



Aplikasi Whatsapp Bajakan sebagai Ancaman Kejahatan Siber di Indonesia

INFO PENULIS

Angelia Pratiwi Mastiurlani Christina Sitorus
Universitas Panca Bhakti
apmchristys@upb.ac.id

Agustinus Astono*
Universitas Panca Bhakti
agustinusastono@upb.ac.id

INFO ARTIKEL

ISSN: 2808-1307
Vol. 4, No. 1, April 2024
<http://jurnal.ardenjaya.com/index.php/ajsh>

*Korespondensi Author

© 2024 Arden Jaya Publisher All rights reserved

Saran Penulisan Referensi:

Sitorus, A. P. M. C., & Astono, A. (2024). Aplikasi Whatsapp Bajakan sebagai Ancaman Kejahatan Siber di Indonesia. *Arus Jurnal Sosial dan Humaniora*, 4 (1), 157-162

Abstrak

Fenomena penggunaan aplikasi WhatsApp bajakan menjadi sorotan penting dalam ranah keamanan siber di Indonesia. Meskipun menawarkan fitur-fitur menarik, seperti pesan anti-lihat dan penyembunyian status online, aplikasi ini melanggar hak cipta serta menimbulkan ancaman terhadap privasi data pengguna. Penelitian ini bertujuan untuk mengungkap peran dan dampak penggunaan aplikasi WhatsApp bajakan terhadap keamanan siber di Indonesia. Dengan menggunakan pendekatan yuridis normatif dan analisis kualitatif terhadap data hukum dan literatur terkait, studi ini mengungkap bahwa penggunaan aplikasi WhatsApp bajakan memicu risiko kebocoran data pribadi dan pelanggaran hak cipta yang berpotensi menimbulkan konsekuensi hukum yang serius. Kesadaran masyarakat akan risiko penggunaan aplikasi bajakan dan penegakan hukum yang efektif menjadi kunci dalam melindungi keamanan dan privasi di era digital yang semakin kompleks.

Kata Kunci: Ancaman privasi, Fouads Mod, Keamanan siber, WhatsApp bajakan, Whatsapp Mod

Abstract

The phenomenon of using pirated WhatsApp applications has become an important focus of cybersecurity in Indonesia. Despite offering attractive features, such as anti-view messages and online status hiding, these apps infringe copyrights and pose a threat to users' data privacy. This study aims to reveal the role and impact of pirated WhatsApp applications on cybersecurity in Indonesia. Using a normative juridical approach and qualitative analysis of legal data and related literature, this study reveals that the use of pirated WhatsApp applications triggers the risk of personal data leakage and copyright infringement with potentially serious legal consequences. Public awareness of the risks of using pirated apps and effective law enforcement is key to protecting security and privacy in an increasingly complex digital era.

Key Words: Privacy threats, Fouads Mod, Cybersecurity, pirated WhatsApp, Whatsapp Mod

A. Pendahuluan

Pada masa ini, teknologi berkembang dengan sangat cepat. Perkembangan teknologi tersebut menciptakan inovasi yang kemudian memudahkan manusia untuk melakukan aktivitasnya. Adapun kemudahan manusia untuk melakukan aktivitas sekaligus interaksi dilihat dari semakin berkembangnya akses komunikasi sosial yang mana bermanfaat tidak hanya untuk melakukan interaksi manusia semata tetapi dapat juga digunakan sebagai sarana lain seperti perdagangan dan akses pembelajaran. Berdasarkan data dari Databoks yang merupakan platform statistik ekonomi dan bisnis yang merupakan bagian dari Katadata, sebuah perusahaan yang bergerak dalam riset dan media daring, pada bulan Januari tahun 2024, mendapatkan data bahwa aplikasi media sosial yang paling banyak digunakan adalah Whatsapp, Instagram, Facebook, TikTok dan Telegram (Annur, n.d.).

Whatsapp sebagai aplikasi yang paling banyak digunakan di Indonesia, tidak terlepas dari fitur-fiturnya yang memudahkan penggunaannya. Fitur-fitur tersebut antara lain ialah menerima dan mengirim berbagai macam media seperti teks, video, foto, suara, dan sebagainya (Koten et al., 2022). Whatsapp sebagai media komunikasi dengan pengguna yang banyak kemudian menambahkan beberapa fitur untuk menjaga keamanan para penggunaannya, fitur tersebut seperti pesan sekali lihat, pemblokir kontak, dan verifikasi keamanan dua langkah. Adapun dengan beberapa fitur canggih tersebut tidak menjamin keamanan para pengguna Whatsapp asli terhadap para pengguna atau dalam hal ini pembajak yang menggunakan Whatsapp modifikasi atau yang biasa disingkat menjadi *WA Mod*.

Aplikasi Whatsapp modifikasi merupakan aplikasi tiruan atau bajakan aplikasi Whatsapp asli. Adapun fitur-fitur yang disediakan oleh aplikasi Whatsapp bajakan antara lain ialah fitur pesan anti sekali lihat, menonaktifkan pesan dibaca, menyembunyikan pengguna melihat status yang dibagikan orang lain, menonaktifkan status online, mengirim foto tidak terbatas dan mengirim durasi video panjang dengan ukuran yang tidak terbatas. Adapun pada saat ini, pengembang aplikasi Whatsapp bajakan di dunia siber sangat banyak, salah satu pengembangnya ialah seperti Fouads Mod atau *FMWA*. Berdasarkan beberapa fitur canggih yang ada dalam Whatsapp bajakan yang dikembangkan oleh berbagai pengembang aplikasi tersebut, memunculkan kekhawatiran terkait dengan tindakan kejahatan siber dalam bidang komunikasi yang dapat dilakukan oleh para penggunaannya (Tayebi et al., 2020).

Kejahatan siber adalah aktivitas melanggar hukum apa pun yang dilakukan melalui komputer atau jaringan yang saling terkoneksi satu sama lain (Dubey & Pateriya, 2023). Adapun kegiatan kejahatan siber sebagian besar didasarkan atas keuntungan materil, tetapi ada pula yang bertujuan untuk mengganggu atau membongkar sistem dan fitur pertahanan tertentu. Kejahatan siber menggunakan internet sebagai medianya untuk menyebarkan virus, data ilegal, atau konten yang tidak pantas. Kejahatan siber secara khusus menyerang seluruh hal yang tersambung dengan media internet, seperti menginfeksi komputer atau *smartphone* dengan virus yang dapat menyebar ke seluruh jaringan perangkat tersebut. Penyimpangan siber ini menimbulkan kerugian finansial, seperti serangan *ransomware*, penipuan online, pencurian identitas, dan upaya mencuri informasi keuangan sensitif seperti rincian rekening bank atau kartu kredit dan sebagainya.

Berdasarkan Undang-Undang Hak Cipta, aktivitas pembajakan sebagaimana dalam dilakukan dalam Whatsapp modifikasi dapat dikenakan pidana dengan ketentuan Pasal 113 ayat (3) dan (4). Sedangkan, berdasar pada Pasal 35 Undang-Undang Nomor 11 Tahun 2008 tentang Transaksi dan Informasi Elektronik (UU ITE), kegiatan pembajakan dapat diartikan sebagai kegiatan yang sengaja dan tidak sah atau melanggar hukum melakukan modifikasi, pembuatan, perubahan, penghapusan, atau merusak informasi elektronik dan/atau dokumen elektronik dengan maksud untuk membuat informasi tersebut terlihat autentik. Adapun ketentuan pidana terkait dengan aktivitas pembajak didalam UU ITE dapat ditemukan dalam Pasal 51 ayat (1), yang menyatakan bahwa setiap individu yang memenuhi kriteria sebagaimana yang dijelaskan dalam Pasal 35 dapat dikenakan hukuman pidana penjara dengan maksimal durasi 12 tahun dan/atau denda setinggi Rp12.000.000.000,00 (dua belas miliar rupiah).

Kegiatan pembajakan aplikasi Whatsapp tidak hanya menimbulkan kerugian bagi pengembang aplikasi Whatsapp, kerugian lain yang dapat ditimbulkan ialah pengguna

Whatsapp asli sangat rentan terkait dengan kebocoran data pribadinya saat melakukan komunikasi dengan para pengguna Whatsapp bajakan. Kebocoran data ini, antara lain dapat disebabkan oleh hilangnya fitur sekali kirim/sekali lihat dalam Whatsapp bajakan sehingga pengguna Whatsapp bajakan leluasa mengakses pesan elektronik yang telah dikirimkan oleh pengguna Whatsapp asli. Penggunaan terkait dengan aplikasi Whatsapp bajakan sangatlah berbahaya terutama pada data-data pribadi pemilik maupun kontak-kontak yang pemilik simpan karena rentan dibobol oleh pengembang aplikasi whatsapp bajakan tersebut.

Berdasarkan permasalahan tersebut, maka kajian ini berjudul "**Aplikasi Whatsapp Bajakan sebagai Ancaman Kejahatan Siber di Indonesia**". Rumusan masalahnya ialah mengapa aplikasi Whatsapp bajakan sebagai ancaman kejahatan siber di Indonesia. Kajian ini bertujuan untuk melakukan riset peranan dan konsekuensi yang ditimbulkan oleh penggunaan aplikasi WhatsApp bajakan sebagai ancaman terhadap keamanan siber di Indonesia. Dengan adanya studi ini, diharapkan dapat tercapai pemahaman yang lebih mendalam mengenai tren penggunaan aplikasi Whatsapp bajakan serta risiko potensial terkait kejahatan siber, sehingga dapat memberikan landasan bagi perumusan kebijakan dan strategi mitigasi yang efektif dalam menghadapi permasalahan ini.

B. Metodologi

Dalam konteks penelitian yang berjudul "Aplikasi Whatsapp Bajakan sebagai Ancaman Kejahatan Siber di Indonesia", pendekatan metodologi yang diterapkan menekankan pada pendekatan yuridis normatif. Data yang dikumpulkan mencakup dokumen-dokumen hukum seperti peraturan perundang-undangan, putusan pengadilan terkait kejahatan siber, dan laporan resmi pemerintah yang relevan. Selain itu, literatur hukum seperti buku, jurnal, dan opini para ahli juga menjadi sumber data. Dengan memanfaatkan metode analisis kualitatif, penelitian ini menginterpretasikan informasi hukum dengan cermat untuk mengidentifikasi dampak dan implikasi dari penyebaran aplikasi WhatsApp bajakan dalam konteks kejahatan siber di Indonesia. Dengan demikian, melalui pendekatan ini, penelitian tersebut bertujuan untuk menyajikan pemahaman yang mendalam tentang fenomena tersebut dan memberikan kesimpulan yang didasarkan pada konteks hukum yang relevan.

C. Hasil dan Pembahasan

Penggunaan situs media sosial seperti Line, Facebook, Telegram, Blackberry Massanger, WhatsApp, dan platform lainnya telah menjadi kegiatan umum di masyarakat, yang dipengaruhi oleh kemajuan teknologi informasi. Seiring dengan perkembangan media sosial, terjadi perubahan dalam pola perilaku masyarakat terkait budaya, etika, dan norma yang diterima. Privasi menjadi isu krusial bagi individu dan lembaga yang terlibat dalam interaksi dengan orang lain atau institusi lainnya. Pelanggaran privasi dapat menyebabkan kerugian baik secara finansial maupun non-finansial, terutama jika informasi yang diungkapkan berkaitan dengan kekuatan dan strategi organisasi yang dapat digunakan dalam persaingan dengan pesaing. Kerentanan terhadap pencurian informasi pribadi, seperti tanggal lahir, email, dan foto pribadi, merupakan hasil umum dari kegagalan dalam mengatur privasi dalam layanan online.

Kerentanan terhadap keamanan privasi dan kebocoran data merupakan diskursus yang esensial pada masa ini. Hal tersebut disebabkan oleh ketergantungan manusia terhadap inovasi teknologi yang terjadi dalam hal ini khususnya sosial media, sehingga membuka peluang besar bagi para peretas untuk mencuri data pribadi orang lain yang terdapat dalam sosial medianya. Kasus seperti peretasan terhadap suatu aplikasi media sosial seperti Whatsapp sering terjadi di Indonesia. Sebagai contoh, kasus yang menimpa Narasi TV, sebuah perusahaan jurnalisme dan berita di Indonesia, adalah saat sebagian besar akun WhatsApp karyawannya diretas pada tahun 2022. Contoh lainnya ialah pada tahun 2023, peretasan akun Whatsapp milik selebritis bernama Baim Wong yang mana peretas menggunakan modus *phising* seperti mengirimkan tautan link, gambar, aplikasi yang telah dimodifikasi dengan virus berbahaya.

Modus-modus dalam pencurian data pribadi dilakukan dengan berbagai cara, adapun secara khusus dalam perangkat *smartphone* modusnya pencurian data pribadi dilakukan dengan cara, antara lain:

1. Aplikasi Berbahaya

Metode umum bagi pelaku pencurian data pribadi dalam mengambil data pribadi pengguna lain dari perangkat seluler adalah dengan menggunakan aplikasi berbahaya yang sering kali menyamar sebagai perangkat lunak yang sah (Wang et al., 2019). Aplikasi tersebut, dengan mungkin meminta izin agar dapat mengakses sejumlah besar data pribadi seperti kontak, email, dan informasi keuangan dari pengguna. Setelah diinstal, aplikasi tersebut secara diam-diam mengirimkan data tersebut ke server jarak jauh yang dikendalikan oleh pelaku pencurian data pribadi.

2. Serangan *Phishing*

Pelaku pencurian data pribadi umumnya melancarkan serangan *phishing* pada perangkat seluler melalui email, SMS atau panggilan suara. Pelaku pencurian data pribadi memanipulasi pengguna dengan pesan yang tampaknya berasal dari sumber yang sah, dengan tujuan membuat pengguna memberikan informasi sensitif seperti kredensial login atau nomor kartu kredit. Tautan atau lampiran berbahaya dalam pesan tersebut mendorong pengguna untuk melakukan tindakan yang mengakibatkan pelanggaran data (Kim et al., 2015).

3. *Spyware* dan *Stalkerware*

Spyware dan *stalkerware* merupakan jenis *malware* yang telah didesain khusus untuk memantau serta merekam aktivitas yang terjadi pada perangkat seluler tanpa sepengetahuan pengguna (Cha & Pak, 2018). Perangkat lunak atau aplikasi tersebut memiliki kemampuan untuk melacak lokasi, merekam panggilan, mencatat penekanan tombol, serta mengakses pesan dan email. Informasi yang terkumpul dapat dimanfaatkan untuk berbagai tujuan yang bersifat merugikan, termasuk pencurian identitas dan pemerasan (Shridhar Kakade & Khaiyum, 2023).

4. Sistem Operasi dan Aplikasi *Outdate*

Pelaku pencurian data pribadi sering memanfaatkan kerentanan keamanan yang ada pada sistem operasi dan aplikasi yang keamanannya sudah tidak relevan atau kadaluwarsa untuk mendapatkan akses tidak sah ke perangkat seluler (Astono, 2022). Setelah berhasil mendapatkan akses, pelaku pencurian data pribadi dapat mengambil data pribadi pengguna lain dan bahkan mengendalikan seluruh perangkat.

Berdasarkan metode-metode pencurian data pribadi tersebut, aplikasi Whatsapp bajakan merupakan aplikasi berbahaya dengan modus pencurian data pribadi dengan cara *spyware*. Adapun aplikasi Whatsapp bajakan didesain mirip dengan aplikasi yang aslinya, kemudian aplikasi tersebut ditambahkan berbagai fitur khusus agar menjadi daya tarik dan di-install oleh orang lain. hal ini kemudian menimbulkan akses tidak sah terhadap perangkat orang lain.

Akses tidak sah adalah sebuah kegiatan atau tindakan akses tidak sah ke sistem dan perangkat *smartphone* merujuk pada upaya untuk memperoleh akses tanpa izin ke jaringan, sistem, aplikasi perangkat lunak, data, atau sumber daya lainnya (Kyrychenko, 2018). Tindakan semacam ini melanggar kebijakan keamanan yang telah ditetapkan oleh pemilik perangkat, dan bisa terjadi dalam berbagai bentuk, baik secara digital maupun fisik. Berdasarkan hal tersebut, penggunaan aplikasi Whatsapp bajakan dapat menimbulkan implikasi kebocoran data bagi penggunanya. Selain hal tersebut, penggunaan aplikasi Whatsapp bajakan juga berakibat hukum bagi para penggunanya dikarenakan pengguna menginstall sebuah aplikasi bajakan atau yang dilarang.

Berdasarkan ketentuan hukum internasional, penggunaan aplikasi bajakan sudah diatur dalam beberapa konvensi internasional. Aturan internasional yang mengatur penggunaan aplikasi bajakan utamanya didasarkan pada hukum dan perjanjian hak cipta, di mana Konvensi Perserikatan Bangsa-Bangsa tentang Hukum Laut (*United Nations Convention on the Law of the Sea*) dan Organisasi Kekayaan Intelektual Dunia (*World Intellectual Property Organization*)

menjadi fondasi awal terkait dengan munculnya aturan terkait dengan pembajakan aplikasi (Danaher et al., 2014). Aturan internasional tersebut kemudian berkembang melalui beberapa konvensi seperti konvensi Berne untuk Perlindungan Karya Sastra dan Seni, Perjanjian TRIPS tentang Aspek Terkait Perdagangan Hak Kekayaan Intelektual, serta Perjanjian Hak Cipta WIPO (WCT), menguraikan perlindungan hak cipta bagi pencipta dan penulis secara internasional. Meskipun tidak secara spesifik menyinggung “aplikasi bajakan,” kerangka kerja ini memberikan dasar bagi perlindungan hak cipta, yang dapat dilanggar oleh praktik pembajakan seperti penggunaan aplikasi bajakan (Rahman & Pandey, 2020).

Di Indonesia aturan terkait pembajakan aplikasi dapat ditemukan dalam beberapa ketentuan hukum seperti Undang-Undang Hak Cipta dan Undang-Undang Informasi dan Transaksi Elektronik. Berdasarkan Pasal 113 ayat (3) dan (4) Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta, aktivitas pembajakan atau penggunaan aplikasi bajakan sebagaimana dalam dilakukan dalam Whatsapp modifikasi dapat dikenakan pidana, yang mana disebutkan bahwa seseorang yang tanpa izin dari Pencipta atau pemegang Hak Cipta melakukan pelanggaran terhadap hak ekonomi Pencipta, seperti yang diatur dalam Pasal 9 ayat (1) huruf a, huruf b, huruf e, dan/atau huruf g untuk kepentingan komersial, dapat dikenai hukuman penjara hingga empat tahun dan/atau denda maksimum satu miliar rupiah. Jika pelanggaran tersebut terjadi dalam bentuk pembajakan, maka hukumannya adalah penjara hingga sepuluh tahun dan/atau denda maksimum empat miliar rupiah. Ketentuan hukum pidana dalam Undang-Undang Hak Cipta tersebut dapat dimaknai bahwa pengguna aplikasi bajakan maupun pelaku yang melakukan pembajakan atau memodifikasi suatu aplikasi tanpa izin yang memiliki hak cipta tidak terlepas dari ancaman hukuman pidana (Koen & Im, 1997).

Berdasarkan Pasal 35 Undang-Undang Informasi dan Transaksi elektronik, dinyatakan bahwa setiap orang yang dengan sengaja dan tanpa izin atau melanggar hukum melakukan tindakan seperti manipulasi, penciptaan, perubahan, penghilangan, atau pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan maksud agar informasi tersebut dianggap sebagai data yang otentik. Berdasarkan Pasal 35 tersebut, mengindikasikan bahwa pelaku yang melakukan pembajakan dalam hal ini yang melakukan modifikasi aplikasi Whatsapp menjadi bajakan dikategorisasikan sebagai suatu hal yang bertentangan dengan hukum. Oleh sebab itu, pada Pasal 51 ayat (1) Undang-Undang Informasi dan Transaksi elektronik, kemudian sanksi pidana yang menyatakan bahwa, “Setiap orang yang memenuhi syarat sebagaimana yang dijelaskan dalam Pasal 35 dapat dihukum dengan pidana penjara maksimum dua belas tahun dan/atau denda maksimum dua belas miliar rupiah”.

Meskipun pengguna mendapatkan berbagai macam fitur premium pada aplikasi Whatsapp bajakan, pengguna aplikasi tersebut juga dapat memicu resiko bocornya data pribadi pengguna yang mana dapat merugikan secara materiil. Penggunaan aplikasi Whatsapp bajakan juga beresiko melanggar hukum karena dianggap melanggar hak cipta dan melakukan modifikasi secara ilegal tanpa sepengetahuan pemilik hak cipta. Berdasarkan hal tersebut, selain menghadapi risiko keamanan data pribadi, pengguna juga terlibat dalam pelanggaran hukum yang dapat memiliki konsekuensi hukum serius (Tomczyk, 2021).

D. Kesimpulan

Penggunaan aplikasi WhatsApp bajakan telah menjadi sumber kekhawatiran terkait dengan ancaman keamanan siber di Indonesia. Meskipun aplikasi ini menawarkan fitur tambahan yang menarik bagi pengguna, seperti pesan anti-lihat dan kemampuan untuk menyembunyikan status online, penggunaan aplikasi ini melanggar hak cipta dan berpotensi membahayakan data pribadi pengguna. Pelanggaran hak cipta ini merujuk pada penyalahgunaan software yang dilindungi oleh undang-undang hak cipta tanpa izin dari pemegang hak cipta, yang merupakan tindakan ilegal dan dapat berdampak serius bagi pengembang asli dan pengguna aplikasi tersebut. Selain hal tersebut, aplikasi WhatsApp bajakan juga berpotensi membocorkan data pribadi pengguna karena seringkali tidak memiliki standar keamanan yang sama dengan aplikasi resmi. Implikasi hukum dari penggunaan WhatsApp bajakan juga patut diperhatikan, dengan adanya sanksi pidana yang dapat dikenakan sesuai dengan ketentuan yang ada dalam Undang-Undang Hak Cipta dan Undang-Undang

Informasi dan Transaksi Elektronik. Oleh sebab itu, masyarakat perlu meningkatkan kesadaran akan risiko yang terkait dengan penggunaan aplikasi bajakan dan mengambil langkah-langkah untuk melindungi keamanan dan privasi mereka, seperti menggunakan aplikasi resmi yang disediakan oleh pengembang yang sah. Di samping hal tersebut, pemerintah dan lembaga terkait juga memiliki peran penting dalam menegakkan hukum dan menerapkan kebijakan yang efektif untuk melindungi masyarakat dari ancaman kejahatan siber yang semakin kompleks. Upaya bersama antara masyarakat, pemerintah, dan sektor swasta diperlukan untuk mengatasi masalah ini dan menciptakan lingkungan digital yang lebih aman dan terpercaya bagi semua orang.

E. Referensi

- Annur, C. M. (n.d.). *Ini Media Sosial Paling Banyak Digunakan di Indonesia Awal 2024*. Retrieved April 1, 2024, from <https://databoks.katadata.co.id/datapublish/2024/03/01/ini-media-sosial-paling-banyak-digunakan-di-indonesia-awal-2024>
- Astono, A. (2022). Perlindungan Hukum Mengenai Kebocoran Data Pribadi Terhadap Akun Microsoft Office 365 Yang Dibeli Melalui Shopee. *Justitia et Pax*, 38(2), 111–145. <https://doi.org/10.24002/jep.v38i2.6339>
- Cha, Y., & Pak, W. (2018). Protecting contacts against privacy leaks in smartphones. *PLOS ONE*, 13(7), e0191502. <https://doi.org/10.1371/journal.pone.0191502>
- Danaher, B., Smith, M. D., & Telang, R. (2014). Piracy and Copyright Enforcement Mechanisms. *Innovation Policy and the Economy*, 14, 25–61. <https://doi.org/10.1086/674020>
- Dubey, P., & Pateriya, S. (2023). Social Media and Cybercrime: A Sociodemographic Study of Awareness Level Among Indian Youth. In *Cybercrime in Social Media* (pp. 23–40). Chapman and Hall/CRC. <https://doi.org/10.1201/9781003304180-2>
- Kim, Y., Oh, T., & Kim, J. (2015). Analyzing User Awareness of Privacy Data Leak in Mobile Applications. *Mobile Information Systems*, 2015, 1–12. <https://doi.org/10.1155/2015/369489>
- Koen, C. M., & Im, J. H. (1997). Software piracy and its legal implications. *Information & Management*, 31(5), 265–272. [https://doi.org/10.1016/S0378-7206\(96\)01090-7](https://doi.org/10.1016/S0378-7206(96)01090-7)
- Koten, F. P. N., Jufriansah, A., & Hikmatiar, H. (2022). Analisis Penggunaan Aplikasi Whatsapp sebagai Media Informasi dalam Pembelajaran: Literature Review. *Jurnal Ilmu Pendidikan (JIP) STKIP Kusuma Negara*, 14(1), 72–84. <https://doi.org/10.37640/jip.v14i1.1409>
- Kyrychenko, V. (2018). “Piracy is a Land-Based Crime”: Analysis of Definition, Drivers, and Governmental Policy. *Journal of Maritime Studies and National Integration*, 2(1), 45. <https://doi.org/10.14710/jmsni.v2i1.3060>
- Rahman, F., & Pandey, P. (2020). Online Software Piracy and Its Related Laws. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3648512>
- Shridhar Kakade, A. S., & Khaiyum, S. (2023). Data Leaks and Its Prevention In Mobile Application. *International Journal of Engineering Research & Technology (IJERT)*, 11(6), 1–8. <https://doi.org/10.17577/NCRTCA-PID-047>
- Tayebi, M. A., Glässer, U., & David B. Skillicorn. (2020). *Open Source Intelligence and Cyber Crime: Social Media Analytics* (M. A. Tayebi, U. Glässer, & D. B. Skillicorn, Eds.). Springer International Publishing. <https://doi.org/10.1007/978-3-030-41251-7>
- Tomczyk, Ł. (2021). Evaluation of Digital Piracy by Youths. *Future Internet*, 13(1), 11. <https://doi.org/10.3390/fi13010011>
- Wang, Y., Chen, Y., Ye, F., Liu, H., & Yang, J. (2019). Implications of smartphone user privacy leakage from the advertiser’s perspective. *Pervasive and Mobile Computing*, 53, 13–32. <https://doi.org/10.1016/j.pmcj.2018.12.006>