https://doi.org/10.57216/pah.v20i2.769

PENINGKATAN PROGRESIF ANCAMAN PEMALSUAN DATA SEBAGAI BENTUK KEJAHATAN SIBER

Neta Nabila Tricintiya[1], Yani Achdiani[2]
[1,2] Universitas Pendidikan Indonesia
e-mail: netanabila03gmail.com

Abstract: The rise of cybercrime in the digital age, such as data forgery, has become an alarming form of crime. This research aims to investigate the progressive growth of the threat of data forgery and its implications for various areas of life. Using a literature review approach, it explores various aspects of data falsification as a cybercrime threat, including the techniques used by cybercriminals, the social, economic, and political impacts of data falsification, and the efforts made to counteract cybercrime. The impact of data falsification is serious, including financial loss, public skepticism, and even potential damage to systems in society. It is hoped that with a better understanding of this phenomenon, effective measures can be taken to maintain data security and integrity in the digital age.

Keywords: *Cybercrime; Digital Technology; Data Forgery*

Abstrak: Kejahatan siber yang meningkat di era digital seperti pemalsuan data, menjadi salah satu bentuk kejahatan yang mengkhawatirkan. Penelitian ini bertujuan untuk menginvestigasi pertumbuhan yang progresif dari ancaman pemalsuan data dan implikasinya terhadap berbagai bidang kehidupan. Dengan menggunakan pendekatan studi literatur ini dapat mengeksplorasi berbagai aspek terkait pemalsuan data dalam ancaman kejahatan siber, termasuk teknik-teknik yang dipakai oleh pelaku kejahatan siber, dampak sosial, ekonomi, dan politik dari pemalsuan data, serta usaha-usaha yang dilakukan untuk menangkal kejahatan siber. Dampak dari pemalsuan data ini sangat serius, termasuk kerugian finansial, keraguan masyarakat, dan bahkan potensi kerusakan pada sistem-sistem dalam masyarakat. Diharapkan dengan pemahaman yang lebih mengenai fenomena ini, langkah-langkah efektif dapat diambil untuk menjaga keamanan dan integritas data di era digital

Kata kunci: *Kejahatan Siber; Teknologi Digital; Pemalsuan Data*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi memiliki sejarah yang panjang. Seiring dengan berjalannya waktu dan semakin berkembangnya di era zaman saat ini, teknologi informasi terus mengalami kemajuan. Saat ini, kecanggihan teknologi informasi dan komunikasi adalah hasil dari evolusi yang akan terus berlanjut seiring berjalannya waktu.

Internet merupakan suatu sistem komputer yang memungkinkan individu maupun organisasi untuk mengakses, menyimpan, dan mengelola data. Di era globalisasi ini, internet telah menjadi bagian penting dalam kehidupan sehari-hari terutama dapat memfasilitasi penyebaran informasi secara luas. Dengan terus berkembangnya teknologi dan komunikasi antar manusia semakin maju, dan proses pengolahan data menjadi lebih cepat dan efisien sehingga dapat memudahkan pendistribusian data.

Perkembangan Teknologi Informasi yang terus berkembang pesat tentu memiliki dampak yang meluas baik pada budaya, sosial, dan politik suatu bangsa. Selain memberikan manfaat yang signifikan, teknologi juga membawa konsekuensi negative, salah satunya adalah penyalahgunaan teknologi oleh individu atau instansi yang tidak bertanggung jawab, dengan tujuan untuk mendapatkan keuntungan dengan cara yang merugikan banyak orang dan bahkan melanggar hukum yang berlaku.

Ketidak amanan dalam infrastruktur Teknologi Informasi dan Komunikasi sehingga memungkinkan terjadinya pemalsuan data menjadi isu yang semakin signifikan dan berkembang pesat. Seiring dengan kemajuan teknologi, hal ini membuka potensi celah keamanan dalam perangkat lunak dan mengurangi praktik keamanan data.

Saat ini, banyak kasus pencurian dan pemalsuan data yang termasuk dalam kategori kejahatan siber. Ancaman kejahatan siber *Cybercrime* dapat timbul dari kepentingan berbagai individu atau kelompok tertentu. Ancaman ini dapat menyebabkan berbagai resiko, baik fisik maupun non-fisik, dalam kehidupan masyarakat. Kejahatan ini dilakukan dengan menggunakan kode-kode computer (software) untuk mencuri informasi dan data, yang pada akhirnya dapat mengancam kedaan data pribadi.

METODE

Penulis menggunakan metode penelitian berupa Studi Literatur. Secara umum, Studi Literatur adalah sebuah metode untuk menyelesaikan masalah dengan menelusuri berbagai sumber tulisan yang telah ada sebelumnya. Metode ini juga sering dikenal sebagai Studi Pustaka. Penulisan dengan metode studi literatur ini bertujuan untuk mencari referensi teori yang relevan dengan kasus atau masalah yang sedang diteliti. Dalam sebuah penelitian, khususnya penelitian akademik, Studi Kepustakaan adalah kegiatan yang sangat penting dan wajib dilakukan. Tujuannya ialah untuk mengembangkan aspek teoritis dan manfaat praktis. Melalui studi kepustakaan, penulis mendapatkan landasan teori, kerangka berfikir dan dapat menentukan hipotesis penelitian. Dengan demikian, peneliti dapat mengelompokkan berbagai sumber Pustaka yang terkait dengan topik yang di bahas. Bagian metode berisi tentang rancangan penelitian, subjek penelitian, instrumen, prosedur pengumpulan data, dan analisis data yang dipaparkan dalam bentuk paragraf.

HASIL

Menurut Adami Chazawi, kejahatan pemalsuan, atau yang disingkat sebagai kejahatan pemalsuan, adalah tindakan kriminal yang melibatkan unsur ketidakbenaran atau kebohongan terhadap suatu objek yang seharusnya terlihat benar dari luar, meskipun sebenarnya bertentangan dengan kenyataan yang sebenarnya.

Harruma (2022) mengemukakan, Kejahatan Siber adalah tindakan kriminalitas yang memanfaatkan elektronik dan koneksi internet sebagai sarana untuk melakukan kejahatan digital. Kejahatan ini memiliki karakteristik global, yang mampu menimbulkan kekacauan yang tidak kasat mata, tidak mengenal batas usia pelaku, bersifat universal, menggunakan teknologi yang kompleks dan sulit dipahami oleh orang awam. Serta dapat menyebabkan kerugian bagi orang-orang sekitar baik secara material maupun non-material.

Maka dapat diartikan bahwa Kejahatan Siber merupakan tindakan kriminal yang menggunakan sistem teknologi baik penggunaan perangkat elektronik ataupun menggunakan koneksi internet untuk tindak pidana yang melanggar hukum. Kejahatan siber dapat berupa penipuan online, pinjol, pemalsuan identitas yang mengatas nama kan orang lain yang memiliki dampak serius terhadap keamanan dan privasi suatu individu.

Berdasarkan studi literatur yang dilakukan, penulis menemukan beberapa kajian teori yang relevan dengan Peningkatan Progresif Ancaman Pemalsuan Data Sebagai Bentuk Kejahatan Siber. Hasil Studi Literatur yang ditemukan yaitu Peningkatan terkait ancaman pemalsuan data sebagai bentuk kejahatan siber di era Teknologi yang semakin canggih ini dan terus mengalami peningkatan yang tentu sangat mengancam sebuah data atau dokumen privasi setiap individunya. Hal tersebut akan dibahas pada pembahasan.

PEMBAHASAN

Pemahaman Mengenai Kejahatan Siber *(Cyber Crime)*

Chintia et al., nd, mengemukakan Kejahatan digital atau *cybercrime* adalah jenis kejahatan baru yang muncul seiring perkembangan Teknologi dan Informasi yang semakin pesat ini. *Cybercrime* dapat diartikan sebagai kejahatan yang melibatkan pemahaman IPTEK dan penggunaan sistem digital seperti komputer dalam pelaksaannnya. Kejahatan ini berhubungan dengan privasi identitas, integritas dan keberadaan data dalam sistem komputer. Pemahaman sistem komputer sangat memerlukan perhatian khusus karena karakteristik komputer sendiri yang berada dari kejahatan konvensional. Penggunaan alat yang diperlukan dalam tindak kejahatan siber ini tidak hanya penggunaan komputer saja, melainkan mencakup penggunaan teknologi lainnya. Semakin pesatnya perkembangan teknologi di Indonesia saat ini , maka semakin besar potensi terjadinya Kejahatan Siber melalui sistem teknologi informasi.

Konsep Pemalsuan Data dalam Konteks Kejahatan Siber

Konsep pemalsuan data dalam konteks kejahatan siber merupakan permasalahan serius yang perlu diperhatikan dalam usaha menjaga keamanan serta privasi data di era digital. Pemalsuan data merupakan tindakan kejahatan siber yang melibatkan penyalahgunaan informasi pribadi yang spesifik. Kemajuan yang cepat dalam teknologi informasi dan komunikasi membuka celah keamanan dalam perangkat lunak dan mengurangi praktik keamanan data. Fenomena peningkatan secara progresif dari ancaman ini menjadi fokus utama dalam upaya menjaga keamanan serta privasi data di era digital.

Pemalsuan data atau Manipulasi data adalah tindakan yang melibatkan perubahan informasi yang tidak akurat atau tidak sesuai dengan realitas. Bentuk-bentuk pemalsuan data sangat beragam, termasuk modifikasi foto, pembuatan dokumen palsu, dan manipulasi perangkat lunak. Salah satu contoh penggunaan rekayasa perangkat lunak adalah dalam memanipulasi informasi dalam sistem teknologi informasi. Sebagai contoh, rekayasa perangkat lunak bisa digunakan untuk mengubah data demografis seperti nama, alamat, atau tanggal lahir dalam database kependudukan.

Risiko yang terjadi dalam menghadapi ancaman kejahatan siber *(cyber crime)* berasal dari dalam maupun luar, dengan memanfaatkan kondisi sosial, politik, budaya, ideologi, dan perkembangan teknologi. Maka, pentingnya peran sistem informasi dan teknologi informasi dalam memperkuat keamanan informasi juga tentu masi berperan penting, namun harus adanya kebijakan mengolah data dan informasi yang tepat.

Peningkatan ancaman pemalsuan data dalam kejahatan siber disebabkan oleh beberapa faktor, termasuk perkembangan teknologi yang memungkinkan manipulasi data menjadi lebih mudah, kurangnya kesadaran keamanan *cyber* di kalangan pengguna internet, dan motif ekonomi atau politik dari para pelaku kejahatan siber yang sangat rendah.

Dampak yang diakibatkan oleh Pemalsuan Data sebagai bentuk Ancaman Kejahatan Siber

Ancaman yang diakibatkan oleh pemalsuan data mendiskusikan konsekuensi dan risiko yang ditimbulkan oleh pemalsuan data. Termasuk dampaknya terhadap privasi individu, kerugian finansial bagi organisasi atau individu, serta potensi kerugian reputasi dan kehilangan kepercayaan publik. Pola atau bentuk kejahatan dunia maya sesungguhnya merupakan tindak kejahat yang dirancang di dunia nyata dan kemudian ditransfer ke dunia maya. Begitupun dengan hasil kejahatannya direalisasikan di dunia nyata. Maka dari itu dapat dikatakan bahwa dunia maya hanya merupakan sarana atau media bagi para pelaku kejahatan untuk melangsungkan segala tindakan kejahatannya.

Pemalsuan data dapat menyebabkan berbagai risiko dan konsekuensi yang sangat besar termasuk dampak yang terjadi sangat merugikan baik terhadap privasi suatu individu, seperti hal nya pemalsuan data kependudukan yang dapat meyebabkan suatu individu menerima hukuman yang tidak sesuai dengan fakta yang ada, kemudian kerugian finansial individu ataupun suatu organisasi misalnya, pemalsuan data keuangan dapat menyebabkan suatu organisasi mengeluarkan dana tidak terduga karena telah adanya transaksi yang tidak sesuai dengan fakta yang ada. Serta potensi kerugian reputasi yang sangat tinggi dan hilangnya kepercayaan di muka publik atau dari sebuah instansi seperti pemalsuan data identitas karyawan suatu perusahaan sehingga menyebabkan kekeliruan publik karena adanya data yang tidak sesuai di muka publik.

Pemalsuan data termasuk sebagai tindak pidana yang dapat dijerat dengan hukuman yang sesuai dengan yang tercantum dalam Peraturan Perndang-undangan. Hukuman pidana yang dikenakan terhadap pelaku pemalsuan data bahkan tidak main-main. Seperti pada ancaman pidana terhadap pelaku Pemalsuan Identitas yang diatur dalam Undang-undang Hukum Pidana (KUHP) dalam Pasal 378 dan UU Perlindungan Data Pribadi (UU PDP) Nomor 27 Tahun 2022 Pasal 66 dan 68. Ancaman pidana bagi pelaku yang memalsukan data pribadi dengan sengaja maka dikenakan pidana penjara selama 6 tahun atau dikenakan denda paling banyak Rp. 6 Miliar.

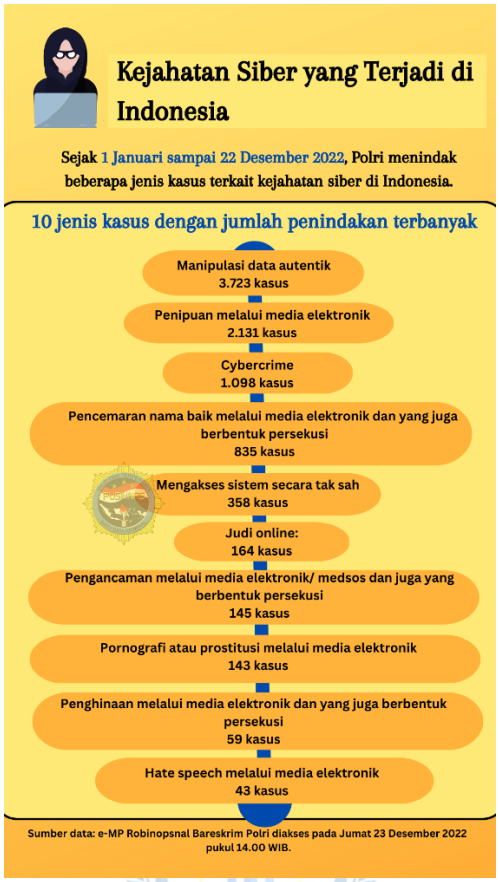
Perkembangan Teknologi Menjadi salah satu penyebab terjadinya Ancaman Kejahatan Siber

Tidak menutup kemungkinan seiring perkembangan zaman saat ini banyak kalangan remaja hingga orang dewasa yang mahir dalam mengoperasikan pengetahuan teknologi dengan berbagai kemampuan ataupun bahan pengetahuan yang mereka miliki untuk senantiasa mendalami IPTEK, karena bagaimana pun teknologi semakin canggih dengan segala fasilitas yang didapatkan dalam mengoprasikan dan mengeskplore teknologi. Namun, nyatanya jika tidak ada kebijakan dalam pemanfaat teknologi tersebut tentu akan mendatangkan mala petakan bagi setiap penggunaya. Karena pada dasarnya perkembangan teknologi merupakan faktor utama penyebab terjadinya ancaman kejahatan siber.

Berkembangnya teknologi dan informasi yang semakin canggih dengan banyak munculnya Teknologi kecerdasan buatan seperti AI (Artificial Intelligence) yang mana AI sendiri sudah banyak bermunculan saat ini bahkan AI sendiri sudah hampir menggantikan fungsi kerja manusia karena kecanggihannya yang luar biasa, oleh karena itu AI saat ini juga digunakan untuk media pemalsuan suatu data yang sulit untuk dideteksi, dan adanya teknologi *blockchain* yang telah memengaruhi kedalaman dan kerumitan pemalsuan data.

Perkembangan teknologi juga membuat penjahat lebih mudah untuk melakukan kejahatan, seperti dengan menggunakan teknologi internet yang mudah digunakan tanpa peralatan khusus. Hal ini membuat penanganan dan pencegahan kejahatan siber menjadi lebih rumit dan memerlukan keahlian khusus dalam bidang teknologi.

Presentase Kasus Ancaman Kejahatan Siber di Indonesia



Gambar 1. Infografis Presentase Peningkatan Kasus Kejahatan Siber yang Terjadi di Indonesia (Dikutip dari pusiknas.polri.go.id)

Kejahatan siber di Indonesia terus meningkat setiap tahunnya hinggal 14 kali. Ditemukan data menurut e-MP Robinopsnal Bareskim Polri menunjukan bahwa kepolisian telah menindak 8.832 kasus kejahatan siber. Sejak 1 Januari hingga 22 Desember 2022. Semua satuan kerja di Bareskrim Polri dan Polda di Indonesia terlibat dalam penanganan kasus ini. Polda Metro Jaya menangani kasus terbanyak yaitu 3.709 kasus. Pada periode yang sama di tahun 2021, penanganan kasus hanya mencapai 612 di seluruh Indonesia.

Strategi Pencegahan dari Ancaman Pemalsuan Data

Fenomena dan kasus-kasus yang berkaitan dengan dunia digital memang sangat mengancam atmosfir pengetahuan teknologi. Namun, teknologi sangat berperan penting demi kemajuan dunia global, maka dari itu sumber daya manusia lah yang harus lebih dikenalkan dengan dunia digital. Untuk mengatasi ataupun pencegahan dari semakin meningkatnya kasus siber di kalangan masyarakat, tentu harus adanya strategi dan kesadaran tiap masyarakatnya terhadap ancaman kejahatan siber.

Semakin berkembangnya dunia digital memang sangat memudahkan kita untuk mengakses segalanya di internet, dengan begitu sudah seharusnya kita dapat memanfaatkan teknologi untuk hal positif juga. Banyak strategi yang dapat dilakukan sebagai bentuk pencegahan ancaman kejahatan siber, yaitu salah satunya di mulai dari lingkungan terkedekat seperti dengan cara penggunaan keamanan digital yang kuat seperti sistem keamanan perangkat lunak,

memperbarui perangkat lunak secara teratur untuk melindungi data dari pemalsuan, mengaktifkan autentikasi untuk kode OTP sebagai perlindungan akun dari pemalsuan hingga penggunaan teknologi verivikasi dan validasi sebagai bentuk kemanan data pribadi dari ancaman kejahatan siber.

SIMPULAN DAN SARAN

Simpulan

Kemajuan dalam bidang teknologi informasi telah membuka peluang bagi ancaman yang semakin meningkat terhadap integritas dan keamanan data. Pemalsuan data menjadi salah satu bentuk kejahatan siber yang semakin mengkhawatirkan, di mana pelaku dapat memanipulasi informasi untuk kepentingan individu atau kelompok, dengan potensi dampak yang sangat merugikan. Ancaman pemalsuan data tidak hanya mencakup manipulasi data atau pembuatan dokumen palsu, tetapi juga melibatkan rekayasa perangkat lunak yang dapat menimbulkan kerugian besar bagi individu, organisasi, atau bahkan masyarakat secara luas.

Ketika kompleksitas ancaman pemalsuan data semakin meningkat, diperlukan respons yang lebih proaktif dari berbagai pihak, termasuk individu, dan lembaga pemerintah. Kolaborasi yang kuat diperlukan dalam mengembangkan strategi perlindungan data yang efektif, menerapkan regulasi serta meningkatkan kesadaran dan pelatihan terkait keamanan siber. Hanya melalui kerja sama dan kewaspadaan yang tinggi, kita dapat mengurangi risiko dan mengatasi dampak negatif dari ancaman pemalsuan data dalam konteks kejahatan siber.

Pemalsuan adalah proses atau cara membuat sesuatu yang tidak asli. Pemalsuan ini menunjukan bahwa suatu barang tidak asli, pemalsuan dan merupakan proses pembuatan sesuatu barang yang palsu, dengan demikian, dalam pemalsuan terdapat pelaku, barang yang dipalsukan dan tujuan pemalsuan. Menurut Adami Chazawi, kejahatan pemalsuan adalah tindakan kriminal yang melibatkan unsur ketidakbenaran atau kebohongan terhadap suatu objek yang tampak benar dari luar, meskipun sebenarnya bertentangan dengan kenyataan sebenarnya.

Saran

Seiring dengan terus meningkatnya ancaman-ancaman kejahatan di bidang teknologi dan digital sehingga mengharuskan kita untuk lebih memperkuat sistem keamanan, baik dari pribadi ataupun data dari suatu Lembaga/instansi. Meningkatan regulasi hukum supaya mendorong pemerintah agar lebih peduli terkait keamanan data dan memberlakukan hukuman yang tepat bagi pelaku kejahatan siber, dan sudah seharusnya setiap organisasi atau Lembaga melakukan transparasi dalam pengolahan data memberikan mekanisme verifikasi yang kuat (Placeholder1)untuk memperjelas integritas sebuah data.

DAFTAR RUJUKAN

Ariyaningsih, S., Andrianto, A. A., Kusuma, A. S., & Prastyanti, R. A. (2023). Korelasi Kejahatan Siber dengan Percepatan Digitalisasi di Indonesia. Justisia: *Jurnal Ilmu Hukum*, 1(1), 1-11. Diakses dari Google Scholar Korelasi Kejahatan Siber dengan Percepatan Digitalisasi di Indonesia | Justisia: Jurnal Ilmu Hukum (pascasarjana-unpas.web.id)

Chintia, E., Nadiah, R., Ramadhani, H. N., Haedar, Z. F., Febriansyah, A., & Kom, N. A. R. S. (2019). Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya. *Journal Information Engineering and Educational Technology) ISSN*,

2549, 869X. Diakses dari google Scholar https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Kasus+Kejahatan+Siber+yang+Paling+Banyak+Terjadi+di+Indonesia+dan+Penanganannya.+Journal+Information+Engineering+and+Educational+Technology%29+ISSN&btnG=

Djanggih, H., & Qamar, N. (2018). Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime). *Pandecta Research Law Journa*l, 13(1), 10-23.Diakses dari Google Scholar Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime) | Djanggih | Pandecta Research Law Journal (unnes.ac.id)

DM, M. Y., Agustantia, M., & Zulaiha, S. (2022). Tindak Pidana Kejahatan Pemalsuan data (Data Forgery) dalam Bentuk Kejahatan Siber (Cyber Crime). *Jurnal Pendidikan Dan Konseling (JPDK)*, 4(6), 6635-6640. Diakses dari Goggle Scolar Tindak Pidana Kejahatan Pemalsuan data (Data Forgery) dalam Bentuk Kejahatan Siber (Cyber Crime) | Jurnal Pendidikan dan Konseling (JPDK) (universitaspahlawan.ac.id)

Jayana, M. A., Rafael, D., & Rahman, A. A. (2022, November). Implementasi Pengamanan Data Pengarsipan Dengan Metode Algoritma Kriptografi AES Studi Kasus pada Bank 8 BJB KCP Pasteur Bandung. In *Prosiding Seminar Sosial Politik, Bisnis, Akuntansi dan Teknik* (Vol. 4, pp. 184-195). Diakses dari Google Scholar https://ejournal.unsrat.ac.id/index.php/informatika/article/view/12231

Kejahatan Siber di Indonesia Naik Berkali-kali Lipat | *Pusiknas Bareskrim Polri*. (n.d.) Kejahatan Siber di Indonesia Naik Berkali-kali Lipat | Pusiknas Bareskrim Polri

Kenfaizah, S. A. (2020). Perbarengan Perbuatan Pemalsuan Data Kependudukan untuk Pengurusan Data Kependudukan Indonesia ditinjau dari Undang-Undang Nomor 24 Tahun 2013. Diakses dari Google Scholar https://repository.ubaya.ac.id/39457/

Maulindar, J., & Hartanti, D. (2023). Pelatihan Perlindungan Data Pribadi dan Keamanan Siber Untuk Siswa SMK Negeri 2 Surakarta. *Madaniya*, 4(4), 1851-1856. Diakses dari Google Scholar https://www.madaniya.pustaka.my.id/journals/contents/article/view/652

Merliana, N. P. E. (2020). Pemanfaatan Teknologi Kriptografi dalam mengatasi kejahatan Cyber. Satya Dharma: *Jurnal Ilmu Hukum*, 3(2), 23-40. https://ejournal.iahntp.ac.id/index.php/satya-dharma/article/view/678

Mulia, A. J., Firmansyah, A., Purba, C. D. A., Mozi, M. F. A., Pramata, A. B., Ilmawan, M. A., ... & Sholihatin, E. (2023). PENCEGAHAN KEJAHATAN SIBER PADA MEDIA SOSIAL MELALUI IDENTIFIKASI BAHASA PARA PELAKU. *Jurnal Membaca Bahasa dan Sastra Indonesia*, 8(2). Diakses dari Google Scholar https://jurnal.untirta.ac.id/index.php/jurnalmembaca/article/view/23412

Nasrullah, R. (2022). Teori dan riset media siber (cybermedia). *Prenada Media*. Diakses dari Google Scholar Teori dan Riset Media Siber (Cybermedia) - Dr. Rulli Nasrullah - Google Buku

Novita, M. S. (2023). IMPLEMENTASI PEMBERIAN SANKSI TERHADAP TINDAK PIDANA PEMALSUAN DATA DITINJAU MENURUT UNDANG-UNDANG NO. 11 TAHUN 2008 TENTANG INFORMASI TRANSAKSI ELEKTRONIK. *Jurnal Ilmiah Hukum D an Keadilan*, 10(1), 123-134.Diakses dari Google Scolar IMPLEMENTASI PEMBERIAN SANKSI TERHADAP TINDAK PIDANA PEMALSUAN DATA DITINJAU MENURUT UNDANG-UNDANG NO. 11 TAHUN 2008 TENTANG INFORMASI TRANSAKSI ELEKTRONIK | Jurnal Ilmiah Hukum dan Keadilan (stihpainan.ac.id)

Popal, D. F. (2023). UPAYA PENANGGULANGAN TINDAK PIDANA MAYANTARA (CYBER CRIME). *Lex Administratum*, 11(5). Diakses dari Google Scholar https://ejournal.unsrat.ac.id/index.php/administratum/article/view/51005

Prabowo, W., Wibawa, S., & Azmi, F. (2020). Perlindungan Data Personal Siber di Indonesia. *Padjadjaran Journal of International Relations*, 1(3), 218-239. Diakses dari google Scholar https://jurnal.unpad.ac.id/padjir/article/view/22138

Putra, A. S. (2019). Penting Nya Kesadaran Hukum Rakyat Indonesia Di Bidang Teknologi Informasi Di Tinjau Dari Keberadaan Cybercrime. *SNIT* 2012, 1(1), 10-14. Diakses dari google Scholar https://seminar.bsi.ac.id/snit/index.php/snit-2012/article/view/327

Rasso, V. S. N. (2021). Upaya Kriminalisasi dalam Hal Penanggulangan Kejahatan Cyber Crime. *Lex Administratum*, 9(4). Diakses dari google sholar UPAYA KRIMINALISASI DALAM HAL PENANGGULANGAN KEJAHATAN CYBER CRIME | LEX ADMINISTRATUM (unsrat.ac.id)

Sari, A. K., & Hwihanus, H. (2023). Peranan Sistem Informasi Akuntansi Dan Implementasi Menghadapi Pemalsuan Data Di Era Digital Pada Masyarakat Desa. *Jurnal Manajemen Riset Inovasi*, 1(1), 186-196. Diakses dari google Scholar https://prin.or.id/index.php/mri/article/view/648

Sila, G. E., & Taufik, C. M. (2023). Literasi digital untuk melindungi masyarakat dari kejahatan siber. *KOMVERSAL*, 5(1), 112-123. Diakses dari Googler Scolar https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=+Literasi+digital+untuk+melindungi+masyarakat+dari+kejahatan+siber.&btnG=

Sinurat, Y. C., Putranti, I. R., & Hanura, M. (2022). The Deception of Art: Analisis Potensi Ancaman NFTs (Non-Fungible Tokens) Terhadap Keamanan Nasional Indonesia. *Journal of International Relations Universitas Diponegoro*, 8(3), 280-288. Diakses dari Google Scholar https://ejournal3.undip.ac.id/index.php/jihi/article/view/34340

Soesanto, E., Saputra, F., Puspitasari, D., & Danaya, B. P. (2023). Determinasi Sistem Manajemen Sekuriti: Analisis Objek Vital, Pengamanan File dan Pengamanan Cyber pada Yayasan Siber Publisher. *Jurnal Ilmu Multidisplin*, 2(1), 23-29. Diakses dari Google Scholar https://greenpub.org/JIM/article/view/221

Suryaningsih, F. S., & Hayati, A. (2023). Peran dan Kedudukan KUA dalam Pengajuan Pembatalan Perkawinan Akibat Pemalsuan Identitas (Putusan 2856/Pdt. G/2022/PA. Mdn). Al-Manhaj: *Jurnal Hukum Dan Pranata Sosial Islam*, 5(1), 373-384.Diakses dari Google Scholar https://ejournal.insuriponorogo.ac.id/index.php/almanhaj/article/view/2490

Tamhidah, M. A. R. (2023). Pengaruh Media Sosial Terhadap Penyebaran Informasi Palsu dan Kejahatan Siber. Innovative: *Journal Of Social Science Research*, 3(6), 9133-9147. Diakses dari google Scholar Pengaruh Media Sosial Terhadap Penyebaran Informasi Palsu dan Kejahatan Siber | Innovative: Journal Of Social Science Research (j-innovative.org)

Taraja, P. M. (2020). PERTANGGUNGJAWABAN PIDANA TERHADAP PEMALSUAN DATA UNTUK MEMPEROLEH DOKUMEN PERJALANAN TANPA MEMENUHI UNDANG-UNDANG NOMOR 6 TAHUN 2011 TENTANG KEIMIGRASIAN (Studi-Putusan No. 35/Pid. Sus/2019/PN. BGR). Diakses dari Google Scholar https://repository.uhn.ac.id/handle/123456789/4044

Tobing, M. S., Wulandari, U., Sihotang, M. S., & Raihana, R. (2023). Tinjauan Terhadap Modus-Modus Kejahatan Dalam Hukum Cyber Crime. *Jurnal Hukum Dan Sosial Politik,*

1(2), 60-67. Diakses dari Google Scholar https://journal.widyakarya.ac.id/index.php/jhsp-widyakarya/article/view/239

Vimy, T., Wiranto, S., Rudiyanto, R., Widodo, P., & Suwarno, P. (2022). Ancaman Serangan Siber Pada Keamanan Nasional Indonesia. *Jurnal Kewarganegaraan*, 6(1), 2319-2327. Diakses dari Google Scholar article.php (kemdikbud.go.id)