



## **Pertanggung Jawaban Pidana UU ITE Terhadap Pembobolan Data Pribadi di Era Serba Digital**

**Bagus Imam Faisal**

Program Studi Pendidikan Pancasila dan Kewarganegaraan  
STKIP PGRI Bangkalan  
*bagusimam@stkipgri-bkl.ac.id*

**Dian Eka Indriani**

Program Studi Pendidikan Pancasila dan Kewarganegaraan  
STKIP PGRI Bangkalan  
*dianindrian79@stkipgri-bkl.ac.id*

### ***Abstract***

The advancement of information technology in Indonesia is especially very rapid once the cell, a computer, and the internet have proven to have a positive impact on better human life. Behind of ease offered by a computer and the internet, having turns a dark side that can destroy life and human culture itself. Methods used in this research is by using an approach to a problem juridical normative namely to the concept of law as the norm, rules, the principle, by adopting regulations that are described in a sort of descriptive set based on a problem with various the rules of law and literature, and search for an opinion the law of issues object the problem. Private data protection on an electronic system in law information and electronic transaction ( ITE) covers protection from the use without any permission, the protection of the creation of this electronic system, as well as efforts to protect leakage of access as well as illegal interference. Criminal sanctions that had been established in the act of ITE in the form of criminal sanctions prison and fines. So common interpretation surely has governed by data protection to the provisions in government regulation number 71 in 2019 on the implementation of the system and electronic transaction article 30-33 and article 35 which was about activities that are not allowed.

***Keywords:*** *information technology criminal, sanctions, information and electronic transaction, ITE*

### **Abstrak**

*Submitted: 12-10-2022 Revised: 30-10-2022 Accepted: 15-11-2022*

652 | Civic Culture



Kemajuan teknologi informasi di Indonesia sangat lah pesat sekali terutama pada bidang Hp, komputer dan internet terbukti telah memberikan dampak positif bagi kemajuan kehidupan manusia. Dibalik kelebihan dan kemudahan yang ditawarkan oleh komputer dan internet, ternyata memiliki sisi gelap yang dapat menghancurkan kehidupan dan budaya manusia itu sendiri.

Metode yang digunakan dalam penelitian ini adalah dengan menggunakan pendekatan masalah yuridis normatif yakni mengkonsepsikan hukum sebagai norma, kaidah, asas, dengan menggunakan pendekatan perundang-undangan yang dijelaskan secara secara deskriptif berdasarkan permasalahan dengan berbagai aturan-aturan hukum dan lieteratur, serta mencari suatu opini hukum tentang masalah yang menjadi objek permasalahannya.

Perlindungan data pribadi pada sebuah sistem elektronik di UU Informasi dan Transaksi Elektronik (ITE) mencakup perlindungan dari penggunaan tanpa adanya izin, proteksi sang penyelenggara sistem elektronika, serta upaya perlindungan kebocoran dari akses serta interferensi ilegal. Sanksi pidana yang ditetapkan dalam Undang-undang ITE berupa sanksi pidana penjara dan denda. maka Interpretasi umum proteksi data sesungguhnya sudah diatur oleh ketentuan di dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik Pasal 30-33 dan pasal 35 yaitu tentang kegiatan yang tidak diperbolehkan.

**Kata Kunci:** teknologi informasi, Sanksi Pidana dan Informasi dan Transaksi Elektronik (ITE)

## I. Pendahuluan

Kemajuan teknologi informasi di Indonesia sangat lah pesat sekali terutama pada bidang Hp, 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. 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. Informasi 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. (Rumlus, Muhamad Hasan; Hartadi, Hanif, 2020)





Nama lengkap, nomor NIK, nomor KK dan data atau informasi formal penting terkait kenegaraan maupun gambar dan video pribadi, percakapan pribadi, dan berbagai kebutuhan pribadi. Jika dilihat lebih lanjut, keberadaan *smartphone* dan internet ini membuat kita semua secara tak sadar memiliki identitas digital yang dapat diakses oleh orang-orang yang tak bertanggung jawab sehingga dapat menjadikan kita korban tanpa kita sadari.

Perhatian terhadap pemberian perlindungan kepada data pribadi (*privacy data protection*) yang dicuri semakin mendapat perhatian dari masyarakat ketika salah satu perusahaan (*company*) media sosial terbesar di dunia mengalami pencurian data pribadi oleh beberapa pihak. Sebuah berita pencurian data pribadi tersebut sudah tersebar dengan cepat di berbagai media elektronik yang kemudian dengan mendapat pengakuan dari perusahaan tersebut bahwa telah terjadi pencurian data pribadi atau pengambilan data pribadi milik orang lain tanpa izin yang kemudian dikenal dengan sebutan infomatik "pencurian data atau pembobolan data". Keadaan ini terjadi disebabkan karena adanya kelemahan pada sistem yang digunakan untuk penyimpanan data yang dimiliki oleh perusahaan sehingga data pribadi milik orang lain dapat dicuri oleh pihak yang tidak bertanggung jawab. (Rumlus, Muhamad Hasan; Hartadi, Hanif, 2020)

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 58 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).

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, phishing (internet banking fraud), malware





(virus/worm/trojan/bots), cybersquatting, pornografi, perjudian online, transnasional crime (perdagangan narkoba, mafia, terorisme, money laundering, human trafficking, underground economy). 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. (Aswandi, Ririn; Muchsin, Putri Rofifah Nabilah ; Sultan, Muhammad, 2020)

Pencurian identitas telah berkorelasi dengan penyalahgunaan komputer, kejahatan komputer dan kejahatan terkait komputer karena Internet memfasilitasi mereka, itu disebut pencurian identitas online, misalnya adalah kasus peretas yang mencuri informasi pribadi seseorang melalui pelanggaran data online. Sehubungan dengan hal tersebut, maka Pembobolan terhadap Nama lengkap, nomor NIK, nomor KK dan data atau informasi formal penting. Di lakukan dengan kejahatan Berdasarkan uraian tersebut maka permasalahan yang akan dibahas adalah: Bagaimanakah penerapan sanksi pidana terhadap pembobolan data pribadi dalam UU ITE? Dan apakah yang mempengaruhi proses penerapan sanksi pidana terhadap UU ITE ?

## **II. Metode Penelitian**

Metode yang digunakan dalam penelitian ini adalah dengan menggunakan pendekatan masalah yuridis normatif yakni mengkonsepsikan hukum sebagai norma, kaidah, asas, dengan menggunakan pendekatan perundang-undangan yang dijelaskan secara deskriptif berdasarkan permasalahan dengan berbagai aturan-aturan hukum dan literatur, serta mencari suatu opini hukum tentang masalah yang menjadi objek permasalahannya. Ketika suatu penelitian hukum normative dapat dimulai dengan suatu masalah/kasus hukum factual (lalu disebut penelitian hukum doktriner), kemudian dicari hukum yang tepat diterapkan terhadap masalah hukum tersebut, sehingga ditemukan kategori hukum, kaidah hukum, prinsip hukum, sampai kemudian teori hukum untuk dapat diterapkan terhadap masalah tersebut. (Munir Fuady, 2018)

## **III. Hasil Dan Pembahasan**

### **3.1 Penerapan Sanksi Pidana Terhadap Pembobolan Data Pribadi**

Kejahatan Siber tidak dapat dipisahkan dari pengaruh Globalisasi. Globalisasi pada dasarnya bermula dari awal abad ke 20, yakni pada saat revolusi transportasi dan elektronika mulai memperluas dan mempercepat perdagangan antar bangsa. Di samping pertambahan dan kecepatan lalu lintas barang dan jasa, berkembang pula secara cepat globalisasi gagasan





modern seperti negara, konstitusi, nasionalisme, kapitalisme, demokrasi, sekularisme, juga industri dan perusahaan media massa. Perusahaan media massa inilah yang menjadi faktor awal berkembangnya teknologi informasi. (Wahid, Abdul; Labib, Mohammad, 2005)

Jenis tindak pidana (*cyber crime*) merupakan tindak pidana yang timbul karena dampak globalisasi. Globalisasi sangat dipengaruhi oleh perkembangan Teknologi Informasi dan Komunikasi (TIK) yang semakin pesat dan canggih. Perkembangan TIK selain menghadirkan dampak positif dan juga memiliki dampak negatif. Dampak positif dan negatif dari perkembangan TIK layaknya dua sisi koin yang harus dibedakan namun tidak dapat dipisahkan. Maknanya terhadap sisi positif, tentu dapat dimanfaatkan untuk melakukan pembangunan dan mencapai tujuan nasional yang dicita-citakan oleh bangsa Indonesia. (Kristian; Gunawan, yopi, 2013)

Pada umumnya, pelaku pencurian data pribadi pengguna sistem elektronik dilakukan dengan teknik peretasan (*hacking*) yaitu dengan meretas atau masuk secara ilegal kedalam database sistem elektronik. Setelah mendapatkan data pribadi berupa *username*, NIP, nomor kartu keluarga, tempat dan tanggal lahir, nomor HP, hingga nama-nama anggota keluarga pengguna sistem elektronik, kemudian dijual belikan oleh pelaku di *online marketplace*. Tindakan jual beli data pribadi sangat rentan disalahgunakan untuk tindakan-tindakan lain yang dapat merugikan pemilik data pribadi tersebut.

Indonesia dalam hal ini untuk mewujudkan perlindungan hukum melalui di bentuknya lembaga-lembaga Negara dalam penegakan hukum seperti Pengadilan,Kejaksaan, dan Kepolisian. Lembaga-Lembaga ini adalah wujud konsistensi bahwa Negara Indonesia adalah Negara Hukum, Yang mana semua aspek dalam berkehidupan dan berbangsa diatur dan berpedoman kepada peraturan perundang undangan yang berlaku,sehingga hukum hadir di dalam sendi- sendi kehidupan di negeri ini. Untuk itu dengan adanya Perlindungan Hukum diharapkan dapat mencapai tujuan untuk memberikan keadilan, khususnya keadilan terkait dengan data pribadi. (Wijaya, Alvian Dwiangga; Anggriawan, Teddy Prima, 2022)

Saat ini perlindungan data pribadi termuat di beberapa peraturan perundang-undangan, antara lain:

1. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;
2. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggara Sistem dan Transaksi Elektronik;





Klasifikasi perihal data pribadi diamanatkan lebih lanjut oleh UU ITE dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE). Perlindungan data pribadi pada sebuah sistem elektronik di UU ITE mencakup perlindungan dari penggunaan tanpa adanya izin, proteksi sang penyelenggara sistem elektronika, serta proteksi berasal akses serta interferensi ilegal. Berhubungan dengan menggunakan proteksi data pribadi berasal pemakaian tiadanya persetujuan, Pasal 26 UU ITE mengharuskan bahwa penerapan setiap data pribadi dalam sebuah media elektronik harus mempunyai izin dari seseorang yang mempunyai data berkaitan. Siapapun yang tidak mengikuti kebijakan ini dapat dituntut atas kerugian yang muncul. Isi pada pasal 26 UU ITE merupakan menjadi berikut: 1) Penggunaan setiap berita melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan. 2) Setiap Orang yang melanggar haknya sebagaimana dimaksud di ayat (1) bisa mengajukan gugatan atas kerugian yang ditimbulkan sesuai Undang-Undang ini pada penjelasannya, Pasal 26 UU ITE menyatakan bahwa data pribadi merupakan bagian dari hak individu atas privasi. Sementara itu, lihat Pasal 1 PP PSTE untuk definisi data langsung artinya, data pribadi seorang individu disimpan, dipelihara, disimpan dengan itikad baik dan dilindungi kerahasiaannya. Penjelasan pasal 26 ayat (1) UU ITE juga menjelaskan lebih dalam seputar pengertian hak pribadi. Pernyataan terkait dengan penggunaan teknologi informasi dan perlindungan informasi atau data pribadi adalah bagian dari hak privasi (*privacy rights*). (Anugerah, Fiqqih; Tantimin, 2022)

Hak pribadi memiliki implikasi yakni hak pribadi adalah hak untuk memiliki kehidupan pribadi dan tidak boleh diganggu, hak pribadi adalah hak untuk bisa berkomunikasi menggunakan dengan orang lain tanpa dimata-matai, dan hak pribadi adalah hak untuk mengakses akses informasi tentang kehidupan langsung dan data seseorang. Interpretasi umum, maka proteksi data sesungguhnya sudah diatur oleh ketentuan UU ITE, yaitu di Pasal 30-33 dan pasal 35 yaitu tentang kegiatan yang tidak diperbolehkan. UU ITE dengan tegas melarang akses ilegal terhadap data orang lain melalui sistem elektronik dengan tujuan melanggar sistem keamanan dan memperoleh informasi. Selain itu, UU ITE dengan jelas menyatakan bahwa penyadapan adalah tindakan yang dilarang kecuali dilakukan oleh pihak yang berhak melakukannya dengan upaya hukum. Siapa pun yang merasa dirugikan oleh perilaku yang ditangguhkan dapat menuntut ganti rugi dan pelaku juga akan bertanggung jawab atas apa yang telah dikerjakannya.





Berdasarkan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik bunyi Pasal 26 ayat (1) menyatakan “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”. Ayat (2) kemudian menyatakan “setiap orang yang melanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini”. Penjelasan Pasal 26 Ayat (1) menyatakan bahwa dalam memaksimalkan media massa (Informasi), merupakan suatu konsep dari hak privasi (pribadi) dalam perlindungan data privasi (pribadi).

### **3.2 Proses Penerapan Sanksi Pidana Terhadap UU ITE**

Tindak pidana ialah sebagai suatu perilaku manusia yang pada suatu saat tertentu telah ditolak di dalam sesuatu pergaulan hidup tertentu dan dianggap sebagai perilaku yang harus ditiadakan oleh hukum pidana dengan menggunakan sarana- sarana yang bersifat memaksa yang terdapat di dalamnya. (Lamintang, P.A.F; Lamintang, Franciscus Theojunior, 2014)

Menurut Amir Ilyas Delik yang dalam bahasa Belanda disebut *Strafbaarfeit*, terdiri atas tiga kata, yaitu *straf*, *baar*, dan *feit*. Yang masing-masing memiliki arti: *Straf* diartikan sebagai pidana dan hukum, *Baar* diartikan sebagai dapat dan boleh dan *Feit* diartikan sebagai tindak, peristiwa, pelanggaran, dan perbuatan. Jadi istilah *Strafbaarfeit* adalah peristiwa yang dapat dipidana atau perbuatan yang dapat dipidana. (Amir Ilyas, 2012)

Sedangkan menurut Vos dalam Adami Chazawi, unsur-unsur tindak pidana yaitu:

1. Kelakuan manusia;
2. Diancam dengan pidana;
3. Dalam peraturan perundang-perundangan. (Adami Chazawi, 2001)

Sanksi pidana yang ditetapkan dalam Undang-undang ITE berupa sanksi pidana penjara dan denda. Kedua macam pidana tersebut ditetapkan secara maksimum khusus saja. Hal ini perlu mendapat perhatian karena terdapat kelemahan jika hanya diberlakukan maksimum khusus saja tanpa minimum khusus, karena dalam praktiknya nanti dimungkinkan terjadi disparitas. Oleh karenanya mengingat kejahatan seperti penghinaan di media sosial ini bukanlah kejahatan biasa yang menimbulkan kerugian yang tidak sederhana.

Kegiatan cyber meski bersifat virtual karena tidak bertemu secara langsung dapat dikategorikan sebagai tindakan dan perbuatan hukum yang nyata. Secara yuridis dalam hal ruang cyber sudah tidak pada tempatnya lagi untuk mengkatégorikan sesuatu dengan ukuran





dan kualifikasi hukum konvensional untuk dapat dijadikan objek dan perbuatan, sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal-hal yang lolos dari jerat hukum. Kegiatan cyber adalah kegiatan virtual yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik. Terdapat 3 (tiga) pendekatan yang dapat dilakukan sebagai upaya pencegahan dan penanggulangan kejahatan melalui cyberspace, yaitu pendekatan teknologi, pendekatan social budaya dan pendekatan hukum. Sanksi pidana merupakan suatu jenis sanksi yang bersifat nestapa yang dikenakan terhadap perbuatan atau pelaku perbuatan pidana atau tindak pidana yang dapat mengganggu atau membahayakan kepentingan hukum, serta proses jalannya pembangunan nasional. Disadari juga bahwa sanksi pidana bersifat ultimatum remidium, atau dalam bahasa kebijakan atau manajemen adalah jalan terakhir yang ditempuh, dari berbagai solusi atau alternatif solusi lainnya. (Gerry Kenjiro Tanos, 2016)

Di dalam pasal 31 undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menyebutkan bahwa Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.

Kemudian masih di dalam UU ITE pasal 30 yang menjelaskan bahwa setiap orang dengan sengaja dan melawan hukum mengakses computer dan/atau system elektronik orang lain untuk tujuan memperoleh informasi elektronik dan/atau dokumen elektronik dengan melakukan pelanggaran, penyusupan, penimpaan, atau pembobolan keamanan sistem dapat dipidana. Pidana yang diberikan kepada pelaku adalah dengan mendapatkan pidana penjara paling lama 6 (enam) sampai dengan 8 (delapan) tahun dan/atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah) sampai dengan Rp 800.000.000,00 (delapan ratus juta rupiah). Kemudian bagi pelaku kejahatan yang juga memperjualbelikan hasil data retasan yang telah mereka dapatkan juga diatur di dalam UU ITE. Di dalam Pasal 34 bahwa setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan, untuk dilakukan mengimpor, mendistribusikan, menyediakan atau memiliki perangkat komputer atau sistem informasi maka menurut Pasal 45 dapat dipidana dengan pidana penjara paling lama 6 (enam) tahun dan.atau denda paling





banyak Rp 1.000.000.000,00 (satu miliar rupiah). (Kusuma, Aditama Candra; Rahmani, Ayu Diah, 2022)

#### **IV. Kesimpulan**

Berdasarkan hasil dan pembebasan, maka dapat disimpulkan sebagai berikut:

4.1 Hak pribadi memiliki implikasi yakni hak pribadi adalah hak untuk memiliki kehidupan pribadi dan tidak boleh diganggu, hak pribadi adalah hak untuk bisa berkomunikasi menggunakan dengan orang lain tanpa dimata-matai, dan hak pribadi adalah hak untuk mengakses akses informasi tentang kehidupan langsung dan data seseorang. Interpretasi umum, maka proteksi data sesungguhnya sudah diatur oleh ketentuan UU ITE, yaitu di Pasal 30-33 dan pasal 35 yaitu tentang kegiatan yang tidak diperbolehkan.

4.2 Sanksi pidana yang ditetapkan dalam Undang-undang ITE berupa sanksi pidana penjara dan denda. Kedua macam pidana tersebut ditetapkan secara maksimum khusus saja. Hal ini perlu mendapat perhatian karena terdapat kelemahan jika hanya diberlakukan maksimum khusus saja tanpa minimum khusus, karena dalam praktiknya nanti dimungkinkan terjadi disparitas. Oleh karenanya mengingat kejahatan seperti penghinaan di media sosial ini bukanlah kejahatan biasa yang menimbulkan kerugian yang tidak sederhana.

#### **DAFTAR PUSTAKA**

- Rumlus, Muhamad Hasan; Hartadi, Hanif. (2020). KEBIJAKAN PENANGGULANGAN PENCURIAN DATA PRIBADI DALAM MEDIA ELEKTRONIK (Policy the Discontinuation of Personal Data Storage in Electronic Media). *Jurnal HAM*, 11(2), 285-299.
- Rumlus, Muhamad Hasan; Hartadi, Hanif. (2020). KEBIJAKAN PENANGGULANGAN PENCURIAN DATA PRIBADI DALAM MEDIA ELEKTRONIK (Policy the Discontinuation of Personal Data Storage in Electronic Media). 11(2), 285-299.
- Aswandi, Ririn; Muchsin, Putri Rofifah Nabilah ; Sultan, Muhammad. (2020). PERLINDUNGAN DATA DAN INFORMASI PRIBADI MELALUI INDONESIA DATA PROTECTION SYSTEM (IDPS). *LEGISLATIF ( lembaga gagasan mahasiswa yang solutif dan inovatif*, 3(2), 167-190.
- Soekanto, Soerjono; Mamudji, Sri. (1985). *Penelitian Hukum Normatif Suatu Tinjauan Singkat*. Jakarta: Rajawali Pers.
- Kristian; Gunawan, yopi. (2013). *Sekelumit tentang Penyadapan dalam Hukum Positif di Indonesia*. Bandung: Nuansa Aulia.





- Munir Fuady. (2018). *Metode Riset Hukum Pendekatan Teori Dan Konsep*. Depok: Rajawali Pers.
- Wijaya, Alvian Dwiangga; Anggriawan, Teddy Prima. (2022). Perlindungan Hukum Terhadap Data Pribadi Dalam Penggunaan Aplikasi di Smartphone. *Journal Inicio Legis*, 3(1), 63-72.
- Wahid, Abdul; Labib, Mohammad. (2005). *Kejahatan Mayantara (Cyber Crime)*. Bandung: Refika Aditama.
- Anugerah, Fiqqih; Tantimin. (2022). PENCURIAN DATA PRIBADI DI INTERNET DALAM PERSPEKTIF KRIMINOLOGI. *JURNAL KOMUNIKASI HUKUM*, 8(1), 419-435.
- Gerry Kenjiro Tanos. (2016). PENERAPAN SANKSI PIDANA TERHADAP PELAKU PENGHINAAN MELALUI MEDIA SOSIAL MENURUT UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK. *Lex et Societatis*, 4(1), 165-173.
- Kusuma, Aditama Candra; Rahmani, Ayu Diah. (2022). Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia). *SUPREMASI JURNAL HUKUM*, 5(1), 46-63.
- Amir Ilyas. (2012). *Asas-Asas Hukum Pidana I : Memahami Tindak Pidana dan Pertanggungjawaban Pidana sebagai Syarat Pemidanaan*. Yogyakarta: Rangkang Education dan PuKAP Indonesia.
- Adami Chazawi. (2001). *Stelsel Pidana, Tindak Pidana, Teori-Teori Pemidanaan dan Batas Berlakunya Hukum Pidana: Pelajaran Hukum Pidana*. Jakarta: Rajawali Press.
- Lamintang, P.A.F; Lamintang, Franciscus Theojunior. (2014). *Dasar-Dasar Hukum Pidana di Indonesia*. Jakarta: Sinar Grafika.
- Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
- Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggara Sistem dan Transaksi Elektronik