

PENEGAKAN HUKUM TERHADAP TINDAK PIDANA PERETASAN SEBAGAI BENTUK KEJAHATAN MAYANTARA (CYBER CRIME)

I Gusti Ayu Suanti Karnadi Singgi, I Gusti Bagus Suryawan, I Nyoman Gede Sugiarta
Fakultas Ilmu Hukum Universitas Warmadewa, Denpasar – Bali, Indonesia

Abstrak

Seiring dengan perkembangan teknologi, ada banyak fasilitas yang tersedia di dunia maya. Perkembangan teknologi ini juga dapat memberikan peluang bagi para pelaku kejahatan khususnya kejahatan di dunia maya. Kejahatan dunia maya merupakan bentuk atau dimensi baru dari suatu kejahatan yang saat ini banyak mendapat perhatian dari dunia internasional. Salah satu jenis kejahatan dunia maya yang dimaksud adalah kejahatan peretasan. Berdasarkan latar belakang tersebut, penelitian ini dilakukan dengan tujuan mendeskripsikan bagaimana penegakan hukum terhadap tindak pidana peretasan (hacking) dan bagaimana upaya penanganan kejahatan mayantara (cyber crime). Penelitian ini dilakukan dengan menggunakan metode penelitian hukum normatif dan pendekatan perundang-undangan. Hasil penelitian ini menunjukkan bahwa penegakan hukum terhadap tindak pidana peretasan diatur dalam Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pelaku akan diberikan sanksi pidana berupa kurungan penjara dan denda atas pelanggaran di bidang peretasan. Selain itu, upaya pemberantasan kejahatan mayantara (cyber crime) mengacu pada Undang-Undang Informasi dan Transaksi Elektronik yang dilakukan dengan tindakan preventif dan represif. Oleh karena itu, tindak pidana peretasan yang termasuk dalam ranah kejahatan siber telah diatur dalam pasal 30 ayat (1), (2) dan (3) UU ITE, sedangkan hukumannya diatur dalam pasal 46 ayat (1), (2), dan (3) dari UU ITE. Berkaitan dengan hal tersebut, pemerintah telah melakukan berbagai tindakan penanggulangan berupa tindakan preventif dan represif.

Kata Kunci: Hacking; Kejahatan Mayantara; Penegakan Hukum

Abstract

Along with technological developments, there are a lot of facilities available in cyberspace. The development of this technology can also provide opportunities for criminals, especially crimes in cyberspace. Cybercrime is a new form or dimension of a crime that is currently receiving a lot of attention from the international community. One type of cybercrime is hacking. Based on this background, this research was conducted with the aim of describing law enforcement against criminal acts of hacking and the efforts to deal with cybercrime. This research was conducted using normative legal research methods and statutory approaches. The results of this study showed that law enforcement against criminal acts of hacking is regulated in Law Number 19 of 2016 amending Law Number 11 of 2008 concerning Electronic Information and Transactions. The perpetrator will be given criminal sanctions in the form of imprisonment and fines for violations in the field of hacking. In addition, efforts to eradicate cybercrime refers to the Law on Information and Electronic Transactions which is carried out with preventive and repressive measures. Therefore, the criminal act of hacking which is included in the realm of cybercrime has been regulated in Article 30 paragraph (1), (2) and (3) of the ITE Law, while the punishment is regulated in Article 46 paragraph (1), (2), and (3) of the ITE Law. In this regard, the government has taken various countermeasures in the form of preventive and repressive measures.

Keywords: Hacking; Cybercrime; Law Enforcement

I. PENDAHULUAN

Teknologi yang berkembang sangat pesat menimbulkan banyak dampak baik dan buruk bagi kehidupan manusia (Ngafifi, 2014; Setiawan, 2018). Globalisasi menjadi salah satu penyebab perkembangan teknologi secara pesat dan tanpa batas. Daya pikir yang juga berkembang menyebabkan timbulnya sebuah pengetahuan. Atas pengetahuan tersebut tidak semua orang dapat memanfaatkannya dengan bijak dan benar, sehingga hal tersebut sangat merugikan banyak orang. Sebagai contoh, tindak pidana peretasan atau hacking yang timbul akibat dampak negatif kemajuan teknologi.

Tindak pidana peretasan ialah salah satu bagian dari kejahatan mayantara atau *cybercrime* yang muncul akibat adanya kemajuan teknologi. Hal ini telah diatur dalam pasal 30 ayat (1), (2), (3) Undang-Undang No. 19 Tahun 2016 perubahan atas Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang selanjutnya disebut dengan UUIE. Dan, untuk sanksi pidananya telah diatur dalam pasal 46 ayat (1),(2),(3) UUIE. Selain mendatangkan keuntungan atau nilai-nilai positif, teknologi juga mengandung muatan yang merugikan kehidupan bangsa (Wahid & Labib, 2005).

Maraknya tindakan peretasan menimbulkan banyak kerugian berupa materiil dan nonmateriil yang diderita oleh korban itu sendiri. Peretasan ini juga tidak hanya dilakukan pada situs web tetapi juga pada akun media sosial milik perseorangan (Nugroho, 2015; Rahmawati, 2017). Dari sekian banyak sisi gelap dari kemajuan teknologi, teknologi masih menyimpan banyak keuntungan positif seperti adanya email, e-commerce, internet banking, dan hal lain semacamnya.

Penelitian terdahulu yang berkaitan dengan penelitian ini dilakukan oleh Hartono, (2014). Penelitiannya berjudul 'Hacker dalam Perspektif Hukum Indonesia'. Penelitian terkait lainnya dilakukan oleh Purnomo (2002) yang berjudul 'Kebijakan Hukum terhadap Kejahatan Cybercrime di Era Informasi dan Masyarakat Virtual'. Muthia dan Arifin (2019) juga melakukan penelitian yang berkaitan dengan penelitian ini. penelitian mereka berjudul 'Kajian Hukum Pidana pada Kasus Kejahatan Mayantara (Cybercrime) dalam Perkara Pencemaran Nama Baik di Indonesia'

Berdasarkan latar belakang yang telah diuraikan di atas, penelitian ini dilakukan dengan tujuan mendeskripsikan bagaimana penegakan hukum terhadap tindak pidana peretasan (hacking) dan bagaimana upaya penanganan kejahatan mayantara (cybercrime).

II. METODE

Sebagaimana yang telah diuraikan di atas, maka metode penelitian yang digunakan adalah metode normatif. Penelitian ini mengkaji hukum tertulis dari berbagai segi dan aspek pendekatan yang dipergunakan, yaitu tipe pendekatan Perundang-Undangan yang bersifat tertulis serta memuat norma hukum yang mengikat dan pendekatan konseptual yakni suatu konsep yang terdapat di masyarakat.

Sumber bahan hukum yang dipergunakan bersumber dari Penelitian Kepustakaan berupa sumber bahan hukum primer berdasarkan atas peraturan Perundang-Undangan mengenai Informasi dan Transaksi Elektronik, yakni Undang-Undang No. 19 Tahun 2016 perubahan atas Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Bahan hukum sekunder diperoleh dari berbagai macam bacaan atau literatur dan peraturan Perundang-Undangan dan pendapat ahli hukum yang berkaitan dengan tulisan ini. Teknik pengumpulan bahan hukum dilakukan dengan mengumpulkan berbagai buku, literatur-literatur, serta bahan hukum lainnya yang berkaitan dengan tulisan ini. Data yang sudah terkumpul dianalisis menggunakan metode kualitatif. Hasil analisis data kemudian disajikan secara deskriptif.

III. HASIL DAN PEMBAHASAN

Penegakan Hukum terhadap Tindak Pidana Peretasan (Hacking)

Kejahatan mayantara (cybercrime) yang timbul akibat adanya kemajuan teknologi yang begitu pesat banyak mengakibatkan dampak negatif dan positif dari adanya teknologi tersebut. Dampak positif dapat berupa adanya e-mail, internet banking, serta hal-hal lain. Namun, perkembangan ini juga membawa pengaruh negatif seperti adanya tindak pidana peretasan (hacking) yang dilakukan guna untuk memperoleh informasi atau data-data penting lainnya.

Tindakan ini dilakukan tidak hanya semata-mata untuk mencari keuntungan dan menemukan titik lemah dari si target. Kejahatan ini dapat digolongkan lebih relatif baru jika dibandingkan dengan kejahatan konvensional lainnya. Meskipun kejahatan jenis ini telah muncul pada awal tahun 1961, ia tak sepopuler kejahatan konvensional yang selalu mudah dijangkau oleh telinga masyarakat. Sekalipun telah lama ada, namun belum ada kesepahaman para ahli untuk memberikan definisi baik itu kejahatan mayantara (cybercrime) maupun tindak pidana peretasan itu sendiri. Kendati demikian, telah banyak yang memakai istilah siber, kejahatan dunia maya, kejahatan firtual, dan bahkan tetap menggunakan istilah *cybercrime*.

Kemampuan membuat suatu program yang disalahgunakan oleh seseorang yang tidak bertanggungjawab menyebabkan terjadinya sebuah pelanggaran norma atau hukum yang berlaku guna

merugikan beberapa pihak yang telah sejak awal menjadi target sasaran. Salah satu contohnya adalah tindakan meretas situs web atau akun media sosial yang bersifat pribadi milik orang lain.

Ketentuan yang secara khusus mengatur mengenai tindak pidana peretasan telah termuat dalam pasal 30 ayat (1), (2), dan (3) UU ITE. Pasal ini menjelaskan bahwa setiap orang yang mencoba masuk atau mengakses sistem elektronik milik orang lain dengan cara apapun dengan sengaja dan tanpa hak melawan hukum. Pasal ini berkaitan langsung dengan pasal 46 ayat (1), (2), dan (3) UU ITE yang mengatur mengenai sanksi pidana atas pelanggaran yang tercantum dalam pasal 30 tersebut diatas.

Dalam hal melakukan penegakan hukum khususnya dalam bidang kejahatan mayantara, kejahatan ini memiliki jangkauan yang sangat luas tanpa mengenal batas wilayah teritorial suatu negara karena kejahatan ini bersifat transnasional. Tipe kejahatan yang tak mengenal batas ini mengharuskan yurisdiksi suatu negara terlibat langsung di dalamnya karena sangat jauh dari jangkauan suatu negara. Jika tanpa melakukan kerja sama antar negara dalam melakukan pemberantasan serta penegakan hukum yang sebagaimana mestinya, kejahatan yang bersifat transnasional ini akan menimbulkan masalahnya sendiri berkenaan dengan yurisdiksi.

Seringkali masalah ini menjadi sangat pelik karena kendala sebuah teritorial batas negara. Yurisdiksi dalam hal ini telah mencakup dan bertanggungjawab atas orang, benda atau peristiwa hukum yang terjadi didalamnya. Hukum Internasional telah membagibeberapa prinsip yang dapat menjadi acuan dalam masalah yurisdiksi yakni prinsip teritorial, prinsip nasionalitas, prinsip perlindungan, serta prinsip universal (Mansur & Gultom, 2005).

1. Prinsip teritorial: prinsip ini tergolong pada prinsip yang paling utama dan fundamental dalam suatu kasus yurisdiksi, dimana negara berhak atas segala kasus yang terjadi dan berada dalam wilayahnya.
2. Prinsip nasionalitas: dalam prinsip ini negara dianggap berhak untuk mengadili setiap warganegaraanya terhadap segala kejahatan yang dilakukannya dimanapun warga negara tersebut berada.
3. Prinsip perlindungan: prinsip ini lebih bersifat melindungi kepentingan vital negaranya.
4. Prinsip universal: prinsip ini lebih bersifat umum dan sebagian dapat diterima oleh masyarakat umum, dimana dalam yurisdiksi ini setiap negara dianggap berhak atau dapat mengadili suatu kejahatan tertentu yang dianggap membahayakan masyarakat dalam lingkup internasional.

Salah satu cara yang dapat dilakukan oleh negara yang memiliki yurisdiksi terhadap pelaku kejahatan yang berada di negara lain adalah dengan meminta kepada negara di tempat pelaku tersebut berada agar dapat menangkap pelaku tersebut. Yurisdiksi terhadap kejahatan mayantara (cybercrime) khususnya dalam tindak pidana peretasan (hacking) dapat dilaksanakan melalui kerja sama internasional berupa ekstradisi, bantuan hukum timbal balik, dan kerjasama antar penegak hukum.

Mengenai ruang lingkup berlakunya hukum pidana dalam kejahatan mayantara ini telah diatur dalam Kitab Undang-Undang Hukum Pidana Indonesia (KUHP) dalam BAB I Buku Kesatu Kitab Undang-Undang Hukum Pidana (KUHP) mengenai batas-batas berlakunya suatu aturan dalam hukum pidana, yang mana hal tersebut termuat sembilan pasal dimulai dari pasal 1 sampai dengan pasal 9. Dalam pasal 1 tersebut diatur mengenai batas berlakunya suatu hukum pidana berdasarkan waktu, sedangkan untuk pasal 2 sampai dengan pasal 9 memuat mengenai batas berlakunya hukum pidana berdasarkan atas tempat terjadinya.

Berkenaan dengan hal tersebut, penegakan hukum mengenai tindak pidana peretasan yang masuk ke dalam ranah kejahatan mayantara dapat dimulai dan dibangun melalui kesadaran masyarakatnya sendiri. Dengan karakteristik yang berbeda dibandingkan dengan kejahatan seperti pembunuhan, pemerkosaan, dan kejahatan lainnya, menyebabkan dalam mengungkap kejahatan ini diharuskan menggunakan teknologi.

Upaya Penanganan Kejahatan Mayantara (Cybercrime)

Undang-Undang No. 19 Tahun 2016 yang merupakan perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang merupakan piranti hukum terbesar yang diharapkan dapat mengakomodir segala jenis pelanggaran dalam bidang IT. Disamping terdapat perlindungan hukum, disana juga terdapat ancaman sanksi pidana atas pelanggaran yang dilakukan.

Tindak pidana peretasan yang diatur dalam pasal 30 ayat (1), (2), dan (3) mengandung unsur sebagai berikut.

Pasal 30 ayat (1) UU ITE: “setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun”.

Dalam pasal ini sudah jelas tertera unsur setiap orang, unsur dengan sengaja dan tanpa hak melawan hukum, unsur mengakses komputer dan/ atau sistem elektronik milik orang lain, serta unsur dengan cara apapun.

- a. Unsur setiap orang
Dalam unsur ini setiap orang yang dimaksud adalah orang sebagai subjek hukum yang dapat bertanggungjawab dan cakap hukum berdasarkan atas Perundang-Undangan.
- b. Unsur dengan sengaja dan tanpa hak melawan hukum
Unsur ini merujuk pada niat atau kesengajaan dan penuh dengan kesadaran dari orang tersebut dalam melakukan suatu tindakan yang melawan hukum.
- c. Unsur mengakses komputer dan/ atau sistem elektronik milik orang lain
Unsur ini memberi gambaran bahwa sistem elektronik milik orang lain itu berarti hal yang bersifat pribadi milik orang lain dan bukan bersifat untuk umum.
- d. Unsur dengan cara apapun
Dengan cara apapun yang dimaksud dalam hal ini adalah baik peretas tersebut masuk menggunakan perangkat milik korban yang diretas atau melalui perangkat atau jaringan internet.

Dalam pasal 30 ayat 1 ini setiap orang dilarang secara tegas masuk kedalam sistem elektronik milik orang lain yang bersifat privasi atau pribadi. Sanksi pidananya dapat menjerat pelaku peretasan tersebut telah diatur secara jelas dalam pasal 46 ayat 1 yakni “setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 30 ayat (1), dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/ atau denda paling banyak Rp.600.000.000,00 (enam ratus juta rupiah).

Pasal 30 ayat (2) UU ITE: “setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/ atau sistem elektronik milik orang lain dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/ atau dokumen elektronik”.

Dalam pasal 30 ayat (2) ini memiliki unsur yang sama seperti pada pasal 30 ayat (1), namun ayat (2) terdapat unsur memperoleh informasi elektronik dan/ atau dokumen elektronik, hal tersebut berarti orang yang mencoba masuk kedalam sistem tersebut memiliki tujuan untuk mencuri suatu data atau informasi elektronik yang terdapat dalam sistem milik korban. Pasal 30 ayat (2) ini berkaitan langsung dengan pasal 46 ayat (2) mengenai ancaman pidana jika melanggar ketentuan pasal 30 ayat (2):

“Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 30 ayat (2), dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/ atau denda paling banyak Rp.700.000.000,00 (tujuh ratus juta rupiah)”.

Unsur dalam pasal 30 ayat (3) terdapat unsur dengan melanggar, menerobos, melampaui, atau menjebol sistem keamanan. Unsur ini memberi indikasi bahwa pelaku peretasan atau *hacker* melakukan tindakan tersebut dengan cara menerobos sistem keamanan komputer tersebut. Untuk sanksi pidananya sendiri telah diatur dalam pasal 46 ayat (3) dimana untuk pelanggaran tersebut dikenakan hukuman kurungan penjara seberat-beratnya 8 (delapan) tahun dan/atau membayar denda sebanyak-banyaknya Rp.800.000.000,00 (delapan ratus juta rupiah).

Pemberatan penjatuhan pidana bagi pelaku peretasan berdasarkan atas objek dan subjek dari tindak pidana yang bersangkutan, yaitu:

1. Berdasarkan objek tindak pidana peretasan atau hacking
 - a. Pasal 52 ayat (2) UU ITE
Dalam pasal ini pemberatan penjatuhan hukuman pidana bagi pelaku tindak pidana peretasan apabila objek dari pelanggaran ini adalah sistem elektronik yang dimiliki oleh pemerintah atau sistem yang dipergunakan untuk pelayanan publik.
 - b. Pasal 52 ayat (3) UU ITE
Pemberatan dalam pasal ini dapat dijatuhkan apabila pelaku peretasan menyerang situs web milik pemerintah yang berhubungan langsung dengan keamanan atau stabilitas negara.
2. Berdasarkan objek tindak pidana peretasan atau hacking
 - a. Pasal 52 ayat (2) UU ITE

Dalam pasal ini pemberatan penjatuhan hukuman pidana bagi pelaku tindak pidana peretasan apabila objek dari pelanggaran ini adalah sistem elektronik yang dimiliki oleh pemerintah atau sistem yang dipergunakan untuk pelayanan publik.

b. Pasal 52 ayat (3) UU ITE

Pemberatan dalam pasal ini dapat dijatuhkan apabila pelaku peretasan menyerang situs web milik pemerintah yang berhubungan langsung dengan keamanan atau stabilitas negara.

3. Berdasarkan atas subjek tindak pidana peretasan atau hacking

Pasal 52 ayat (4) UU ITE, pemberatan dapat dijatuhkan apabila terbukti bahwa peretasan tersebut dilakukan oleh korporasi.

Pemerintah dalam melakukan upaya menanggulangi kejahatan mayantara dengan skala nasional telah menerapkan peraturan Perundang-Undangan yang mengatur secara khusus mengenai IT. Undang-Undang No. 19 Tahun 2016 perubahan atas Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Kejahatan yang tanpa mengenal batas ini bisa saja sangat membahayakan jika tidak ditanggulangi dan tidak memiliki payung hukum yang kuat untuk mengakomodirnya.

Upaya penanggulangan kejahatan tersebut dapat berupa upaya preventif dan upaya represif (Alam & Ilyas, 2018).

1. Upaya preventif

Upaya ini merupakan upaya pencegahan yang dilakukan guna mencegah timbulnya suatu kejahatan didalam lingkup masyarakat. Beberapa hal yang dapat dilakukan guna mencegah terjadinya suatu kejahatan adalah dengan melakukan edukasi terhadap masyarakat, melakukan pemblokiran, membentuk Badan Siber dan Sandi Negara (BSSN).

2. Upaya represif

Upaya ini merupakan salah satu upaya yang bersifat konsepsional, dimana upaya ini dilakukan setelah terjadinya suatu kejahatan. Upaya ini bertujuan untuk menindak pelaku kejahatan seperti penjatuhan sanksi atau penjatuhan pidana sesuai dengan pelanggaran yang telah dilakukan.

IV. SIMPULAN DAN SARAN

Simpulan

Berdasarkan hasil dan pembahasan di atas, ada beberapa simpulan yang dapat dibuat, yaitu: pertama, penegakan hukum yang dilakukan terhadap tindak pidana peretasan atau hacking yang tergolong ke dalam ranah kejahatan mayantara atau *cybercrime* dilakukan dengan menerapkan Undang-Undang No. 19 Tahun 2016 yang merupakan perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-undang ini akan memberikan sanksi berupa membayar denda serta hukuman kurungan penjara sebagaimana telah dicantumkan dalam pasal 30 ayat (1), (2), dan (3). Sanksi pidananya telah diatur dalam pasal 46 ayat (1),(2), dan (3). Kedua, upaya dalam melakukan penanggulangan kejahatan mayantara atau *cybercrime* telah mengacu pada Undang-Undang Informasi dan Transaksi Elektronik, dan berbagai upaya lain seperti upaya preventif seperti pemblokiran, edukasi terhadap masyarakat, dan hal-hal positif lainnya yang dapat mencegah terjadinya suatu kejahatan, serta melakukan upaya represif yang mana upaya ini dilakukan setelah terjadinya suatu tindak pidana, seperti penjatuhan sanksi terhadap pelaku.

Saran

Selain simpulan, ada beberapa saran yang perlu disampaikan berdasarkan hasil penelitian ini, yaitu: diharapkan agar dalam prakteknya segala bentuk pelanggaran dapat ditindak sesuai dengan hukum yang berlaku, dan ketentuan hukum dalam Undang-Undang No. 19 Tahun 2016 perubahan atas Undang-Undang No.11 Tahun 2008 dilaksanakan dengan baik dan bijak serta dapat menjadi payung hukum bagi masyarakat luas. Selain itu, pemerintah dalam mengemban tugasnya hendaknya melakukan kerja sama antar lembaga guna tercapainya keselarasan, keseimbangan serta kenyamanan dimasyarakat, dan mengoptimalkan segala bentuk sanksi dalam penjatuhan pidana agar memberikan efek jera bagi pelaku.

DAFTAR PUSTAKA

- Alam, A. S., & Ilyas, A. (2018). *Kriminologi: Suatu Pengantar* (1st ed.).
Hartono, B. (2014). Hacker Dalam Perspektif Hukum Indonesia. *MMH*, 43(1), 23–30.

- Mansur, D. M. A., & Gultom, E. (2005). *Cyber Law : Aspek Hukum Teknologi Informasi*.
- Muthia, F. R., & Arifin, R. (2019). Kajian Hukum Pidana pada Kasus Kejahatan Mayantara (Cybercrime) dalam Perkara Pencemaran Nama Baik di Indonesia. *Resam Jurnal Hukum*, 5(1), 21–39.
- Ngafifi, M. (2014). Kemajuan Teknologi dan Pola Hidup Manusia dalam Perspektif Sosial Budaya. *Jurnal Pembangunan Pendidikan: Fondasi Dan Aplikasi*, 2(1), 33–47.
- Nugroho, I. Y. (2015). Sanksi Hukum Kejahatan Peretasan Website Presiden Republik Indonesia. *AL-DAULAH: JURNAL HUKUM DAN PERUNDANGAN ISLAM*, 5(1), 171–203.
- Purnomo. (2002). Kebijakan Hukum terhadap Kejahatan Cybercrime di Era Informasi dan Masyarakat Virtual. *PALIMPSEST*, 9(2), 77–83.
- Rahmawati, I. (2017). Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) dalam Peningkatan Cyber Defense. *Jurnal Pertahanan & Bela Negara*, 7(2), 51–66.
- Setiawan, D. (2018). Dampak Perkembangan Teknologi Informasi dan Komunikasi terhadap Budaya. *JURNAL SIMBOLIKA: Research and Learning in Communication Study*, 4(1), 62–72.
- Wahid, A., & Labib, M. (2005). *Kejahatan Mayantara (Cyber Crime)* (1st ed.).