengakses asal Indonesia. Sumber kebocoran data di seluruh sektor tersebut berasal dari peretasan pihak luar (*malicious outsider*) dan pihak dalam (*malicious insider*), kebocoran data yang tak disengaja akibat sistem tak aman (*accidental loss*), *hacktivist*, gawai atau ponsel yang raib, perangkat pemeras (*ransomware*), dan beragam sumber yang tidak dapat diketahui. Peretasan data pengguna bisa terjadi jika sistem perlindungan data dalam situs tersebut tidak ketat. Akibatnya, data pribadi bisa diperjualbelikan. Padahal, jaminan perlindungan data sudah diatur dalam Pasal 15 ayat (1) UU ITE, yang mengharuskan setiap penyelenggara sistem elektronik untuk menjaga keamanan platform.²⁵

2. Kasus Jual Beli Data dan Informasi Pribadi

Data dan informasi pribadi merupakan hal harus dilindungi dan disimpan secara ketat agar tidak terjadi kasus peretasan ataupun penjualan data pribadi dan informasi yang dilakukan oleh pihak ataupun orang yang tidak bertanggungjawab, berikut sebagian kecil kasus-kasus penjualan data dan informasi pribadi yang terjadi di Indonesia:

Tabel 3. Beberapa Kasus Jual Beli Data Pribadi

No	Pihak Penjual/Tempat Penjualan	Jenis Data dan informasi Pribadi yang diperjualbelikan	Tahun
1.	Data dan informasi seseorang diperjualbelikan melalui group media sosial <i>facebook</i> “ <i>Dream Market Official</i> ”.	diketahui menyimpan jutaan data pribadi warga negara Indonesia yang terdiri dari 761.435 nomor ponsel, 129.421 kartu kredit,	2019 ²⁶

²⁵ Rommy Roosyana, 2019, *Pemerintah mestiindungi privasi dan data pribadi warganya*, [online] tersedia di: <https://beritagar.id/artikel/berita/pemerintah-mesti-lindungi-privasi-dan-data-pribadi-warganya> (Diakses Pada 13 Desember 2019).

²⁶ Kompas.com, 2019, *Polri: Kasus Jual-Beli Data Pribadi di Web Berbeda dengan di Grup Facebook*, [online] tersedia di: <https://nasional.kompas.com/read/2019/08/16/08272631/polri-kasus-jual-beli-data-pribadi-di-web-berbeda-dengan-di-grup-facebook?page=all> (Diakses Pada 13 Desember 2019).

LEGISLATIF

(LEMBARAN GAGASAN MAHASISWA YANG SOLUTIF DAN INOVATIF)
LEMBAGA PENALARAN DAN PENULISAN KARYA ILMIAH
FAKULTAS HUKUM UNIVERSITAS HASANUDDIN

		1.162.864 Nomor Induk Kependudukan (NIK), 50.854 Nomor Kartu Keluarga (KK), dan 64.164 nomor rekening	
2	Melalui akun twitter @hendralm. Data pribadi yang diperjualbelikan berupa NIK dan KK hingga foto <i>selfie</i> .	Data (KK) dan Data NIK (Nomor Induk Kependudukan)	2019 ²⁷
	Penjualan data ditemukan di aplikasi belanja online besar yakni Tokopedia dan Bukalapak.	Data terbagi atas 75.824 data nasabah deposito, dan 64.769 data nasabah kartu kredit.	2019 ²⁸
4.	Pelaku berinisial C mengumpulkan data nasabah dari marketing bank dan marketing institusi keuangan lainnya.	Data pribadi dan Informasi nasabah bank, Data yang dijual berisi informasi nama, nomor telepon, alamat, hingga nama orangtua. Namun, ada juga yang dilengkapi dengan informasi kemampuan finansial pemiliknya.	2019 ²⁹

²⁷ CNN Indonesia, 2019, *kemendagri adu jual beli data pribadi ke polisi di apresiasi*, [online] tersedia di: <https://www.cnnindonesia.com/teknologi/20190731182440-185-417177/kemendagri-adu-jual-beli-data-pribadi-ke-polisi-diapresiasi> (Diakses Pada 13 Desember 2019).

²⁸ Kompas.com, 2019, *Data Pribadi Nasabah Juga Dijual Secara Online, Jumlahnya Jutaan*, [online] tersedia di: <https://money.kompas.com/read/2019/05/13/120800426/data-pribadi-nasabah-juga-dijual-secara-online-jumlahnya-jutaan-?page=all>. (Diakses Pada 13 Desember 2019).

²⁹ Kompas.com, 2019, *"Data Pribadi Dijual Bebas, dari Gaji hingga Info Kemampuan Finansial"*, [online] tersedia di: <https://money.kompas.com/read/2019/05/13/081753626/data-pribadi-dijual-bebas-dari-gaji-hingga-info-kemampuan-finansial?page=all>. (Diakses Pada 13 Desember 2019).

Identifikasi penulis mengenai problematika pengelolaan data dan informasi pribadi menunjukkan bahwa *pertama*, kasus pembobolan atau pencurian data dan informasi pribadi di Indonesia merupakan hal yang harus menjadi perhatian pemerintah Indonesia, karena dengan melalui kebocoran ataupun pembobolan data dan informasi seseorang, maka pihak-pihak yang tidak bertanggungjawab akan menyalahgunakan data dan informasi pribadi seseorang tersebut. Kejadian pembobolan atau pencurian data pribadi dikarenakan lemahnya pengawasan dan juga sebagai perusahaan maupun instansi pemerintah tidak mengetahui bagaimana semestianya mengelola data yang baik dan juga mengamankannya. *Kedua*, kasus penjualan data pribadi seseorang seperti data kependudukan menunjukkan bahwa pengelolaan data dan informasi tidak dikelola, diawasi, dan disimpan dengan baik dan aman. Data pribadi yang seharusnya disimpan dan dilindungi dengan baik, justru beberapa oknum yang memperjual belikan data dengan bebas mulai dari Nomor Induk Kependudukan (NIK), KTP elektronik (KTP-el) dan Kartu Keluarga (KK).

Penjualan data secara online ini merupakan penghasilan bagi para telemarketer dan pelaku kejahatan. Mereka bisa mendapatkan data valid nasabah bank dengan mudah dan murah untuk kepentingan pekerjaan. Bagi telemarketing, data pribadi digunakan untuk menawarkan produk bank atau asuransi. Ini sebabnya banyak nasabah kartu kredit yang kemudian kerap mendapatkan telepon tawaran produk bank atau asuransi.³⁰ Kasus pembobolan dan penjualan data dan informasi pribadi akan terus terjadi jika pengelolaan data dan informasi itu tidak ada yang memastikan pengelolaannya dan tidaknya pusat penyimpanan data atau yang mengamankan semua data yang ada di Indonesia sehingga dengan mudah disalahgunakan oleh orang yang tidak bertanggungjawab.

Kebebasan perusahaan swasta mengakses informasi melalui data yang tertera di Kartu Tanda Penduduk (KTP). Direktorat Jenderal Kependudukan dan Pencatatan Sipil (Dukcapil) memberikan akses Nomor Induk

³⁰ Mawa Kresna, 2019, *Bagaimana Data Nasabah Kartu Kredit Diperjualbelikan*, [online] tersedia di: <https://tirto.id/bagaimana-data-nasabah-kartu-kredit-diperjualbelikan-djSv> (Diakses Pada 13 Desember 2019).

Kependudukan (NIK) dan KTP kepada swasta yang diajak bekerjasama. Data itu diklaim digunakan untuk menunjang layanan perusahaan tersebut. Beberapa riset membuktikan bahwa kesadaran masyarakat Indonesia terhadap perlindungan data personal mereka di internet masih rendah. Akibatnya masyarakat Indonesia kurang menanggapi secara serius kasus pelanggaran terhadap perlindungan data personal ini.³¹ Belum adanya regulasi atau aturan tentang kejahatan siber dan juga kejahatan pada penyalahgunaan data dan informasi pribadi merupakan salah satu penyebab tingginya kasus penyalahgunaan data dan informasi di Indonesia. Pemerintah perlu mempertimbangkan pengamanan pada infrastruktur informasi dan ekonomi digital. Upaya perlindungan dan proteksi juga perlu digerakkan.³²

Berdasarkan analisis penulis mengenai problematika tentang kasus-kasus kejahatan diatas menunjukkan bahwa sektor pengelolaan data dan informasi pribadi di Indonesia saat ini sangat rentan terhadap kejahatan pencurian/pembobolan ataupun jual beli data dan informasi pribadi hal ini semakin diperburuk karena belum adanya regulasi yang mengatur tentang perlindungan data dan informasi di Indonesia. Sehingga untuk mengatasi masalah tersebut maka dibutuhkan sebuah sistem yang mengatur mengenai pengelolaan data dan informasi di Indonesia.

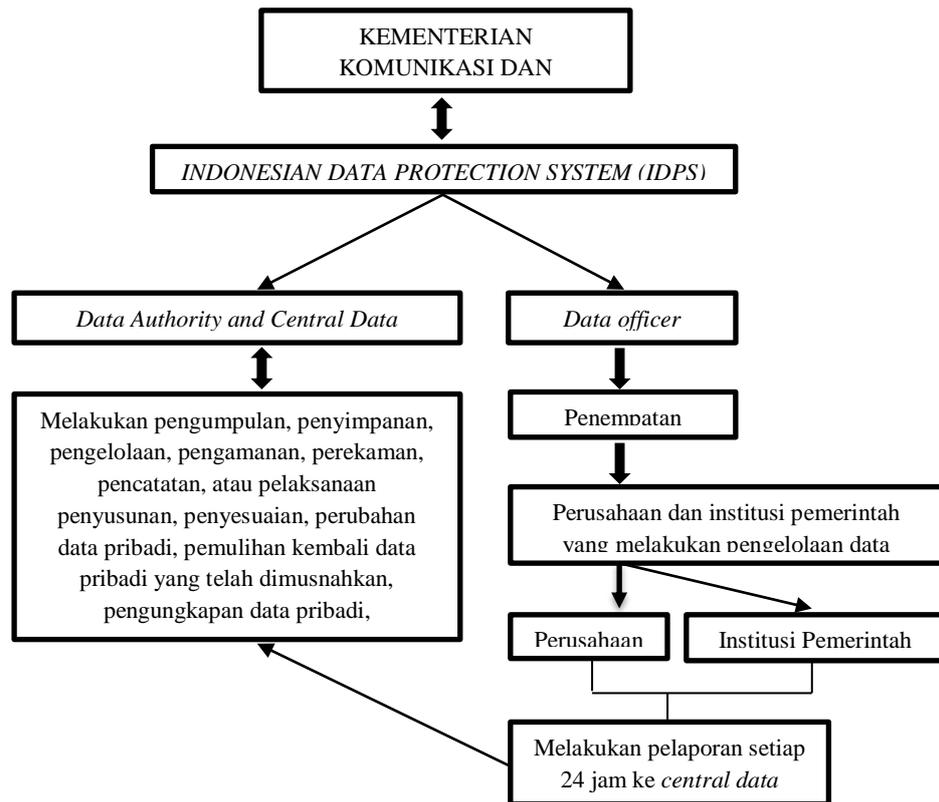
2.2 Mekanisme Penerapan Konsep *Indonesian Data Protection System (IDPS)* Melalui Pengelolaan Data dan Informasi Sebagai Upaya *Cyber Surveillance and Data Protection*

Indonesia Data Protection System (IDPS) merupakan sebuah sistem yang mampu meminimalisasi kejahatan siber khususnya pada penyalahgunaan data dan informasi pribadi. Sistem ini bekerja untuk

³¹ Dewa Ayu Diah Angendari, 2019, *Kasus data Dukupil: Pelajaran terkait privasi dan data pribadi di Indonesia*, [online] tersedia di: dari <http://theconversation.com/kasus-data-dukupil-pelajaran-terkait-privasi-dan-data-pribadi-di-indonesia-121264> (Diakses Pada 14 Desember 2019).

³² Tirto.id, 2019, *UU ITE Dinilai Belum Cukup Lawan Kejahatan Siber*, [online] tersedia di: <https://tirto.id/uu-ite-dinilai-belum-cukup-lawan-kejahatan-siber-dgqU> (Diakses Pada 14 Desember 2019).

mengamankan data pribadi seseorang pada *central data* atau pusat pengumpulan data, selain itu IDPS juga memastikan pengelolaan data dan informasi seseorang dikelola dengan tepat, dengan adanya sebuah koordinasi dari sistem ini. Berikut adalah bagan mengenai kerja IDPS sebagai sebuah sistem.



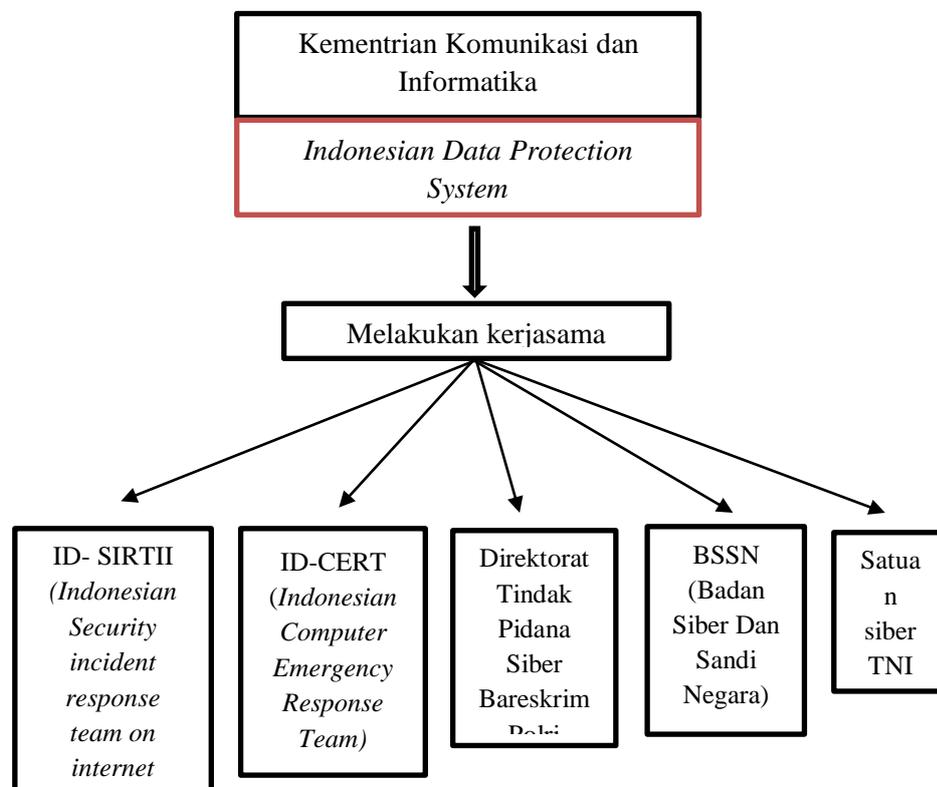
(Gambar 1: Skema Sistem IDPS)

Sistem IDPS ini dilekatkan kepada Kementerian Komunikasi dan Informatika (Kominfo) yang dimana IDPS mempunyai dua unsur yang sangat penting atau *urgent*, yaitu *central data* atau *data authority* serta *data officer*. *Central data* atau *data authority* fungsinya adalah untuk mengumpulkan dan mengamankan setiap data dan informasi pribadi yang masuk dari *data officer*, maka dari itu *data officer* ditempatkan pada seluruh perusahaan dan instansi pemerintahan yang melakukan pengelolaan data dan informasi pribadi agar lebih mudah untuk melakukan koordinasi terkait

dengan data dan informasi pribadi yang dimiliki seseorang.

Central data atau *data authority* merupakan tempat ataupun pusat penyimpanan data dan hanya dikelola oleh orang yang memiliki kewenangan untuk melakukan pengelolaan data dan informasi pribadi tersebut, *central data* juga harus memiliki keamanan yang sangat ketat karena merupakan tempat utama penyimpanan data. Sedangkan *data officer* merupakan orang-orang yang mempunyai kewenangan dan keahlian yang ditunjuk oleh *central data* atau *data authority* untuk melakukan pengelolaan data dan informasi pribadi pada setiap perusahaan dan instansi pemerintah, yang kemudian dalam pekerjaannya ini harus melakukan koordinasi tentang pengelolaan data dan informasi pribadi yang dikelola sekali dalam 24 jam, agar *central data* mempunyai informasi yang *up to date* terhadap pengelolaan data pribadi oleh perusahaan dan instansi pemerintah. Melihat pekerjaan yang sangat sulit oleh seseorang *data officer*, maka dari itu harus memiliki kualifikasi tersendiri agar sumber daya manusia yang bekerja sebagai *data officer* adalah orang-orang yang berkompeten dan seseorang yang profesional, orang-orang yang bekerja dalam bidang privasi dan perlindungan data harus memiliki keahlian yang sama baik dalam hukum dan teknologi keamanan siber untuk membantu perusahaan dan instansi pemerintah mengatur penyimpanan, pemrosesan, serta perlindungan data digital yang sesuai dengan undang-undang.

IDPS sebagai sebuah sistem yang dilekatkan pada Kominfo, untuk mendukung kinerja dari sistem ini juga perlu adanya kerjasama terhadap badan atau pun tim yang sudah dibentuk oleh pemerintah sebelumnya, kerjasama ini dilakukan untuk mewujudkan adanya *cyber surveillance* dan perlindungan data terhadap data dan informasi seseorang yang sedang diproses, fungsi dari adanya kerjasama ini adalah untuk lebih meningkatkan ketahanan dari IDPS itu sendiri yang nantinya akan menjadi pusat pengelolaan data pribadi dan sebagai pusat kontrol data pribadi seseorang yang dilaporkan oleh *data officer*. Adapun bagan mengenai mekanisme kerjasamanya sebagai berikut:



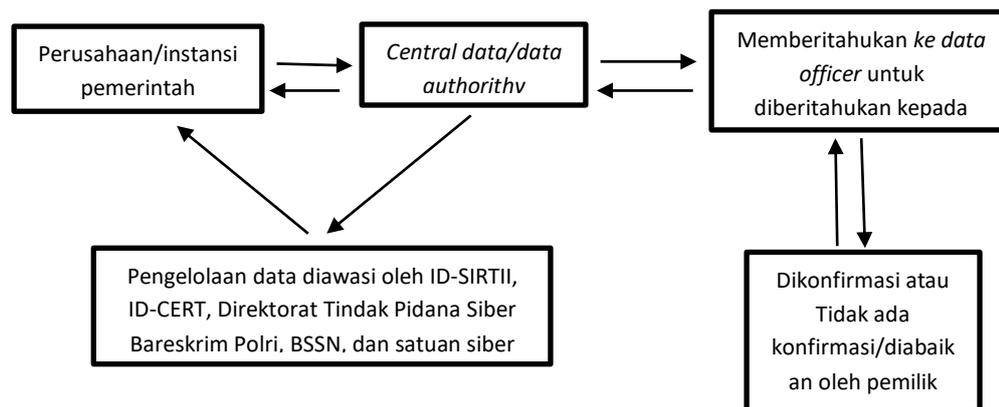
(Gambar 2. Skema Hubungan Kerjasama)

Kerjasama Kominfo sebagai implementasi dari sistem IDPS ini sangat diperlukan agar IDPS dalam implementasinya menjadi sebuah sistem yang kuat dan kokoh terhadap berbagai ancaman. ID-SIRTII, ID-CERT, Direktorat Tindak Pidana Siber Bareskrim Polri, BSSN, dan satuan siber TNI, merupakan wujud nyata pemerintah dalam menyikapi tantangan *cybercrime* yang terjadi di Indonesia, namun kelima lembaga tersebut masih belum menjangkau sepenuhnya terkait dengan *data protection* dan *data surveillance*, proteksi data yang dimaksud adalah proteksi data dan informasi yang dimiliki oleh seseorang, keempat lembaga ini hanya fokus pada penanggulangan, dan deteksi dini, dan tidak memperhatikan bagaimana sebenarnya pengelolaan data dan informasi seseorang itu, apakah data dan informasi pribadi seseorang sudah dikelola secara tepat dan baik, dengan adanya kerjasama ini juga sekaligus lembaga yang bertugas

melakukan pengawasan terhadap kinerja oleh *data officer*. Kerjasama yang dilakukan kominfo oleh keempat lembaga ini adalah untuk meningkatkan keamanan siber dibidang pengelolaan data dan informasi pribadi.

Sistem IDPS juga mampu mengatasi dan meminimalisir banyaknya kejahatan-kejahatan di bidang pengelolaan data dan informasi pribadi, yang diketahui bersama kejahatan terhadap pengelolaan data pribadi ini akan semakin meningkat seiring perkembangan teknologi yang begitu pesat, dan diperburuk dengan belum adanya regulasi yang mengatur mengenai perlindungan data pribadi dan kejahatan siber itu sendiri.

Permasalahan yang terkait dengan kewanitaan data dan informasi seseorang adalah data pribadi seseorang biasanya langsung diberikan oleh pihak pengelola data tanpa sepengetahuan pemilik data pribadi tersebut, dengan adanya IDPS ini jika sebuah perusahaan maupun instansi pemerintah ingin menggunakan data dan informasi seseorang maka harus dilaporkan terlebih dahulu dan memiliki jangka waktu selambat-lambatnya 60 menit dan paling lambat 3 x 24 jam untuk melakukan konfirmasi, jika lewat dari jangka waktu tersebut atau pemilik data mengabaikannya maka perusahaan dan instansi terkait berhak diberikan data dengan pemberiannya disertai dengan pengawasan. Adapun skemanya sebagai berikut:



(Gambar 3. Skema pemberitahuan oleh pemilik data)

Kepastian pengelolaan data dan informasi pribadi secara tepat dan baik diperlukan agar data pribadi seseorang tidak disalahgunakan, maka dari itu

IDPS sebagai sebuah sistem menjadi sebuah solusi dari permasalahan pengelolaan data dan informasi pribadi yang saat ini menjadi masalah di Indonesia. Hal ini ditunjukkan dengan identifikasi problematika yang telah diuraikan sebelumnya. Adapun beberapa keunggulan yang dimiliki oleh IDPS yaitu adalah: (1) memastikan pengelolaan data dan informasi seseorang dilakukan secara tepat dan baik; (2) melakukan izin terlebih dahulu jika data dan informasi seseorang akan digunakan kepada pemiliknya dengan jangka waktu yang ditentukan; (3) memiliki *data officer* yang dimana sebagai pusat pengelolaan data yang langsung mengkoordinasikannya kepusat dengan waktu sekali dalam 24 jam; (4) adanya kerjasama kominfo dengan lembaga kemanan siber untuk lebih memastikan dan meningkatkan pengawasan dan kontrol data; dan (5) meminimalisir adanya penyalahgunaan data dan informasi pribadi seseorang oleh pihak ketiga, karena adanya *data officer* yang ditempatkan diperusahaan dan institusi pemerintah.

3. Penutup

Berdasarkan uraian pembahasan atas rumusan masalah diatas, maka Penulis menarik beberapa kesimpulan sebagai berikut:

1. Pengelolaan data dan informasi pribadi di Indonesia dinilai sangat penting untuk diawasi dan dikelola dengan sistem keamanan yang baik dan terjamin sehingga dapat meminimalisir kejahatan pencurian atau pembobolan data dan informasi serta kejahatan jual beli data dan informasi online di Indonesia, karena dampak dari kejahatan tersebut adalah adanya penyalahgunaan data dan informasi pribadi seorang oleh pihak yang tidak bertanggungjawab, selain perlunya pengawasan dan kepastian pengelolaan yang baik dan tepat, juga dibutuhkan sebuah peraturan yang berkaitan dengan kejahatan dunia maya (*cybercrime*) dan juga perlindungan data dan informasi pribadi di indonesia.
2. Dibutuhkan sebuah sistem yang mampu mengatasi masalah terkait dengan perlindungan data dan informasi pribadi yaitu *Indonesia Data Protection*

System (IDPS) yang bertujuan untuk melakukan pengelolaan data dan informasi pribadi sebagai bentuk perlindungan data dan informasi pribadi di Indonesia. *Indonesia Data Protection System (IDPS)* memiliki dua unsur yang sangat penting atau *urgent*, yaitu *central data* atau *data authority* serta *data officer*. *Central data* atau *data authority* fungsinya adalah untuk mengumpulkan dan mengamankan setiap data dan informasi pribadi yang masuk dari *data officer*, maka dari itu *data officer* ditempatkan pada seluruh perusahaan dan instansi pemerintahan yang melakukan pengelolaan data dan informasi pribadi agar lebih mudah untuk melakukan koordinasi terkait dengan data dan informasi pribadi yang dimiliki seseorang. *Data officer* juga harus melakukan koordinasi tentang pengelolaan data dan informasi pribadi yang dikelola sekali dalam 24 jam, agar *central data* mempunyai informasi yang *up to date* terhadap pengelolaan data pribadi oleh perusahaan dan instansi pemerintah. IDPS sebagai sebuah sistem yang dilekatkan pada Kominfo, untuk mendukung kinerja dari sistem ini juga perlu adanya kerjasama terhadap badan atau pun tim yang sudah dibentuk oleh pemerintah sebelumnya, kerjasama ini dilakukan untuk mewujudkan adanya *cyber surveillance* dan perlindungan data terhadap data dan informasi seseorang yang sedang diproses, fungsi dari adanya kerjasama ini adalah untuk lebih meningkatkan ketahanan dari IDPS itu sendiri yang nantinya akan menjadi pusat pengelolaan data pribadi dan sebagai pusat kontrol data pribadi seseorang yang dilaporkan oleh *data officer*.

DAFTAR PUSTAKA

Buku

- Amiruddin, Dan Asikin, H. Z., 2004, *Pengantar Metode Penelitian Hukum*, Jakarta: Pt. Rajagrafindo Persada.
- Amiruddin, Dan Asikin, H. Z., 2016, *Pengantar Metode Penelitian Hukum*, Edisi Revisi, Jakarta: Rajawali Pers.
- Arief, B. W., 2007, *Tindak Pidana Mayantara Perkembangan Kajian Cybercrime*

Di Indonesia, Jakarta: PT Rajagrafindo Persada.

Bungin, B., 2008, *Analisis Data Penelitian Kualitatif*, Jakarta: Rajawali Pers.

Dewi, S., 2009, *cyberlaw*, Bandung: Widya Padjadjaran.

Mansur, D. M. A., dan Gultom, E., 2005, *cyber law aspek hukum teknologi informasi*, Bandung: PT Refika Aditama.

Marzuki, P. M., 2015, *Penelitian Hukum*, Edisi Revisi, Jakarta: Kencana.

Mertokusumo, S., 1996, *Penemuan Hukum Sebuah Pengantar*, Yogyakarta: Liberty.

Miles, M. B., Dan Huberman, A. M., 1992, *Analisis Data Kualitatif*, Cetakan 1, Jakarta: Universitas Indonesia (Ui-Press).

Munir, N., 2017, *Pengantar Hukum Siber Indonesia*, Depok: Rajawaji Pers, Halaman 27.

Rahardjo, S., 2006, *Ilmu Hukum*, Bandung: Pt Citra Aditya Bakti.

Rifai, A., 2010, *Penemuan Hukum Oleh Hakim Dalam Perspektif Hukum Progresif*, Jakarta: Sinar Grafika.

Siahaan, A. P. U., 2018, *Pelanggaran Cybercrime Dan Kekuatan Yurisdiksi Di Indoneisa*, Jurnal Teknik Dan Informatika, Vol. 5, No. 1.

Sujamto, 1983, *Beberapa Pengertian di Bidang Pengawasan*, Ghalia Indonesia: Jakarta, Halaman 17. Perhatikan juga Sujamto, 1987, *Aspek – aspek Pengawasan di Indonesia*, Sinar Grafika; Jakarta.

Sunggono, B., 2013, *Metodologi Penelitian Hukum*, Jakarta: Rajawali Pers.

Yusuf, A. M., 2017, *Metode Penelitian Kuantitatif, Kualitatif Dan Penelitian Gabungan*, Cetakan Ke-4, Jakarta: Kencana.

Jurnal

Agus, A. A. dan Riskawati., 2016, Penanganan Kasus Cybercrime di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar), *Jurnal Supremasi*, Vol. 10, No. 1.

Anggara, B. dan Darmadha, I. N., 2016, Penegakan Hukum Kejahatan Dunia Maya (CybeCrime) yang Dilakukan Anak Dibawah Umur, *kertha wicara journal ilmu hukum*, Vol. 5, No. 5.

Arianto, A. R. dan Anggraini, G., 2019, Membangun Pertahanan dan Keamanan

Siber Nasional Indonesia Guna Menghadapi Ancaman Siber Global Melalui Indonesia Security Incident Response Team On Internet Infrastructure (ID – SIRTII), *Jurnal Pertahanan & Bela Negara*, Vol. 9, No. 1.

Chotimah, H. C., 2019, Tata Kelola Keamanan Siber Dan Diplomasi Siber Di Indonesia Dibawah Kelembagaan Badan Siber Dan Sandi Negara, *Jurnal politica*, Vol. 10, No. 2.

Cunha, T. E. D. C. Helan, Y. G. T. dan Tadeus, D. W., 2019, Implementasi Aplikasi Feeder Dihubungkan Dengan Perlindungan Data Pribadi Dosen Dan Mahasiswa Ditinjau Dari Undang-Undang Nomor 12 Tahun 2012 Tentang Pendidikan Tinggi, *Jurnal Akrab Juara* Vol.4, No. 3.

Danuri, M. dan Suharnawi., 2017, Trend Cybercrime Dan Teknologi Informasi Di Indonesia, *Jurnal AMIK JTC Infokam*, Vol. 13, No. 2.

Dewi S. dan Gumelar, G., 2018, Perlindungan Privasi dan Data Pribadi Dalam Era Ekonomi Digital di Indonesia, *Jurnal Vej*, Vol. 4, No. 1.

Dewi, S., 2016, Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia, *Jurnal Yusticia*, Vol. 5, No. 1.

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

Elsinda, E., 2014, Aspek Hukum Perlindungan Data Pribadi di Dunia Maya, *Jurnal Gema Aktualita*, Vol. 3, No. 2.

Islami, M. Y., 2017, Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index, *Jurnal Masyarakat Telematika Dan Informasi*, Vol. 8 No. 2

Kwarto, F. dan Angsito, M., 2018, Pengaruh Cybercrime Terhadap Cyber Security Compliance Di Sektor Keuangan, *Jurnal Akuntansi Bisnis*, Vol. 11, No.2.

Latumahina, R. E., 2014, Aspek Hukum Perlindungan Data Pribadi Di Dunia Maya, *Jurnal Gema Aktualita*, Vol. 3 No. 2.

Lutfi, M., 2007, *Hermeneutika: Pemahaman Konseptual Dan Metodologis*, *Jurnal Nasional Masyarakat, Kebudayaan Dan Politik*, Vol. 10, No. 5.

- Mustafa, I., 2016, *Jendela Logika Dalam Berfikir: Deduksi Dan Induksi Sebagai Dasar Penalaran Ilmiah, Jurnal Pemikiran Dan Pendidikan Islam El-Banat, Vol. 6, No. 2.*
- Napitupulu, D., 2017, Kajian Peran Cyber Law Dalam Memperkuat Keamanan Sistem Informasi Nasional, *Deviance Jurnal Kriminologi, Vol. 1 No. 1.*
- Rahmawati, I., 2017, Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cybercrime) Dalam Peningkatan Cyber Defense, *Jurnal Pertahanan & Bela Negara, Vol. 7, No. 2.*
- Sari, N. W., 2018, Kejahatan Cyber Dalam Perkembangan Teknologi Informasi Berbasis Komputer, *Jurnal Surya Kencana Dua: Dinamika Masalah Hukum Dan Keadilan, Vol. 5 No. 2.*
- Sari, N. W., 2018, kejahatan cyber dalam perkembangan teknologi informasi berbasis komputer, *jurnal surya kencana dua: dinamika masalah hukum dan keadilan, Vol. 5, No. 2.*
- Sautunnida, L., 2018, Urgensi Undang – Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia, *Kanun Jurnal Ilmu Hukum, Vol. 20, No. 2.*
- Siagian, L. Budiarto, A. Dan Simatupang., 2018, Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional, *Jurnal Prodi Perang Asimetris, Vol. 4, No. 3.*
- Situmorang, E. L., 2014, Kajian Yuridis Pembuktian Kejahatan Mayantara (Cybercrime) Dalam Lingkup Transnasional (Studi Putusan), *Jurnal Mahupiki, Vol. 3, No. 1.*
- Tumalun, B., 2018, Upaya Penanggulangan Kejahatan Komputer Dalam Sistem Elektronik Menurut Pasal 30 Undang-Undang Nomor 11 Tahun 2008, *Jurnal Lex Et Societatis Vol. 6, No. 2.*

Situs Internet/Halaman Web

- Angendari, D. A. D., 2019, *Kasus data Dukcapil: Pelajaran terkait privasi dan data pribadi di Indonesia*, [online] tersedia di: dari <http://theconversation.com/kasus-data-dukcapil-pelajaran-terkait-privasi-dan-data-pribadi-di-indonesia-121264> (Diakses Pada 14 Desember 2019).

- Anonim, 2019, *Kasus data Dukcapil: Pelajaran terkait privasi dan data pribadi di Indonesia*, [online] tersedia di: <https://elsam.or.id/pentingnya-melindungi-data-pribadi-bagi-perusahaan/> (Diakses Pada 22 November 2019).
- Badan Siber dan Sandi Negara, 2018, *Badan Sandi dan Siber Negara*, [online] tersedia di <https://bssn.go.id>, (Diakses pada 25 Desember 2019).
- CNN Indonesia, 2019, *kemendagri adu jual beli data pribadi ke polisi di apresiasi*, [online] tersedia di: <https://www.cnnindonesia.com/teknologi/20190731182440-185417177/kemendagri-adu-jual-beli-data-pribadi-ke-polisi-diapresiasi> (Diakses Pada 13 Desember 2019).
- Davis, J., 2019, *What is Cyber Surveillance*, [online] tersedia di <https://www.quora.com/What-is-cyber-surveillance>, (Diakses pada 05 Desember 2019).
- Dramanda, W., 2014, *Apakah Hak atas Privasi Termasuk HAM?*, [online] tersedia di <https://www.hukumonline.com/klinik/detail/ulasan/lt4f5f850ec2388/apakah-hak-atas-privasi-termasuk-ham/>, (Diakses pada tanggal 04 Desember 2019).
- Elnizar, N. W., 2019, *Perlindungan Data Pribadi Tersebar di 32 UU, Indonesia Perlu Regulasi Khusus*, [online] tersedia di: <https://www.hukumonline.com/berita/baca/lt5d1c3962e01a4/perlindungan-data-pribadi-tersebar-di-32-uu--indonesia-perlu-regulasi-khusus/> (Diakses Pada 22 November 2019).
- ID-CERT, 2013, *Profil Indonesian Computer Response Team*, [online] Tersedia di <https://www.cert.or.id/tentang-kami/id/>, (Diakses Pada 25 Desember 2019).
- Id-SIRTII/CC, 2018, *Indonesia Security Incident Response Team on Internet Infrastructure / Coordination Center*, [online] tersedia <https://www.idsirtii.or.id/>, diakses pada tanggal 24 Desember 2019.
- Kompas.com, 2019, *"Data Pribadi Dijual Bebas, dari Gaji hingga Info Kemampuan Finansial"*, [online] tersedia di: <https://money.kompas.com/read/2019/05/13/081753626/data-pribadi-dijual-bebas-dari-gaji-hingga-info-kemampuan-finansial?page=all>. (Diakses Pada

13 Desember 2019).

Kompas.com, 2019, *Data Pribadi Nasabah Juga Dijual Secara Online, Jumlahnya Jutaan*, [online] tersedia di: <https://money.kompas.com/read/2019/05/13/120800426/data-pribadi-nasabah-juga-dijual-secara-online-jumlahnya-jutaan-?page=all>. (Diakses Pada 13 Desember 2019).

Kompas.com, 2019, *Polri: Kasus Jual-Beli Data Pribadi di Web Berbeda dengan di Grup Facebook*, [online] tersedia di: <https://nasional.kompas.com/read/2019/08/16/08272631/polri-kasus-jual-beli-data-pribadi-di-web-berbeda-dengan-di-grup-facebook?page=all> (Diakses Pada 13 Desember 2019).

Kompasiana.com, 2019, *Regulasi Siber Sangat Penting Dibentuk Secepatnya*, [online] tersedia di: https://www.kompasiana.com/lumiere_28/5d23d1470d82306be96ce6a8/regulasi-siber-sangat-penting-dibentuk-secepatnya?page=all (Diakses Pada 9 Desember 2019).

Lembaga Studi dan advokasi masyarakat, *Pentingnya Melindungi Data Pribadi bagi Perusahaan* [online] tersedia di: <https://elsam.or.id/pentingnya-melindungi-data-pribadi-bagi-perusahaan/> (Diakses Pada 22 November 2019).

Lingga, M. A., 2019, *Penyalahgunaan Data Pribadi Konsumen Sudah Masuk Kategori Gawat Darurat*, [online] tersedia di: <https://money.kompas.com/read/2019/07/27/201200426/penyalahgunaan-data-pribadi-konsumen-sudah-masuk-kategori-gawat-darurat?page=all> (Diakses Pada 22 November 2019).

Liputan6.com, 2018, *4,5 Miliar Data Dicuri Selama 6 Bulan Pertama 2018*, [online] tersedia di: <https://www.liputan6.com/tekno/read/3665291/45-miliar-data-dicuri-selama-6-bulan-pertama-2018> (Diakses Pada 13 Desember 2019).

Mawa Kresna, 2019, *Bagaimana Data Nasabah Kartu Kredit Diperjualbelikan*, [online] tersedia di: <https://tirto.id/bagaimana-data-nasabah-kartu-kredit-diperjualbelikan-djSv> (Diakses Pada 13 Desember 2019).

Patroli Siber, 2019, *Direktorat Tindak Pidana Siber (Dittipidsiber)*, [online] tersedia di <https://patrolisiber.id>, (Diakses pada 25 Desember 2019).

Ristianto, C., 2019, "*LBH Jakarta Terima 5.000-an Laporan terkait Perlindungan Data Pribadi*", [online] tersedia di: <https://nasional.kompas.com/read/2019/08/02/12571121/lbh-jakarta-terima-5000-an-laporan-terkait-perlindungan-data-pribadi>. (Diakses pada 22 November 2019).

Roosyana, R., 2019, *Pemerintah mesti lindungi privasi dan data pribadi warganya*, [online] tersedia di: <https://beritagar.id/artikel/berita/pemerintah-mesti-lindungi-privasi-dan-data-pribadi-warganya> (Diakses Pada 13 Desember 2019).

Satsiber TNI, 2019, *Satuan Siber TNI*, [online] tersedia di <https://satsiber-tni.mil.id>, (Diakses pada 25 Desember 2019).

Tirto.id, 2019, *UU ITE Dinilai Belum Cukup Lawan Kejahatan Siber*, [online] tersedia di: <https://tirto.id/uu-ite-dinilai-belum-cukup-lawan-kejahatan-siber-dgqU> (Diakses Pada 14 Desember 2019).

Wardani, A. S., 2019, *Malindo: Kebocoran Data Gara-Gara Mantan Staf Perusahaan Kontraktor*, <https://www.liputan6.com/tekno/read/4069498/malindo-kebocoran-data-gara-gara-mantan-staf-perusahaan-kontraktor> (Diakses Pada 13 Desember 2019).

Skripsi/Tesis/Disertasi

Amanda, A. P. B. A., 2013, *Tinjauan Yuridis Perlindungan Data Pribadi Dari Penyalahgunaan Data Pribadi Pada Media Sosial (Ditinjau Dari Privacy Policy Facebook Dan Undang – Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik)*, Tesis, Fakultas Hukum Universitas Brawijaya Malang.

Peraturan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Republik Indonesia Nomor 24 Tahun 2013 Tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan

Peraturan Pemerintah Republik Indonesia Nomor 37 Tahun 2007 Tentang Pelaksanaan Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan.

Undang Undang Republik Indonesia No. 19 tahun 2016 tentang perubahan atas undang undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

Peraturan Menteri Komunikasi dan Informatika No.29/PER/M. KOMINFO/12/2010.

Lain-lain

Djafar, W., 2019, *Hukum Perlindungan Data Pribadi Di Indonesia: Lanskap, Urgensi, Dan Kebutuhan Pembaharuan.*

GDPR (*General Data Protection Regulation*)

ICCPR (*International Covenant on Civil and Political Rights*)

UDHR (*Universal Declaration of Human Rights*)