Jurnal Ilmu Komputer dan Sistem Informasi
JIKSI, Vol. 02, No. 01, Februari 2021: 30-36
Received: 5 Januari 2021; Revised: 29 Januari 2021; Accepted: 27 Februari 2021

Cookie dan Spyware: Stui Literatur Permasalahan Etika Pada Teknologi Informasi

Muhammad Zaki
Program Magister Teknik Informatika
Universitas Bina Darma
email : muhammadzakisafira050198@gmail.com
Jl. A. Yani No. 12, Palembang 30624, Indonesia

Abstract

The rapidly evolving digital era, information technology has become the backbone of modern life, providing unlimited access to information and services. However, alongside its benefits, significant ethical issues have also emerged, particularly concerning the use of cookies and spyware. Cookies, intended to enhance user experience, often raise questions about privacy and data control. Meanwhile, spyware, which secretly collects information without user consent, poses serious threats to privacy and security. This article aims to explore the ethical issues related to cookies and spyware within the context of information technology through an analysis of relevant literature studies. By examining aspects such as privacy, transparency, and user control, we identify the main challenges faced as well as the associated legal and regulatory implications. This literature study provides valuable insights for developing ethical frameworks and effective policies to address these issues in the future. Therefore, this article is expected to make a significant contribution to the understanding and resolution of ethical problems in information technology related to cookies and spyware.

Keywords: *Ccookies, spyware, ethics, social media*

Abstrak

Dalam Dalam era digital yang terus berkembang, teknologi informasi telah menjadi tulang punggung kehidupan modern, memberikan akses tak terbatas ke informasi dan layanan. Namun, bersamaan dengan manfaatnya, muncul pula permasalahan etika yang signifikan, terutama terkait dengan penggunaan cookie dan spyware. Cookie, yang bertujuan untuk meningkatkan pengalaman pengguna, sering kali memunculkan pertanyaan tentang privasi dan kontrol data. Di sisi lain, spyware, yang secara diam-diam mengumpulkan informasi tanpa izin pengguna, menimbulkan ancaman serius terhadap privasi dan keamanan. Artikel ini bertujuan untuk mengeksplorasi permasalahan etika yang terkait dengan cookie dan spyware dalam konteks teknologi informasi, dengan menganalisis studi literatur yang relevan. Dengan memperhatikan aspek-aspek seperti privasi, transparansi, dan kontrol pengguna, kami mengidentifikasi tantangan utama yang dihadapi serta implikasi hukum dan regulasi yang berkaitan. Studi literatur ini memberikan wawasan yang berharga dalam mengembangkan kerangka kerja etis dan kebijakan yang efektif dalam menghadapi permasalahan ini di masa depan. Dengan demikian, diharapkan artikel ini dapat memberikan kontribusi yang signifikan dalam pemahaman dan penyelesaian permasalahan etika pada teknologi informasi terkait cookie dan spyware.

Kata kunci: *: cookie, spyware, etika, media Sosial*

1. PENDAHULUAN

Dalam pesatnya perkembangan era digital, keamanan barang dan file menjadi hal yang sangat penting yang merupakan masalah besar dalam hal keamanan cyber. Item penting seperti infrastruktur penting, data sistem sensitif dan sistem kritis lainnya memiliki nilai strategis yang tinggi dan rentan serangan cyber yang dapat menimbulkan kerugian serius. Keamanan file juga penting dalam lingkungan digital karena file-file ini sering kali berisi informasi-informasi penting dan rahasia yang harus dilindungi dari akses tidak sah. Ancaman terhadap keamanan objek danfile penting berkembang pesat. Penjahat dunia maya menjadi lebih pintar dan mahir dalam mengeksploitasi kerentanan dalam sistem digital, termasuk serangan malware, peretasan, dan serangan jaringan canggih. (Sanjaya et al., 2022).

Dalam era digital yang terus berkembang, teknologi informasi telah menjadi tulang punggung dari kehidupan modern, mengubah cara kita berinteraksi, bekerja, dan berkomunikasi. Namun, di balik kemudahan dan kenyamanan yang ditawarkan oleh teknologi informasi, terdapatjuga tantangan yang signifikan terkait dengan permasalahan etika, terutama terkait dengan penggunaan cookie dan spyware.

Cookie, yang merupakan komponen esensial dari pengalaman web modern, memungkinkan situs web untuk menyimpan informasi tentang preferensi pengguna, riwayat penelusuran, dan aktivitas online lainnya. Meskipun bertujuan untuk meningkatkan pengalaman pengguna dengan menyediakan konten yang disesuaikan, penggunaan cookie sering kali menimbulkan pertanyaan tentang privasi dan keamanan data pengguna. Di sisi lain, spyware, yang seringkali beroperasi secara diam-diam dan tanpa izin pengguna, menjadi ancaman serius terhadap privasi dan keamanan. Spyware dapat mengumpulkan informasi sensitif, mengawasi aktivitas online, dan bahkan mengendalikan perangkat pengguna tanpa pengetahuan mereka.

Malware dapat menyusup ke sistem operasi dan membuat sistem komputer menggunakan sumber daya tanpa sepengetahuan pemilik perangkat, bahkan mengumpulkan informasi pribadi untuk dibagikan ke pihak ketiga tanpa persetujuan pengguna (Rusdi & Sulastri, 2019). Beberapa varian klasik malware yang dapat membahayakan pengguna antara lain adware, spyware, ransomware, virus (overwriting virus, prepending virus, appending virus, file infector virus, boot sector virus, multipartie virus, dan macro virus), Worms, dan Trojan Horse (remote access, trojan, password sending trojan, keylogger, estructive trojan, FTP trojan, software detection killer, procy trojan (Manopo & Karouw, 2022).

Dalam konteks ini, permasalahan etika seputar cookie dan spyware menjadi semakin penting untuk dibahas. Pertanyaan mendasar tentang privasi, transparansi, dan kontrol pengguna atas data pribadi mereka menjadi fokus utama. Bagaimana kita dapat memastikan bahwa pengguna diberikan informasi yang cukup dan kontrol penuh atas data mereka, Apakah penggunaan cookie dan spyware dilakukan dengan cara yang etis dan sesuai dengan kepentingan pengguna.

Artikel ini akan mengeksplorasi permasalahan etika yang terkait dengan cookie dan spyware dalam konteks teknologi informasi. Dengan menganalisis studi literatur yang relevan, kami akan menyelidiki dampak, implikasi, dan solusi yang mungkin untuk mengatasi tantangan ini. Dengan pemahaman yang lebih dalam tentang permasalahan ini, diharapkan kita dapat mengembangkan kerangka kerja etis dan kebijakan yang efektif dalam menghadapi permasalahan ini di masa depan.

2. METODOLOGI PENELITAN

Penulisan artikel ini menggunakan metode literature review yaitu melakukan riview artikel atau jurnal ilmiah, tesis, disertasi dan prosiding berdasarkan kriteria, standar, dan terstruktur. Pengumpulan data dilakuka melalui tiga sumber data, yaitu PubMed, ScienceDirect, dan Google Scholar. Artikel yang menjadi bahan referensi dari jurnal nasional maupun internasional, baik ditulis dalam Indonesia maupun Bahasa Inggris. Kata kunci yang digunakan dalam penelusuran artikel yaitu : cookie, spyware, etika, media sosial. Pencarian dibatasi dalam artikel terbaru, sehingga tahun publikasi dibatasi dalam 5 tahun terakhir. Artikel yang digunakan dalam bentuk Original article, full text, dan open access. Pada tahap awal pencarian artikel dari online adalah sebanyak 20 artikel. Dari jumlah tersebut terdapat 15 artikel yang terpilih untuk dijadikan Literature Riview.

3. HASIL DAN PEMBAHASAN

Berdasarkan hasil pencarian, dari keseluruhan penelitian dari beberapa referensi terdapat total studi yang dilakukan di beberapa akun media social terdapat 4 artikel yang dipublikasi pada tahun 2023, 3 artikel dipublikasi pada tahun 2022, 3 artikel di publikasi pada tahun 2021, dan 2 artikel dipublikasi 2018- 2019. Dari 20 artikel 12 artikel menggunakan metode penelitian kualitatif.

Tabel 1: Hasil dan Temuan Jurnal

No	Judul	Penulis	Temuan
1	Kejahatan cyber dalam perkembangan teknologi informasi berbasis komputer. Jurnal Surya Kencana Data Dinamika Masalah Hukum dan Keadilan	(Sari, N. W., 2018)	Kemajuan teknologi informasi berbasis computer telah mengakibatkan munculnya Tindakan kejahatan cyber yang melibatkan penggunaan data atau informasi yang dikirim melalui internet.
2	A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments	(Li, y & Liu, Q., 2021)	Cyberspace dan teknologi terkait merupakan salah satu sumber kekuatan yang paling penting di milenium ketiga. Karakteristik dari dunia maya, seperti biaya masuk yang rendah, anonimitas, kerentanan, dan ketidaksimetrisan, telah menciptakan fenomena penyebaran kekuatan, yang berarti jika pemerintah sejauh ini telah membagi permainan kekuasaan di antara mereka, maka harus ada aktor lain, seperti perusahaan swasta, kelompok teroris terorganisir, dan individu.

3	Advanced feature extraction and selection approach using deep learning and Aquila optimizer for IoT intrusion detection system	(Fatani, A., Dahou,et al, 2022)	Performa tinggi menggunakan algoritma SI yang baru dikembangkan, Aquila optimizer (AQU). Selain itu, untuk menilai kualitas pendekatan IDS yang dikembangkan, empat dataset publik yang terkenal, yaitu CIC2017, NSL-KDD, BoT-IoT, dan KDD99
4	Economic and Mathematical Modelling of the Effectiveness of the National System for Countering Cyber Fraud and Criminal Proceeds Legalisation Based on Survival Analysis Methods	(Kuzmenko, O. V et al, 2021)	Efektifivitas sistem nasional dalam mengatasi kejahatan siber dan legalisasi dana illegal bergantung pada rentang waktu setelah terdeteksinya pelanggaran.
5	The rise of crypto- ransomware in a changing cybercrime landscape:	(Connolly, L. Y., & Wall, D. S., 2019)	Respons terhadap crypto ransomware menjadi lebih kompleks oleh hubungan nuansa antara aspek teknis
	Taxonomising countermeasures		(malware yang mengenkripsi) dan aspek manusia (rekayasa sosial yang masih menjadi penyebab utama infeksi). Akibatnya, tidak ada 'senjata ajaib' teknologi sederhana yang akan menghapus ancaman crypto-ransomware. Sebaliknya, diperlukan pendekatan berlapis yang terdiri dari Langkah-langkah sosio-teknis, manajer garis depan berdedikasi, dan dukungan aktif dari manajemen senior.
6	Strategi Pengamanan Cyber: Lingkup Kerjasama dalam menghadapi Ancaman Cyber	(Putri, C, P et al., 2023)	Penjahat dunia maya semakin cerdik dan terampil dalam memanfaatkan celah keamanan informasi dalam sistem digital. Meningkatkan keamanan cyber membutuhkan analisis menyeluruh terhadap ancaman dalam lingkungan digital dan solusi yang dapat diterapkan. Tujuan penelitian ini adalah menganalisis target utama, mengidentifikasi tantangan utama dalam melindungi mereka dari serangan dunia maya, serta mengevaluasi dan merekomendasikan langkah-langkah dan strategi untuk meningkatkan keamanan file

7	Mobile Spyware Identificatio and Categorization: A Systematic Review	(Soesanto, Edy., et al., 2023)	Pencurian informasi dan data yang bersifat rahasia sebagai ancaman kejahatan siber ditujukan untuk menyerang individu, instansi pemerintah, dan militer yang dapat mengancam pertahanan suatu negara. Oleh karena itu, penting untuk memiliki manajemen risiko yang terkait dengan informasi dan komunikasi guna mengurangi kerentanan terhadap penyalahgunaan informasi dan data di ruang siber (cyberspace), yang dapat berdampak pada banyak warga negara dan informasi yang bersifat rahasia. Selain memiliki pertahanan negara yang kuat, juga dibutuhkan dukungan hukum yang saling terkait dan saling mempengaruhi dalam menghadapi ancaman kejahatan siber.
8	Mobile Spyware Identification and Categorization: A Systematic Review	(Naser, M. et al ., 2023)	Popularitas ponsel pintar yang semakin meningkat menyebabkan banyak tantangan keamanan, dengan spyware menjadi masalah yang paling umum. Peneliti telah berusaha untuk mengatasi masalah ini, dengan beberapa penelitian dilakukan tentang deteksi spyware di ponsel pintar. Makalah ini menyajikan survei tentang teknik-teknik deteksi spyware terbaru, hasil yang dicapai, dan akan menjadi referensi penting bagi peneliti di bidang ini.
9	Strategi Indonesia Membentuk Cyber Security dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber dan Sandi Negara	(Ginanjar, Yosep., 2022)	Keamanan cyber telah menjadi prioritas global karena teknologi informasi dan komunikasi digunakan dalam berbagai aspek kehidupan. Tingkat risiko dan ancaman penyalahgunaan teknologi semakin tinggi seiring dengan penggunaan yang semakin luas. Indonesia membentuk Badan Siber dan Sandi Negara (BSSN) sebagai respons terhadap ini. Penelitian ini menggunakan metode deskriptif untuk memahami strategi Indonesia dalam menghadapi ancaman kejahatan cyber melalui BSSN
10	Aktivitas Sniffing pada Malware Pencuri Uang di Smsrphone Android	(Zulfa, et al, 2023)	Kejahatan online sering dilakukan oleh malware seperti virus atau trojan, yang bertujuan merusak file atau sistem komputer dan

			smartphone. Namun, ada juga kejahatan yang bertujuan mencuri informasi berharga seperti akun email atau internet banking melalui metode seperti sniffing, yang umumnya menggunakan spyware. Untuk mencegah kedua jenis kejahatan ini, langkah-langkah seperti menginstal antivirus dengan fitur antitrojan dan antispyware untuk komputer, dan memastikan aplikasi smartphone didownload dari sumber resmi seperti Google Play Store, serta berhati-hati terhadap file dari pengirim yang tidak dikenal serta permintaan akses aplikasi, dapat dilakukan.
11	Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0	(Budi, et al, 2021)	Hasil dari penelitian ini adalah pandemi Covid - 19 menjadi topik utama dalam tren keamanan siber. Para peretas memanfaatka keresahan masyarakat sebagai celah dalam meluncurkan berbagai serangan, mulai dari phishing hingga ransomware, kasus kebocoran data 91 juta pengguna situs belanja online Tokopedia dan kebocoran data 1,2 juta pengguna situs Bhinneka. Indonesia pun terdampak oleh kasus keamanan siber global seperti Coronavirus Ransomware, Covidlock Malware, peretasan Border Gateway Protocol, kerentanan pada produk router Draytek Vigor, adanya Remote Code Execution pada beberapa versi produk sistem operasi Windows, kerentanan terjadinya Arbitrary Code Execution pada seluruh sistem operasi Google Android, hingga eksploitasi produk Solar Winds Orion Platform.

4. KESIMPULAN

Berdasarkan pada penelitian yang telah dilakukan menggunakan metode literature review terhadap artikel yang telah diperoleh sebelumnya, mengenai Cookie dan spyware, didapatkan hasil bahwa dampaknya terhadap privasi individu dan perluasan regulasi untuk mengatasi kekhawatiran tersebut. Penggunaan teknologi ini menimbulkan isu privasi, kepercayaan, kontrol pengguna, serta menekankan perlunya pertimbangan etika dalam pengembangan dan implementasi. Kesimpulannya, penting untuk meningkatkan kesadaran akan privasi, memperkuat transparansi, memberikan kontrol kepada pengguna, serta menegakkan regulasi yang sesuai dengan prinsip etika.

Referensi

S. Rusdi, N. Widiyasono, and H. Sulastri, (2019). Analisis Infeksi Malware Pada Perangkat Android Dengan Metode Hybrid Analysis, J. Ilm. Inform., vol. 7, no. 2, pp. 99–107, 2019.

Budi, Eko, et al (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0 (Strategies For Strengthening Cyber Security To Achieve National Security in Society 5.0). Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia -Akademi Angkatan Udara, Volume 3, 223–234

Connolly, L. Y., & Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures.Computers & Security,87, 101568.

Fatani, A., Dahou, A., Al-Qaness, M. A., Lu, S., & Abd Elaziz, M. (2022). Advanced feature extraction and selection approach using deep learning and Aquila optimizer for IoT intrusion detection system.Sensors,22(1), 140.

Ginajar, Yosep (2022). Strategi Indonesia Membentuk Cyber Security dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber dan Sandi Negara. Jurnal Dinamika Global Vol. 7 No. 2, Desember 2022.

Hapsah, Z F & M Irwan, P N. (2023). Analisis Tingkat Keamanan Data Perusahaan yang Rentan Terhadap Serangan Cyber dalam Sisitem Informasi Manajemen. Jurnal Manajemen dan Akuntansi Vol. 1 No. 2 Januari 2023, 338-343

Kuzmenko, O. V., Dotsenko, T. V., & Skrynka, L. O. (2021). Economic and Mathematical Modelling of the Effectiveness of the National System for Countering Cyber Fraud and Criminal Proceeds Legalisation Based on Survival Analysis Methods. Scientific Bulletin of Mukachevo State University. Series "Economics, 8(1), 144-153.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments.Energy Reports,7, 8176-8186.

Naser. Muawya, et al, (2023). Mobile Spyware Identification and Categorization: A Systematic Review. Jurnal Informatica An International Journal of Computing and Informatics Vol. 47 N0. 8 2023.

Putri, Chintya P, et al. (2023). Strategi Pengama n Cyber: Lingkup Kerjasama dalam Menghadapi Ancaman Cyber. Insologi Jurnal Sains dan Teknologi Vol. 2 No. 6 Desember 2023.

Sari, N. W. (2018). Kejahatan cyber dalam perkembangan teknologi informasi berbasis komputer.Jurnal Surya Kencana Data Dinamika Masalah Hukum dan Keadilan. 5(2): 577-592.

Sanjaya, B, R, et al (2022). (2022). Pengembanga Cyber Security dalam menghadapi cyber warfare di. Journal of Advanced Research in Defense and Security Studies, Vol. 1, No. 1, 19–34.

Soesanto, Edy., et al (2023). Analisi dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital untuk mengamankan Objek Vital dan file. Jurnal Penelitian Bisnis dan Manajemen Vol. 1 No. 2 Juni 2023.

Manoppo, A. S. . Lumenta, and S.D. . Karouw, (2020) Analisa Malware Menggunakan Metode Dynamic Analysis Pada Jaringan Universitas Sam Ratulangi," J. Tek. Elektro Dan Komput., vol. 9, no. 3, pp. 181–188, 2020.

Zulfa, M, I, et al. (2023). Aktivitas Sniffing pada Malware Pencuri Uang di Smarphone Android.RENATA Jurnal Pengabdian Masyarakat Kita Semua Vol. 1 April 2023