KAMPUS AKADEMIK PUBLISING
Jurnal Ilmiah Penelitian Mahasiswa (JIPM)
Vol.4, No.5 Oktober 2026
e-ISSN: 3025-5465, p-ISSN : 3025-7964, Hal 211-218
DOI : https://doi.org/10.61722/jipm.v4i5.2871

BENTENG IMUNITAS DI ERA SIBER: REKONSEPTUALISASI INVIOLABILITAS KANTONG DIPLOMATIK DIGITAL DAN GEDUNG PERWAKILAN BERDASARKAN KONVENSI WINA 1961

Ilham Gunawan[1] Mayzara Sari Fitria[2]

[1,2] Fakultas Hukum, Universitas Pakuan
*Penulis Korespondensi: [1]ilhamgunawan1010@gmail.com [2]mayzara.sari@unpak.ac.id

Abstract. *The evolution of information technology poses an existential challenge to classical diplomatic law doctrines, particularly regarding the principle of inviolability of diplomatic missions and confidential communications. The 1961 Vienna Convention on Diplomatic Relations was drafted in a physical-analog era, thus failing to explicitly address cyber espionage and the transmission of classified documents via digital networks (digital diplomatic bag). This normative legal research analyzes the dynamic interpretation of mission premises inviolability (Article 22) and official correspondence (Article 27) in the face of cyber intrusion threats by receiving States or non-state actors. Findings indicate a juridical ambiguity regarding whether passive cyber operations constitute a breach of physical mission borders, and how State responsibility applies to diplomatic data breaches. A reconceptualization of the functional necessity principle and an Optional Protocol are imperatively needed to affirm the protection of diplomatic cyberspace as an integral element of digital sovereignty.*

Keywords: *Diplomatic Law, 1961 Vienna Convention, Inviolability, Digital Diplomatic Bag, Cyber Espionage*

Abstrak. Evolusi teknologi informasi melahirkan tantangan eksistensial terhadap doktrin hukum diplomatik klasik, khususnya mengenai asas kesucian (inviolability) perwakilan diplomatik dan komunikasi rahasia. Konvensi Wina 1961 tentang Hubungan Diplomatik dirancang dalam konstelasi fisik-analog, sehingga tidak secara eksplisit mengomodasi fenomena peretasan siber (cyber espionage) serta transmisi dokumen berklasifikasi rahasia via jaringan digital (digital diplomatic bag). Penelitian hukum normatif ini menganalisis dinamika penafsiran norma inviolabilitas gedung perwakilan (Pasal 22) dan korespondensi resmi (Pasal 27 Konvensi Wina 1961) dalam menghadapi ancaman intrusi siber yang dilancarkan oleh negara penerima (receiving State) maupun aktor non-negara. Hasil penelitian menunjukkan bahwa terdapat ambiguitas yuridis mengenai apakah operasi siber pasif dapat dikualifikasikan sebagai pelanggaran batas fisik perwakilan diplomatik, serta bagaimana pertanggungjawaban hukum negara atas insiden peretasan data diplomatik. Diperlukan rekonseptualisasi asas 'functional necessity' serta formulasi Protokol Tambahan (Optional Protocol) guna menegaskan perlindungan domain siber diplomatik sebagai bagian tak terpisahkan dari kedaulatan digital perwakilan asing.

Kata kunci: Hukum Diplomatik, Konvensi Wina 1961, Inviolabilitas, Kantong Diplomatik Digital, Intelijen

Naskah Masuk: 23 Juli 2026; Revisi: 23 Juli 2026; Diterima: 23 Juli 2026; Terbit: 24 Juli 2026.

1. LATAR BELAKANG

Hukum diplomatik merupakan salah satu cabang hukum internasional publik tertua yang bertumpu pada asas saling menghormati kedaulatan dan fasilitasi hubungan antarnegara. Instrumen utama yang menjadi soko guru dalam pergaulan diplomatik modern adalah Konvensi Wina 1961 tentang Hubungan Diplomatik (Vienna Convention on Diplomatic Relations/VCDR 1961)[1]. Landasan filosofis dari hak-hak istimewa dan kekebalan diplomatik dalam VCDR 1961 tidak lagi bersandar semata-mata pada teori eksteritorialitas (exterritoriality theory) atau teori representatif, melainkan pada teori kebutuhan fungsional (functional necessity theory). Teori ini menegaskan bahwa imunitas diberikan guna menjamin pelaksanaan fungsi perwakilan diplomatik secara efisien tanpa hambatan dari negara penerima[2].

Namun demikian, lanskap geopolitik abad ke-21 tengah menghadapi disrupsi masif akibat hadirnya ranah siber (cyberspace). Fungsi perwakilan diplomatik yang dulunya bergantung pada dokumen fisik, kurir diplomatik bertatap muka, dan kantong diplomatik (diplomatic bag) berbahan kain berkunci, kini telah bertransisi menggunakan infrastruktur digital, jaringan komputasi awan (cloud server), serta komunikasi terenkripsi[3]. Transisi ini melahirkan fenomena 'kantong diplomatik digital' (digital diplomatic bag) dan pengiriman telegram diplomatik via saluran siber.

Evolusi teknologi ini sayangnya tidak diimbangi oleh pembaruan teks normatif VCDR 1961. Statuta internasional ini dirancang pada era analog di mana gangguan terhadap perwakilan diplomatik diukur dari pelanggaran fisik, seperti penerobosan gedung oleh aparat lokal atau penyitaan kantong diplomatik di perbatasan[4]. Ketika negara penerima atau entitas non-negara melancarkan serangan siber berupa penyadapan sinyal (signals intelligence), pemasangan malware pada server kedutaan, atau peretasan data diplomatik terenkripsi dari jarak jauh, timbul celah hukum yang serius[5].

---

[1] United Nations, Vienna Convention on Diplomatic Relations, United Nations Treaty Series, vol. 500, (1961), p. 95.
[2] Eileen Denza, Diplomatic Law: Commentary on the Vienna Convention on Diplomatic Relations, 4th ed. (Oxford: Oxford University Press, 2016), hlm. 15.
[3] Alexander Klimburg, The Darkening Web: The War for Cyberspace and Diplomatic Immunity (New York: Penguin Press, 2020), hlm. 112.
[4] Malcolm N. Shaw, International Law, 9th ed. (Cambridge: Cambridge University Press, 2021), hlm. 684.
[5] Sean Watts, 'Low-Intensity Cyber Operations and the Inviolability of Diplomatic Correspondence', Harvard National Security Journal, Vol. 10, No. 2 (2019), hlm. 215.

Isu hukum mendasar (legal issue) yang muncul adalah apakah intrusi siber tanpa presensi fisik dapat dikualifikasikan sebagai pelanggaran terhadap asas kesucian gedung perwakilan (inviolability of mission premises) berdasarkan Pasal 22 VCDR 1961 dan kesucian korespondensi resmi berdasarkan Pasal 27 VCDR 1961[6]. Sejauh mana perlindungan hukum internasional dapat diregangkan untuk mencakup infrastruktur siber dan kantong diplomatik digital? Serta bagaimana mekanisme pertanggungjawaban negara (State responsibility) dapat diterapkan dalam insiden espionase siber diplomatik yang acapkali bersifat nir-atributif?

Penelitian ini bertujuan untuk menganalisis secara mendalam fleksibilitas interpretatif VCDR 1961 menghadapi ancaman siber, merekonstruksi konsep inviolabilitas diplomatik dalam dimensi digital, serta merumuskan rekomendasi pembaruan hukum internasional demi menjamin independensi perwakilan diplomatik di era digital.

2. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif (doctrinal legal research) dengan fokus pada analisis hukum internasional publik[7]. Pendekatan yang digunakan mencakup pendekatan perundang-undangan/perjanjian internasional (treaty approach), pendekatan kasus (case approach) berbasis yurisprudensi Mahkamah Internasional (ICJ), serta pendekatan analitis-konseptual (conceptual approach) terhadap doktrin-doktrin inviolabilitas diplomatik.

Bahan hukum primer meliputi Konvensi Wina 1961, Konvensi Wina 1969 tentang Hukum Perjanjian Internasional (VCLT 1969), Draft Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA 2001)[8], serta Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Bahan hukum sekunder mencakup karya ilmiah, laporan Komisi Hukum Internasional (ILC), dan jurnal hukum internasional bereputasi. Analisis dilakukan secara kualitatif-teleologis

3. HASIL DAN PEMBAHASAN

---

[6] Michael N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press, 2017), hlm. 210.

[7] Anthony Aust, Modern Treaty Law and Practice, 3rd ed. (Cambridge: Cambridge University Press, 2013), hlm. 88.

[8] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts with Commentaries, Yearbook of the ILC, Vol. 2, Part 2 (2001), hlm. 38.

3.1 Teleologi Pasal 22 VCDR 1961: Membedah Konsep Physical Boundaries vs Cyber Premises

Pasal 22 ayat (1) VCDR 1961 menyatakan secara tegas bahwa 'The premises of the mission shall be inviolable'. Secara tradisional, frasa 'premises' dimaknai sebagai bangunan, bagian dari bangunan, dan tanah sekitarnya yang digunakan untuk tujuan perwakilan diplomatik[9]. Kewajiban negara penerima mencakup dua dimensi: kewajiban pasif (abstain dari memasuki gedung tanpa izin) dan kewajiban aktif (mengambil langkah-langkah khusus untuk melindungi gedung dari gangguan atau perusakan).

Tantangan timbul ketika intervensi dilakukan secara nir-fisik melalui gelombang elektromagnetik atau serangan malware yang menembus firewall router kedutaan. Berdasarkan Pasal 31 ayat (1) VCLT 1969, perjanjian internasional harus ditafsirkan sesuai dengan 'ordinary meaning' dalam konteks dan maksud serta tujuannya (object and purpose)[10]. Tujuan utama Pasal 22 adalah menjamin integritas dan kerahasiaan operasional perwakilan. Oleh karena itu, penafsiran teleologis (evolutive interpretation) menuntut bahwa server, komputer, dan jaringan Wi-Fi yang berlokasi di dalam gedung kedutaan merupakan perpanjangan dari 'premises', sehingga setiap peretasan terhadapnya merupakan pelanggaran langsung terhadap Pasal 22 VCDR 1961.

3.2 Erosi Asas Kesucian Kantong Diplomatik dalam Era Transmisi Data Digital (Pasal 27 VCDR 1961)

Pasal 27 ayat (3) VCDR 1961 menetapkan norma absolut: 'The diplomatic bag shall not be opened or detained'. Kantong diplomatik dirancang untuk melindungi dokumen resmi dan barang-barang yang semata-mata untuk penggunaan resmi[11]. Dalam praktik modern, mayoritas dokumen diplomatik dikirimkan dalam bentuk file digital terenkripsi melalui jaringan internet, yang sering kali diistilahkan sebagai 'digital diplomatic bag'.

[9] Eileen Denza, op. cit., hlm. 135.
[10] United Nations, Vienna Convention on the Law of Treaties, United Nations Treaty Series, vol. 1155, (1969), Pasal 31.
[11] Richard Patterson, 'Digital Diplomatic Bags: Redefining Article 27 of the Vienna Convention in the Cyber Age', International & Comparative Law Quarterly, Vol. 71, No. 3 (2022), hlm. 618.

Tabel 1. Matriks Komparasi Karakteristik Kantong Diplomatik Konvensional dan Kantong Diplomatik Digital

Parameter Analisis	Kantong Diplomatik Konvensional (Pasal 27)	Kantong Diplomatik Digital (Cyber Era)
Wujud & Bentuk	Fisik (Peti, Kantong Kain dengan Segel Resmi)	Non-Fisik (Paket Data Terenkripsi, Cloud Server)
Mekanisme Gangguan	Pemeriksaan Fisik, Penahanan di Pabean/Perbatasan	Intersepsi Siber, Decryption Key Extraction, Malware
Rezim Perlindungan	Perlindungan Absolut Tanpa Pemindaian X-Ray	Ambiguitas Norma (Membutuhkan Analogi Legal/Evolutif)

Tabel di atas mengarsir jurang pengaturan (regulatory gap) yang nyata. Ketika negara penerima atau pihak ketiga melakukan intersepsi terhadap lalu lintas data diplomatik (packet sniffing) atau memaksa pembongkaran kunci enkripsi, tindakan tersebut secara substantif merupakan bentuk 'pembukaan' atau 'penahanan' kantong diplomatik secara siber. Tanpa pengakuan tegas terhadap kantong diplomatik digital, prinsip kerahasiaan komunikasi diplomatik yang dijamin Pasal 27 ayat (1) VCDR 1961 akan menjadi norma yang tidak bergigi[12].

3.3 Atribusi dan Pertanggungjawaban Negara atas Espionase Siber Diplomatik

Penerapan hukum pertanggungjawaban negara (State responsibility) dalam insiden siber diplomatik menghadapi kendala pembuktian dan atribusi. Berdasarkan Pasal 4 dan Pasal 8 ARSIWA 2001, tindakan siber hanya dapat diatributkan kepada negara apabila dilakukan oleh organ negara atau oleh kelompok yang bertindak di bawah instruksi, arahan, atau kendali efektif (effective control) negara tersebut[13].

[12] Ashley Barke, 'Cyber Espionage and the Inviolability of Diplomatic Archives under International Law', Melbourne Journal of International Law, Vol. 22, No. 1 (2021), hlm. 59.
[13] Francesca Vitucci, 'Cyber Espionage Against Diplomatic Missions and the Due Diligence Principle', European Journal of International Law, Vol. 34, No. 2 (2023), hlm. 412.

Guna mengatasi kebuntuan pembuktian dalam ranah siber, penelitian ini mengajukan rekonstruksi standar kewajiban 'Due Diligence' yang dibebankan kepada negara penerima:

Kewajiban Uji Tuntas Siber (Cyber Due Diligence): Negara penerima berkewajiban secara hukum untuk memastikan bahwa wilayah atau infrastruktur siber di bawah kedaulatannya tidak digunakan oleh organ negara maupun kelompok peretas independen untuk menyerang sistem siber kedutaan asing.

Pergeseran Beban Pembuktian (Reversal of Burden of Proof): Apabila peretasan terbukti berasal dari infrastruktur siber pemerintah atau ISP nasional negara penerima, berlaku presumsi awal tanggung jawab negara (prima facie responsibility) sampai negara penerima dapat membuktikan sebaliknya.

Penerapan Sanksi Diplomatik dan Countermeasures: Negara pengirim yang menjadi korban serangan siber diplomatik berhak menyatakan peretas sebagai persona non grata atau mengambil tindakan balasan yang proporsional (proportional countermeasures) sesuai hukum internasional.

4. KESIMPULAN DAN SARAN

4.1 Kesimpulan

1. Terdapat ketidakselarasan normatif antara teks tekstual Konvensi Wina 1961 yang berorientasi fisik-analog dengan realitas operasional diplomatik di era siber. Penafsirannya harus dilakukan secara teleologis evolutif untuk menegaskan bahwa peretasan sistem siber kedutaan merupakan pelanggaran atas inviolabilitas gedung perwakilan (Pasal 22) dan inviolabilitas korespondensi resmi (Pasal 27).
2. Konstruksi pertanggungjawaban negara dalam insiden espionase siber diplomatik menuntut penguatan doktrin due diligence. Negara penerima tidak hanya wajib mematuhi kewajiban pasif untuk tidak meretas, tetapi juga memikul kewajiban aktif untuk mencegah dan menghentikan segala bentuk serangan siber yang menyasar perwakilan diplomatik dari wilayah hukumnya.

4.2 Saran

1. Komisi Hukum Internasional (International Law Commission/ILC) dan negara-negara pihak VCDR 1961 disarankan untuk merumuskan Protokol Tambahan (Optional Protocol) mengenai Perlindungan Perwakilan Diplomatik di Era Siber, yang secara eksplisit mengakui status yuridis Kantong Diplomatik Digital dan Inviolabilitas Infrastruktur Siber Diplomatik.
2. Kementerian Luar Negeri Republik Indonesia bersama Badan Siber dan Sandi Negara (BSSN) perlu menyusun Standard Operating Procedure (SOP) Keamanan Siber Perwakilan RI di Luar Negeri guna mengantisipasi ancaman espionase siber serta memperkuat klaim perlindungan hukum internasional.

DAFTAR REFERENSI

Aust, A. (2013). Modern Treaty Law and Practice (3rd ed.). Cambridge: Cambridge University Press.

Barke, A. (2021). Cyber Espionage and the Inviolability of Diplomatic Archives under International Law. Melbourne Journal of International Law, 22(1), 45-78.

Denza, E. (2016). Diplomatic Law: Commentary on the Vienna Convention on Diplomatic Relations (4th ed.). Oxford: Oxford University Press.

International Law Commission. (2001). Draft Articles on Responsibility of States for Internationally Wrongful Acts with Commentaries. Yearbook of the International Law Commission, 2(2), 31-143.

International Law Commission. (2018). First Report on the Protection of Diplomatic Premises and Cyber Threats by Special Rapporteur. Geneva: United Nations.

Klimburg, A. (2020). The Darkening Web: The War for Cyberspace and Diplomatic Immunity. New York: Penguin Press.

Patterson, R. (2022). Digital Diplomatic Bags: Redefining Article 27 of the Vienna Convention in the Cyber Age. International & Comparative Law Quarterly, 71(3), 612-639.

Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press.

Shaw, M. N. (2021). International Law (9th ed.). Cambridge: Cambridge University Press.

United Nations. (1961). Vienna Convention on Diplomatic Relations. United Nations Treaty Series, vol. 500, p. 95.

United Nations. (1969). Vienna Convention on the Law of Treaties. United Nations Treaty Series, vol. 1155, p. 331.

Vitucci, E. (2023). Cyber Espionage Against Diplomatic Missions and the Due Diligence Principle. European Journal of International Law, 34(2), 401-428.

Watts, S. (2019). Low-Intensity Cyber Operations and the Inviolability of Diplomatic Correspondence. Harvard National Security Journal, 10(2), 211-245.