IRSHAD

INTERNATIONAL JOURNAL OF LAW AND POLICY

Virtual Embassies and Digital Consular Services Transforming Traditional Diplomatic Practice

[Boburhon Ziyamov][1]

[1]*Tashkent State University of Law*

Keywords:

Virtual Embassies, Digital Consular Services, Data Embassy, Diplomatic Inviolability, Vienna Conventions, Electronic Apostille, Digital Diplomacy

ABSTRACT

Diplomacy now moves through websites, cloud servers, and online consular portals. These tools reach citizens abroad quickly, yet the governing treaties were written for physical missions. This study aims to examine whether the Vienna Conventions protect virtual embassies and digital consular services. It also identifies legal changes needed to secure their status. The study follows a qualitative design using doctrinal and document analysis of treaties, policies, and scholarly works. The results show that virtual embassies do not qualify as diplomatic missions under current law. Consular functions fit partly within existing rules, while servers outside mission premises lack clear protection. Digital archives can gain protection through a functional treaty reading. Cross-border recognition of digital consular documents depends on bilateral and regional agreements. The study recommends data embassy agreements, wider electronic apostille use, and an additional protocol to the Vienna Conventions. Such reforms would let diplomatic law keep pace with digital statecraft.

How to Cite: Ziyamov, B. (2026). Virtual Embassies and Digital Consular Services Transforming Traditional Diplomatic Practice. *International Journal of Law and Policy, 4*(10), 105-124. https://doi.org/10.59022/ijlp.572

I. Introduction

In 2011, the United States opened an embassy for Iran that had no building. American diplomats could not enter Tehran, so they served Iranians through a website. This example shows how technology now reshapes one of the oldest practices of statecraft. Diplomacy once depended on buildings, flags, sealed letters, and personal meetings between envoys. Today, many states deliver visas, passports, and legal documents through secure online platforms. Citizens living abroad can request urgent help without travelling long distances to a consulate. These digital tools save public money and reach people in remote or hostile regions. Yet a virtual embassy has no premises, while premises sit at the centre of diplomatic protection. The legal value of an online consular act also remains unclear in many states. This topic matters to lawyers, foreign ministries, and citizens living abroad. Digital platforms have already changed how states engage foreign publics (Bjola et al., 2019).

Modern diplomatic law grew from centuries of customary practice between sovereign rulers. States later codified these customs in the Vienna Convention on Diplomatic Relations of 1961. Two years later, the Vienna Convention on Consular Relations regulated consular posts and their functions. Both treaties assume that diplomats work from physical premises inside the receiving state. They protect buildings, archives, bags, and personnel, but they say nothing about digital spaces. In practice, Sweden opened a virtual embassy in Second Life in 2007 to promote its national image. Estonia later placed its government data in a protected server room in Luxembourg. The pandemic then forced consulates worldwide to move routine services onto online platforms. Early studies focused on technology adoption, public communication, and management challenges. They rarely tested these new practices against the binding rules of diplomatic and consular law. Electronic diplomacy research mostly examined factors behind its implementation (Al-Muftah et al., 2018).

States now perform many diplomatic and consular functions through screens rather than offices. Scholars already know that digital tools improve speed, reach, and cost in diplomacy. They also know that ministries use social media to reach foreign audiences. The legal side of this shift remains far less clear than its practical benefits. The Vienna Conventions protect the inviolability of premises, archives, and official correspondence. These protections do not clearly extend to servers, cloud storage, or online portals. A receiving state may block or monitor a virtual embassy without clear consequences. Consular officers may also issue digital documents that other states refuse to recognize. Citizens using online consular help may lose protection when platforms fail. This study addresses missing legal rules for virtual diplomatic institutions. It asks how existing treaty law can protect digital missions and their users. Technological change has already placed pressure on diplomatic and consular law (András, 2023).

Recent research shows that digital technology has entered the daily work of professional diplomats. Studies of multilateral diplomacy reveal that diplomats now negotiate through messaging applications and video calls. Such tools allow quick coordination between national delegations during busy international conferences. Diplomats also use private messaging groups to share draft texts and build informal alliances. These practices change the speed and style of negotiation inside international organizations. They also blur the line between official communication and purely personal conversation. Messages sent through commercial applications may fall outside the protection of diplomatic archives. Such data may also travel through servers located in third states with different privacy laws. This research explains adaptation, but it does not test the legal status of messages. The legal protection of digital diplomatic correspondence therefore remains an open question. Evidence from Geneva shows that diplomats adapt to digital tools through gradual practice (Cornut et al., 2022).

Other recent findings link digital diplomacy with the protection of national interests. Developing states increasingly use online platforms to explain their foreign policy positions to the world. They also use digital channels to engage Diaspora communities living in many countries. Such engagement can attract investment, tourism, and political support for the home state. Digital outreach also helps small or poorer states compete with powerful states for attention. These benefits depend on reliable internet access, trained staff, and secure communication systems. Weak cyber security may expose diplomatic messages to manipulation by hostile actors. False information spread online may also damage the reputation of a state abroad. This research highlights strategic gains, but it gives little attention to binding legal obligations. It also does not discuss consular services delivered to their citizens through digital platforms. The Ethiopian experience shows that digital diplomacy can actively support the national interest of developing states (Ayenew, 2024).

The reviewed literature offers strong evidence on the practical value of digital diplomacy. It explains how diplomats adapt and how ministries adopt new technology. Its main weakness lies in its limited engagement with binding rules of international law. Few studies ask whether a virtual embassy qualifies as a diplomatic mission under treaty law. Fewer studies examine the inviolability of servers, digital archives, and online consular portals. The legal effect of digital consular documents across borders also lacks careful analysis. Most researchers recommend future work on regulation, accountability, and clear legal frameworks. This study responds directly to that repeated call for careful legal analysis. It examines virtual embassies and digital consular services through the lens of diplomatic and consular law. It also proposes practical directions for adapting existing treaties to modern digital diplomatic practice. New technical models test artificial intelligence for consular services without settling legal status (Aljohani et al., 2026).

1. To examine whether virtual embassies and digital consular services fall within the scope of the Vienna Convention on Diplomatic Relations of 1961 and the Vienna Convention on Consular Relations of 1963.

2. To analyse the legal protection of servers, digital archives, and online consular portals under the rules of inviolability and immunity.
3. To propose legal measures for adapting existing diplomatic and consular law to virtual diplomatic practice.

How far can the Vienna Conventions on diplomatic and consular relations protect virtual embassies and digital consular services, and what legal changes are needed to secure their status?

This study matters because diplomatic law must keep pace with digital state practice. It offers legal scholars a clear analysis of virtual missions under the Vienna Conventions. It also adds new knowledge on the inviolability of servers and digital archives. Foreign ministries can use its findings to design safer and lawful online services. Consular officers may gain clearer guidance on issuing and recognizing digital documents. Lawmakers can draw on its proposals when negotiating bilateral agreements on digital missions. Citizens abroad will benefit from stronger protection when they seek help online. Virtual missions may give poorer states a lawful and cheaper presence abroad. International organizations may use its findings to start talks on a new protocol. Digital tools carry the values and policy choices of states, not only their services. Swedish practice shows that digital diplomacy can also express and change the foreign policy direction of states (Aggestam et al., 2022).

II. Methodology

This study follows a qualitative design suited to legal questions about rules and meaning. It examines laws, treaties, and state practice rather than numbers or statistical trends. The core legal sources include the Vienna Convention on Diplomatic Relations and the Vienna Convention on Consular Relations. The study also reviews the Hague Apostille Convention, the General Data Protection Regulation, and the European digital identity framework. Recent European rules on digital visas and consular protection complete this legal sample. Official texts were collected from the United Nations Treaty Collection, the Hague Conference website, and the European Union legal portal. Foreign ministry websites provided policy statements and descriptions of digital consular services. Search terms included virtual embassy, digital consular services, data embassy, diplomatic inviolability, electronic apostille, and digital diplomacy. These keywords helped the study locate legal rules and relevant academic debate.

The study took several steps to keep its sources valid and reliable. It selected mainly peer-reviewed journal articles published within the last five years. Older works appear only when they shaped the core scholarly debate on digital diplomacy. Each source was checked for author expertise, journal quality, and clear academic purpose. Legal texts were taken only from official portals to ensure accurate and current wording. The study also confirmed that every treaty and regulation remained in force during the research period. The analysis combined doctrinal legal analysis with careful document analysis. Doctrinal analysis

examined the text, purpose, and structure of each treaty provision. It tested whether existing rules on missions, premises, archives, and consular functions extend to digital practice. Document analysis reviewed policy papers, official statements, and scholarly articles to trace state practice. Together, these methods linked abstract legal rules with real developments in virtual embassies and digital consular services.

This study relied only on official documents and scholarly works available in the public domain. It involved no human participants, interviews, or any personal data. Every idea drawn from scholarly work carries a proper reference to its original author. This practice respects academic integrity and gives credit to earlier researchers. The researcher has no conflict of interest, and the study serves purely academic purposes. The study also sets clear boundaries for its scope and coverage. It focuses on the two Vienna Conventions and selected state practice from 2007 to 2026. It does not examine domestic criminal law or the internal rules of every foreign ministry. Some weaknesses remain beyond the control of the researcher. Technology evolves rapidly and constantly produces new forms of digital diplomacy. States can also amend laws and policies at any time. Some findings may therefore need review as digital practice and legal rules continue to change.

III. Results

Diplomacy now operates through websites, portals, video calls, and secure digital archives. This shift raises a clear legal question about the reach of existing treaty law. The study asked how far the Vienna Conventions protect virtual embassies and digital consular services. It also asked which legal changes states need to secure the status of these services. To answer these questions, the study examined treaty texts, state practice, and recent scholarship. It tested each digital practice against the rules on missions, premises, archives, and consular functions. The early results concern the legal recognition of virtual missions and online consular functions. Later results concern the protection of servers, digital archives, and electronic correspondence. The final result concerns the cross-border recognition of digital consular documents. Together, these findings show where current law protects digital diplomacy and where it fails. Emerging artificial intelligence tools may soon deepen this transformation of diplomatic practice (Manor, 2026).

The study finds that neither Vienna Convention mentions virtual embassies or digital missions. Article 1 of the Diplomatic Convention defines mission premises as buildings and land. This definition reflects the physical world of diplomacy in 1961. A virtual embassy has no building, no land, and often no resident staff. It therefore cannot meet the plain wording of the treaty definition. Article 2 also requires mutual consent before states establish diplomatic relations and missions. The United States Virtual Embassy Tehran operated without any consent from Iran. Iran blocked the website within hours, and no treaty offered a remedy. This case shows that virtual missions exist outside the formal protection of diplomatic law. States treat them as public diplomacy tools rather than legal diplomatic

missions. This result answers the first objective and confirms a clear legal gap. Online embassy portals already serve travelers well, yet their legal identity remains undefined (Hill, 2020).

The study also finds that consular law is more flexible than diplomatic law. Article 5 of the Consular Convention lists consular functions in broad and open terms. These functions include issuing passports, visas, and notarial documents for nationals. The text regulates the function itself rather than the method of its delivery. This wording allows states to perform many consular tasks through online platforms. Several states now accept digital visa applications and electronic passport renewals. Consular officers can also advise detained nationals through secure video calls. Some functions still need physical presence, such as prison visits and emergency evacuation. Consular acts must also respect the laws of the receiving state. A receiving state may therefore restrict online services through its own data laws. This result partly answers the first objective of the study. Digital governance models show that public services can move online without losing their core legal function (Jobe, 2024).

The study finds a serious weakness in the protection of digital diplomatic assets. Article 22 of the Diplomatic Convention declares mission premises inviolable. Agents of the receiving state cannot enter these premises without consent of the head of mission. This rule protects physical rooms, furniture, and other property located inside the mission. Many embassies now store sensitive data on servers outside their premises. Commercial cloud providers often host this data in third states. These servers do not qualify as mission premises under the plain treaty definition. A receiving state may lawfully demand access to data held by local providers. A third state may also seize servers under its own criminal law. No treaty rule clearly forbids such interference with remote diplomatic data. This result addresses the second objective and exposes a major protection gap. Science and technology now demand a fresh theoretical approach to diplomatic practice (Kaltofen & Acuto, 2018).

The study finds stronger protection for digital archives than for digital premises. Article 24 of the Diplomatic Convention protects mission archives and documents at any time. The phrase “wherever they may be” frees this protection from physical location. Article 1 of the Consular Convention defines consular archives broadly to include papers and documents. A functional reading can extend these terms to electronic files and digital records. Article 27 also protects official correspondence relating to the mission and its functions. Emails and encrypted messages perform the same function as traditional diplomatic letters. Scholars increasingly accept this functional approach to treaty interpretation. Messages on public social media accounts may lack the same protection. These messages are public by nature and fall outside confidential correspondence. This result answers the second objective with a partly positive finding. Greek practice shows how official diplomatic communication now flows through public digital platforms (Kacziba et al., 2025).

The study finds that digital consular documents face uneven recognition across borders. A digital certificate issued by a consulate may carry no legal value abroad. Each receiving state decides whether to accept electronic signatures and digital seals. The Consular Convention contains no rule on the validity of electronic consular acts. States fill this gap through bilateral consular agreements and mutual recognition arrangements. Some agreements now accept electronic signatures for visas, apostilles, and civil registration documents. Other states still demand paper originals with handwritten wet ink signatures. This difference creates delay, extra cost, and legal uncertainty for citizens living abroad. Regional cooperation can reduce these problems through shared standards for digital documents. Small states with limited consular networks benefit most from such cooperation. This result addresses the second objective and points toward treaty reform. Western Balkan experience shows that regional digital diplomacy depends on close cooperation between neighboring states (Justinek, 2019).

IV. Discussion

A. The Vienna Conventions do not Expressly Recognized Virtual Embassies as Diplomatic Missions

This result asks a deep question about what counts as an embassy in law. The answer is clear: a website or social media account is not a diplomatic mission. Article 3 of the Diplomatic Convention lists the core tasks of a mission. These tasks include representing the sending state, protecting nationals, and negotiating with the host government. A virtual embassy performs only a few of these tasks, mainly public outreach. It cannot negotiate formally because it lacks an accredited head of mission. It also cannot protect nationals inside a territory where it has no staff. Virtual embassies therefore act as communication channels rather than legal representatives of the state. Representation in law requires consent, accreditation, and a physical point of contact. This finding moves the debate from technology to legal status. Russian scholars reached a similar view after studying American virtual embassy projects in hostile states (Arlyapova & Ponomareva, 2023).

The absence of legal status creates real risks for states, diplomats, and ordinary users. A host government may block a virtual embassy without breaching any treaty duty. It may also punish local citizens who visit or contact such platforms. Users in authoritarian states often take serious personal risks when they seek foreign help online. Their messages may reach security services rather than the foreign diplomats they trust. The sending state cannot claim immunity for its digital staff working from abroad. It also cannot invoke inviolability to stop the hacking of its virtual platform. These gaps matter because states now invest large public budgets in online representation. Foreign ministries train officers to manage digital channels as part of their normal daily diplomatic work. Such investment deserves a stable legal base that protects both providers and users. Technological advancement has already reshaped how diplomats represent states and communicate across borders (Rashica, 2026).

State practice strongly supports this finding across several regions and decades. The American virtual embassy for Iranians still offers visa information without approval. Israel launched a Twitter account in 2013 to speak directly with citizens of Gulf states. The account invited dialogue with audiences that Israel could not reach through formal channels. Washington also created virtual presence posts for cities without a physical consulate. None of these projects received accreditation from the host state. None claimed protection under the Diplomatic Convention either. Each sending state instead treated its platform as a public information service. A similar tension appeared in Beijing when the American embassy published hourly air quality data. Chinese officials argued in 2012 that this practice breached diplomatic rules and local sovereignty. The dispute showed how digital embassy activity can trigger formal legal objections. Recent research traced public effects after the United States ended embassy air monitoring (Zhou, 2026).

This study relies mainly on treaty texts, official statements, and published academic work. Such sources reveal the formal legal position but not private diplomatic arrangements. Some states may accept virtual missions through confidential exchanges of notes. Such private consent would never appear in public treaty collections. Court decisions on virtual embassies are almost absent, so guidance remains thin. Most documented cases come from Western states with strong digital budgets. Smaller states in Africa, Asia, and Latin America receive far less scholarly attention. Their practice may show different attitudes toward consent and digital presence. Language also narrows the sources, since most reviewed material appears in English. Technology also changes faster than legal research can record it. Popular platforms today may vanish within a few years. These gaps suggest caution before treating the finding as a universal rule. African digital diplomacy, for example, follows distinct priorities that deserve separate study (Wekesa, 2021).

Data embassies offer a useful contrast with virtual embassies. Estonia stores copies of key state data in Luxembourg under a bilateral agreement. The arrangement protects government services if a cyberattack or invasion disrupts systems at home. That agreement grants the servers protection similar to diplomatic premises. Monaco later signed a comparable arrangement with Luxembourg for its own state data. These cases show that states can extend diplomatic protection to digital assets by consent. Virtual embassies lack such agreements because they often target hostile or closed states. Closed regimes rarely grant consent to platforms designed to bypass their own censorship. Political relations therefore shape legal protection more than technology does. Internet controls, cyber capacity, and domestic law in the host state also play a role. A friendly host may tolerate digital outreach, while a rival sees interference. Online diplomacy differs from traditional diplomacy in form, speed, and legal visibility (Sakamoto, 2024).

This finding carries clear lessons for foreign ministries and treaty makers. States should notify host governments before launching virtual embassies wherever relations allow. They should also sign bilateral agreements that define the status of digital missions. These agreements should cover staff, servers, user data, and dispute settlement. Such agreements

can follow the data embassy model tested by Estonia. The Council of the European Union adopted conclusions in 2022 and 2023. These conclusions make digital diplomacy a core part of external action. Regional bodies can build on this work through common standards for virtual representation. A future additional protocol to the Diplomatic Convention could settle the question globally. Until then, virtual embassy users need clear warnings about their legal exposure. Lawyers advising ministries should treat these platforms as public diplomacy tools, not protected missions. Scholars have called for practice-based research to guide the digital transformation of diplomacy (Hedling & Bremberg, 2021).

B. Digital Consular Functions Fall Partly within the Existing Scope of Consular Law

This result shows that consular law can absorb many digital services without new treaty text. Article 5 of the Consular Convention describes what consuls do, not how they do it. Issuing a passport online still counts as issuing a passport under the treaty. Registering a birth through a secure portal still counts as civil registration. The final clause of Article 5 also allows any function that the receiving state does not oppose. This clause gives states room to test digital tools. The word partly matters, because some duties still need a consul in person. Article 36 grants consular officers the right to visit detained nationals in prison. A video call cannot fully replace that personal visit and its protective value. Consular law therefore accepts digital delivery for routine tasks, not urgent protection. Foreign ministries now see communication with nationals as their main consular task in the digital age (Melissen, 2020).

This finding matters because millions of people now live, study, and work outside their home states. Pakistan alone has a very large Diaspora spread across the Gulf, Europe, and North America. Its Pak-ID application lets overseas citizens apply for identity cards remotely. Nepal launched the application in 2026 for complaints, rescue requests, and embassy contact. Such tools save travel costs and reduce long queues at crowded consulates. Consular staff can then focus on complex cases that need personal attention. They also reach workers in remote labor camps far from any consular office. Faster service can protect vulnerable migrants from exploitation by agents and employers. Legal certainty for these services gives citizens confidence that online acts carry real value. Without it, digital help could become a weak substitute for protection. States have increasingly placed the safety of their nationals at the centre of digital diplomacy (Melissen & Caesar-Gordon, 2016).

Recent policy shows how quickly consular work has moved online. The European Union adopted a regulation in 2023 to digitalize the Schengen visa procedure. The United Kingdom replaced many physical immigration documents with electronic visas during 2024 and 2025. India, Turkey, and Pakistan already issue electronic visas through official government portals. Applicants upload documents, pay fees, and receive decisions without visiting any consulate. These systems rest on the consular power to issue visas under Article 5. No state has argued that online visas breach the Consular Convention. Receiving states rarely object, because these services seldom occur on their territory. The pandemic tested

this model when consulates organized repatriation flights through online registration. Thousands of stranded travelers returned home through systems built within a few weeks. Silence from other states suggests broad acceptance of such digital delivery. Officers at the digital frontlines often shape these services through professional judgment (Hedling, 2026).

This study cannot measure how well digital consular services work in daily practice. It reviews legal texts and policy rather than surveys of users or officials. Official websites often describe services in ideal terms that hide technical failures. Complaints from users rarely reach academic studies or public reports. Users without smart phones, stable internet, or digital skills may not benefit at all. Elderly citizens and low-income migrants often face the greatest barriers to online access. Some states also limit online services to nationals who hold digital identity credentials. These gaps may weaken the protection the law appears to offer. The study also gives less attention to honorary consuls, who often lack digital systems. Honorary consuls serve many small states and remote regions across the world. Data on cyber attacks against consular portals remains scarce and rarely published. Recent work shows technology transforming consular services, though practice differs widely (Mitev & Anichienco, 2025).

Diplomatic missions and consular posts receive different treatment under the two treaties. Representation depends on accreditation and consent, while consular service depends on function. This difference explains why consular tasks move online more easily than diplomatic tasks. A consulate can serve nationals online without asking the host to accept new representation. Some tension appears in visa practice, where digital systems meet human judgment. Algorithms can sort applications, but officers still decide difficult or sensitive cases. The final decision remains a sovereign act performed by a human officer. Domestic data laws also shape how far online services can operate across borders. The General Data Protection Regulation restricts transfers of personal data outside Europe. Political relations matter, because a hostile host may block consular websites. Language, cost, and digital skills shape who uses these services. Research on visa issuance in China shows that consular officers keep discretion despite diplomatic pressure (Dupont, 2025).

This result offers guidance for ministries designing digital consular services. States should anchor each online service in a clear function listed under Article 5. They should keep physical channels open for detention visits, emergencies, and vulnerable users. Online and offline channels should work together rather than compete for limited public resources. Clear notice to receiving states can prevent disputes over online services. Every consular platform needs strong authentication and data protection. Regional cooperation can also help citizens who lack a consulate of their own. The European Union already allows unrepresented citizens to seek help from other member states. A 2015 directive on consular protection sets detailed rules for this cooperation. A shared digital channel could extend this cooperation to online consular assistance. Such reforms would turn a partial legal fit into a reliable framework. Consular cooperation within the European Union also engages the fundamental rights of citizens abroad (Csatlós, 2018).

C. Inviolability of Premises does not Clearly Extend to Servers and Cloud Storage

This result exposes the weakest point in the protection of digital diplomacy. Article 22 links inviolability to premises that agents of the receiving state can physically enter. A server located inside the embassy building shares this protection. A server rented from a commercial provider elsewhere does not. That server sits under the ordinary jurisdiction of the state where it operates. Modern embassies rarely keep all data inside their own walls. Email systems, visa databases, and video platforms often run on cloud services. These services may sit in the receiving state, the sending state, or a third state. Each location brings a different legal regime and a different level of protection. Diplomatic lawyers rarely see these contracts before ministries sign them. The legal shield thus covers the building but not always the data. Scholars of diplomatic immunity stress that inviolability rests on a physical reading of treaty terms (Allah Rakha, 2024).

The risk is not theoretical, because data laws now reach deep into foreign servers. The American Clarifying Lawful Overseas Use of Data Act of 2018 allows authorities to demand data held abroad by American providers. The European Union adopted its own rules on cross-border access to electronic data in 2023. Such laws target criminal cases but can touch diplomatic data held by private firms. A foreign ministry may not even know where its cloud provider stores sensitive files. Hostile states can also target cloud systems through cyber operations without ever entering any embassy. Loss of visa records or diplomatic cables could endanger staff, sources, and ordinary applicants. Weak protection also reduces trust between states that share highly confidential information. Estonia answered this risk by agreeing special status for state servers placed in Luxembourg. That project tested whether Vienna rules stretch to a government data centre abroad (Robinson et al., 2019).

State practice confirms that governments treat digital infrastructure as a new frontier of protection. Ukraine moved large parts of its state data to foreign cloud providers after the 2022 invasion. This step kept public services running while missiles struck servers inside the country. The pandemic also pushed embassies to rely on video platforms for daily negotiation and outreach. Many ministries signed contracts with private technology firms without any diplomatic guarantees. Such contracts often allow providers to store data in several countries. These contracts follow commercial law, not the Vienna Conventions. Courts in the host state may therefore treat such data as ordinary commercial property. No state has yet won a case extending premises inviolability to remote servers. Practice shows growing reliance on cloud tools, but legal protection has not followed. Diplomacy has moved from digital adaptation toward digital adoption, creating a new hybrid form of practice (Bjola & Manor, 2022).

This study faces gaps that readers should clearly note. Contracts between ministries and cloud providers are rarely public. Ministries treat them as confidential security documents rather than ordinary procurement records. Security agencies keep cyber incidents against embassies secret. The study therefore cannot confirm how often states seize or

access diplomatic data. Details of server location and encryption remain hidden from researchers. Legal analysis must rely on general rules and a small number of public cases. Those cases often reach courts only years after the original incident. Platform dependence adds another risk, because private firms may close services without warning. Early virtual embassies in online worlds lost their content when platforms declined. Their data belonged to private companies, not sending states. A virtual presence is only as stable as its host platform. Sweden learned this lesson after it built an embassy inside a popular commercial virtual world in 2007 (Bengtsson, 2011).

Data embassies and met averse embassies show two very different paths. A data embassy rests on a treaty between two consenting states. A met averse embassy rests on terms of service written by a private platform. The platform can change those terms, suspend accounts, or close the world entirely. Barbados opened a met averse embassy in 2021 and described it as a step toward digital representation. Its servers, rules, and data remain under private corporate control. The Tallinn Manual accepts inviolability for cyber infrastructure located on mission premises. It offers no clear rule for infrastructure outside those premises. That silence leaves cloud and platform services in a legal grey area. Encryption, server location, and provider nationality all influence actual protection. Political trust between states also decides whether special agreements become realistic options. Legal writers have questioned whether such a met averse embassy can satisfy the 1961 Vienna Convention at all (Zhahira & Christianti, 2023).

This result calls for clear action from states, providers, and treaty makers. Ministries should store their most sensitive data inside mission premises or in sovereign facilities. They should also choose cloud providers that agree to resist foreign data demands. Contracts should require notice before any disclosure to foreign authorities. Bilateral agreements can grant special status to state servers placed abroad. Such agreements should cover access, inspection, seizure, and cyber defense duties. A future protocol could define digital premises as part of a diplomatic mission. Such a protocol would give remote servers the same shield as embassy buildings. States could also adopt a political declaration against cyber operations on diplomatic systems. Lawyers should review cloud contracts with the Vienna rules in mind. These steps can align legal protection with the real location of diplomatic data. Technology now plays a transformative role in international relations and demands matching legal safeguards (Romero, 2026).

D. Digital Archives and online Correspondence can gain Protection through Functional Interpretation

This result offers more hope than the findings on premises and servers. Article 24 of the Diplomatic Convention protects archives and documents at any time and wherever they may be. These words do not tie protection to a building, a country, or a medium. Protection follows the document itself, even when it leaves the mission. Article 33 of the Consular Convention gives consular archives the same strong protection. The consular definition of

archives even includes films, tapes, registers, ciphers, and codes. Such a list shows that the drafters expected new forms of recording. A functional reading asks what a document does rather than what it looks like. An encrypted email performs the same task as a sealed diplomatic letter once did. A digital visa file performs the same task as a paper register. Diplomatic archives have always held both political and commercial correspondence of great value to states (Gallo, 1996).

Strong protection for digital archives matters for the daily safety of diplomacy. Foreign ministries now create most of their records in electronic form. Negotiating drafts, reports, and instructions travel through secure networks rather than couriers. Many ministries have even abandoned paper archives for routine daily records. If these files lacked protection, receiving states could read them through local providers. Courts could also admit leaked diplomatic files as ordinary proof in trials. Sources and local staff named in such files could face serious personal danger. Protection of correspondence also allows honest reporting between missions and capitals. Diplomats report frankly only when they trust that their messages remain confidential. Without such trust, capitals would receive cautious reports that hide real risks. A functional reading of Article 24 protects this trust in the digital era. Studies of foreign ministries on social media show how much official diplomatic communication now happens online (Sevin, 2016).

Legal writing and court practice support a functional approach to digital archives. Leading commentators argue that Article 24 must cover computer storage and cyberspace. This view reflects the treaty purpose of keeping diplomatic communication confidential. The United Kingdom Supreme Court addressed leaked diplomatic cables in the Bancoult case in 2018. It allowed use of a cable that a third party had already published. The Court did not deny that electronic cables count as diplomatic documents. It only limited protection once the document had entered the public domain. The judgment thus treated publication, not the electronic format, as the decisive point. Article 27 also allows missions to use all appropriate means of communication. Email and encrypted messaging fall naturally within this broad treaty phrase. Recent agreements for international organisations now protect documents in whatever form they exist. These developments suggest growing acceptance that digital records deserve full legal protection (Abu Samra, 2023).

This finding also faces important gaps. Functional reading is a scholarly argument rather than a settled treaty rule. Some receiving states may prefer a strict reading tied to the original 1961 context. They may argue that the parties never agreed to protect electronic systems. Few courts have ruled directly on hacked or intercepted diplomatic emails. National judges may therefore reach different answers in similar cases. The Bancoult decision shows that leaks can weaken protection in practice. Data stolen by hackers and published online may lose much of its legal shield. Diplomatic messages sent through commercial applications raise further doubt. Their servers belong to private firms that may comply with local court orders. Diplomats sometimes use such applications for speed, even against internal security

rules. The study cannot test how often states quietly read such messages. These gaps mean functional protection depends on good faith and reciprocity between states (Pérez, 2026).

Public social media accounts receive different treatment from confidential archives. A tweet or public post aims to reach audiences, not to stay secret. Such content cannot claim protection designed for confidential correspondence. A private message sent through the same platform may deserve stronger protection. The test should turn on confidentiality and official purpose, not on the platform. This split creates an uncertain space between public diplomacy and private communication. Platform ownership also matters, because private companies control storage and deletion of content. Some states now rely on foreign platforms to project culture and national image. Others build national platforms to reduce dependence on foreign technology companies. Russia and China, for example, promote domestic platforms for official communication. These choices influence how much real control a state keeps over its own official records. Korean experience shows how digital platforms can serve as a powerful apparatus of national soft power (Jin, 2024).

This result gives ministries a practical path to protect digital records today. States should mark sensitive electronic files clearly as official archives of the mission. They should use encrypted systems owned or controlled by the state for confidential work. Such systems keep confidential files away from commercial servers in foreign jurisdictions. Public social media should carry only content that the ministry is ready to share openly. Joint statements can confirm that Article 24 covers electronic records. International courts can adopt this reading when disputes arise. A future protocol could remove any doubt by naming digital archives expressly. Training for diplomats should explain which channels enjoy legal protection and which do not. Internal rules can stop officers from using personal messaging accounts for work. Such measures can turn a scholarly argument into accepted state practice. Comparative work on public diplomacy shows that policy and practice develop together over time (Czarnecka-Gallas, 2026).

E. Cross-Border Recognition of Digital Consular Documents Depends on Bilateral Agreements

This result concerns the value of digital consular documents outside the issuing state. A consul may issue a digital birth certificate, power of attorney, or notarial act. The document has value only if authorities in another state accept it. Many authorities still treat paper with a wet signature as the safer choice. The Consular Convention gives consuls power to act as notaries and civil registrars. It says nothing about whether foreign authorities must accept their electronic versions. Each state therefore applies its own rules on electronic signatures and digital seals. Recognition thus depends on domestic law, bilateral treaties, and regional arrangements. A document valid in one country may still fail at a bank or court elsewhere. Digital consular service therefore remains only as strong as the recognition network behind it. Digital diplomacy has expanded the tools of foreign policy, but legal recognition has not yet kept equal pace (Adesina, 2017).

Uneven recognition causes real harm to families, workers, and businesses abroad. A migrant may need a power of attorney to sell property at home. A student may need verified documents to enrol at a foreign university. A family may need a death certificate to repatriate a body quickly. Each of these acts often happens under deep stress and strict time limits. Rejection of digital documents forces people to travel, pay fees, and wait for weeks. Such delays fall hardest on low-income workers with little time or money. Businesses also suffer when contracts and company papers face doubtful recognition. Investors may delay projects when they cannot rely on consular paperwork. Trust in consular services declines when digital documents fail in practice. Reliable recognition would make digital consular work a genuine and trusted public service. Consular activity during the pandemic showed how heavily citizens depend on fast digital help (Romero Vara, 2021).

Recent developments confirm that recognition now moves through specialized legal networks. The Hague Apostille Convention of 1961 was designed for paper documents. An Apostille certifies the origin of a public document for use abroad. Its electronic Apostille Programmed began in 2006 to support digital certificates and online registers. More than twenty contracting parties now issue electronic Apostilles. More than forty maintain electronic registers for online checks. Lithuania plans to issue electronic Apostilles from October 2026. Its notaries will issue them through a national electronic system. Pakistan joined the Apostille Convention in 2023, and China followed soon. These steps reduce the need for consular legalization of many public documents. Applicants save both time and fees under this much simpler route. They also show that states prefer targeted agreements over changes to the Consular Convention. Electronic signature laws and trusted verification systems now decide whether digital public documents cross borders (Pamment, 2013).

This study has some gaps that shape its conclusions on recognition. It focuses on treaty rules rather than daily decisions by banks, courts, and registries. Officials often reject valid digital documents because they lack training or clear guidance. A bank clerk may not know how to verify a foreign digital seal. Such informal refusals rarely appear in published sources. The study also could not review every bilateral consular agreement in force. Many older agreements predate the internet and contain no digital provisions. Others exist only in national languages or remain unpublished. Practice in small states and developing regions receives less attention in available literature. Their officials may face the greatest technical barriers to verification. Technology standards also change faster than treaties and domestic laws. A digital seal accepted today may need new verification tools tomorrow. These gaps call for empirical studies that follow digital documents through real procedures (Burkadze, 2023).

Regional systems show stronger recognition than global rules. The European Union revised its electronic identification and trust services rules in 2024. Member states must now offer European Digital Identity Wallets to citizens by 2026. These wallets will help citizens

present verified documents across all member states. Banks and many public bodies must accept these wallets under the new rules. No similar system yet exists at the global level for consular documents. Bilateral agreements fill some gaps, but they create a patchwork of different rules. A citizen may face one rule in Madrid and another in Dubai. Political trust strongly shapes whether two states accept each other's electronic signatures. Technical capacity also matters, because some states lack secure and reliable verification systems. Data protection laws can further limit the sharing of personal records across borders. Regional integration therefore offers a useful model for wider cooperation on digital consular documents (Allahrakha, 2023).

This result points toward practical reform at national, regional, and global levels. States should recognize electronic signatures of foreign consuls through clear domestic rules. They should join and implement the electronic Apostille Programmed. Bilateral consular agreements should include standard clauses on digital documents and seals. Regional bodies can build shared verification platforms modeled on European digital identity wallets. The United Nations Commission on International Trade Law offers model rules on electronic signatures. Its 2022 model law covers identity management and cross-border trust services. States can draw on these rules when updating consular and civil registration laws. A future protocol to the Consular Convention could set minimum standards for digital acts. Training should reduce informal refusals of valid electronic documents. These reforms would let digital consular documents travel as easily as citizens. The American virtual embassy for Iran shows that digital channels can keep communication open between estranged states (Williams, 2022).

F. Implication

This study questions the classic idea that diplomatic protection depends on physical territory and buildings. It shows that diplomatic law protects function, yet still ties full status to premises. Consular law adapts well to digital service, while diplomatic law struggles with virtual missions and remote servers. This split offers promise, because citizens abroad already receive faster passports and visas online. It also carries risk, because hostile states can block platforms or seize cloud data. Foreign ministries can use these findings to design lawful digital services and safer data storage. Estonia and Monaco protect state data through agreements with Luxembourg. The European Union now digitalizes Schengen visas and offers digital identity wallets to its citizens. Nepal and Pakistan have launched mobile tools that connect overseas citizens with their missions. Lawmakers should still adopt clear and binding rules on digital archives, data embassies, and electronic consular acts. An additional protocol to the Vienna Conventions could settle these questions for all states. Migrants, students, diplomats, and small states would gain the most from such reform. Courts and treaty bodies can apply functional readings of archive protection today. Rapid technological change and frequent amendment of national rules may require fresh review of these conclusions.

Conclusion

Embassies once stood as stone buildings guarded by flags, walls, and sealed doors. Today, many of them also live on screens, servers, and secure mobile apps. This study asked whether the law that protects traditional missions can protect these new digital forms. The question matters because states now serve millions of citizens through online consular channels. A worker in the Gulf can renew documents through an app instead of a crowded office. A student abroad can book urgent help with a few clicks. Nepal launched such a tool for its overseas workers in 2026. These gains rest on rules written in 1961 and 1963, long before the internet existed. Digital diplomacy now shapes trade, migration, crisis response, and national image worldwide. Any gap between law and technology therefore touches ordinary families as much as foreign ministries. This study placed virtual embassies and digital consular services at the centre of this gap.

The Vienna Conventions do not treat virtual embassies as true diplomatic missions. Such platforms work as outreach tools, lacking consent, accreditation, and physical premises. Consular law proved more flexible, since it regulates tasks rather than methods of delivery. Online visas, electronic passports, and digital registration therefore fit within existing consular functions. Servers and cloud storage outside mission buildings remain the weakest point of legal protection. Foreign data laws and cyber operations can reach diplomatic records held by private providers. Ukraine showed both the value and the risk of foreign cloud storage after 2022. Digital archives fare better, because Article 24 protects documents wherever they may be. These findings share one thread: function, not form, should guide protection in a digital age. Diplomatic law stays strong only when states read it in light of present needs. Without such a reading, the oldest rules of statecraft risk losing meaning for modern citizens.

These conclusions offer clear guidance to ministries, courts, and treaty makers. States can sign data embassy agreements, as Estonia and Monaco did with Luxembourg. They can join the electronic Apostille Programmed, which Lithuania will expand in October 2026. Regional systems such as European digital identity wallets can also support trusted consular documents. Lawyers can review cloud contracts before ministries store sensitive files abroad. Courts can read archive protection broadly when leaked diplomatic files appear in litigation. Scholars should next examine how users actually experience digital consular services. Surveys of migrants, students, and officials could reveal gaps that legal texts cannot show. Studies should also test how artificial intelligence may change visa decisions. Another open question concerns the status of embassies built inside met averse platforms. States should also discuss a protocol that names digital premises, archives, and documents. Such steps would let diplomacy move online without leaving its legal protection behind.

Bibliography

Melissen, J. (2020). Consular diplomacy's first challenge: Communicating assistance to nationals abroad. *Asia & the Pacific Policy Studies, 7*(2), 217–228. https://doi.org/10.1002/app5.298

Melissen, J., & Caesar-Gordon, M. (2016). "Digital diplomacy Abu Samra, L. A. (2023). Diplomatic agents' privileges and immunities. *Közigazgatási és Infokommunikációs Jogi PhD Tanulmányok*, 2023(1). https://doi.org/10.47272/KIKPhD.2023.1.3

Adesina, O. S. (2017). Foreign policy in an era of digital diplomacy. *Cogent Social Sciences, 3*(1), Article 1297175. https://doi.org/10.1080/23311886.2017.1297175

Aggestam, K., Bergman Rosamond, A., & Hedling, E. (2022). Feminist digital diplomacy and foreign policy change in Sweden. *Place Branding and Public Diplomacy, 18*(4), 314–324. https://doi.org/10.1057/s41254-021-00225-3

Aljohani, M., Kečo, D., Jawad, M. S., & Alzahrani, T. (2026). Blockchain-anchored AI ambassador for consular services: Architecture, adoption modelling, and evaluation. *International Journal of E-Services and Mobile Applications, 18*(1), 1–19. https://doi.org/10.4018/IJESMA.420859

Allah Rakha, N. (2024). Cybercrime and the law: Addressing the challenges of digital forensics in criminal investigations. *Mexican Law Review, 16*(2), 23–54. https://doi.org/10.22201/iij.24485306e.2024.2.18892

Allahrakha, N. (2023). Balancing cyber-security and privacy: Legal and ethical considerations in the digital age. *Legal Issues in the Digital Age, 4*(2), 78–121. https://doi.org/10.17323/2713-2749.2023.2.78.121

Al-Muftah, H., Weerakkody, V., Rana, N. P., Sivarajah, U., & Irani, Z. (2018). Factors influencing e-diplomacy implementation: Exploring causal relationships using interpretive structural modelling. *Government Information Quarterly, 35*(3), 502–514. https://doi.org/10.1016/j.giq.2018.03.002

András, A. (2023). A technológiai változások hatása a diplomáciai és konzuli jogra [The impact of technological changes on diplomatic and consular law]. *Államtudományi Szemle, 15*(2), 17–32. https://doi.org/10.58528/JAP.2023.15-2.17

Arlyapova, E., & Ponomareva, E. (2023). Virtual embassy: New technologies of representation and influence (Rethinking the American experience). *International Organisations Research Journal, 18*(3), 32–47. https://doi.org/10.17323/1996-7845-2023-03-02

Ayenew, M. Y. (2024). Relevance of digital diplomacy in promoting the national interest of states: Reflection on Ethiopian case. *Cogent Social Sciences, 10*(1), Article 2371665. https://doi.org/10.1080/23311886.2024.2371665

Bengtsson, S. (2011). Virtual nation branding: The Swedish embassy in Second Life. *Journal of Virtual Worlds Research, 4*(2). https://doi.org/10.4101/jvwr.v4i2.2111

Bjola, C., & Manor, I. (2022). The rise of hybrid diplomacy: From digital adaptation to digital adoption. *International Affairs, 98*(2), 471–491. https://doi.org/10.1093/ia/iiac005

Bjola, C., Cassidy, J. A., & Manor, I. (2019). Public diplomacy in the digital age. *The Hague Journal of Diplomacy, 14*(1–2), 83–101. https://doi.org/10.1163/1871191X-14011032

Burkadze, K. (2023). Legal aspects of digital diplomacy. *Law and World, 9*(25), 70–76. https://doi.org/10.36475/9.1.6

Cornut, J., Manor, I., & Blumenthal, C. (2022). WhatsApp with diplomatic practices in Geneva? Diplomats, digital technologies, and adaptation in practice. *International Studies Review, 24*(4), Article viac047. https://doi.org/10.1093/isr/viac047

Csatlós, E. (2018). Consular cooperation of EU member states in a fundamental rights approach. *Marmara Journal of European Studies, 26*(2), 1–23. https://doi.org/10.29228/mjes.31

Czarnecka-Gallas, M. (2026). The metaverse as a tool and domain of economic diplomacy: Governance, systemic risk and competitiveness. *Horyzonty Polityki, 17*(59), 383–406. https://doi.org/10.35765/hp.2834

Dupont, J. (2025). Consulates under diplomatic pressure? Bureaucratic resistance and relational discretion in visa issuance in China. *Political Research Exchange, 7*(1), Article 2546328. https://doi.org/10.1080/2474736X.2025.2546328

Gallo, I. C. D. (1996). Os arquivos do Quai d'Orsay (Ministério de Relações Exteriores): Correspondência política e correspondência comercial [The archives of the Quai d'Orsay (Ministry of Foreign Affairs): Political correspondence and commercial correspondence]. *História, 3*(3), 98–110. https://doi.org/10.53000/hs.v3i3.98

Hedling, E. (2026). Coping with digitalization in diplomacy: Autonomy and discretion at the digital frontlines. *European Journal of International Relations, 32*(2), 375–397. https://doi.org/10.1177/13540661251343006

Hedling, E., & Bremberg, N. (2021). Practice approaches to the digital transformations of diplomacy: Toward a new research agenda. *International Studies Review, 23*(4), 1595–1613. https://doi.org/10.1093/isr/viab027

Hill, J. (2020). Virtual Embassy Portal: The future of travel. *International Business Research, 13*(7), 199–208. https://doi.org/10.5539/ibr.v13n7p199

Jin, D. Y. (2024). The rise of digital platforms as a soft power apparatus in the New Korean Wave era. *Communication and the Public, 9*(2), 161–177. https://doi.org/10.1177/20570473241234204

Jobe, P. S. (2024). A roadmap for a Metaverse-based digital governance: A case of the Gambia. *PLOS ONE, 19*(12), Article e0314388. https://doi.org/10.1371/journal.pone.0314388

Justinek, G. (2019). Digital diplomacy in practice: A case study of the Western Balkan countries. In A. Visvizi & M. D. Lytras (Eds.), *Politics and technology in the post-truth era* (pp. 187–202). Emerald Publishing. https://doi.org/10.1108/978-1-78756-983-620191013

Kacziba, P., Gibárti, S., & Lechner, Z. (2025). Assessing Greece's transition to digital diplomacy: Insights from Twitter/X (2021–2022). *Southeast European and Black Sea Studies, 22*(1), 1–32. https://doi.org/10.1080/14683857.2025.2457813

Kaltofen, C., & Acuto, M. (2018). Rebalancing the encounter between science diplomacy and international relations theory. *Global Policy, 9*(S3), 5–14. https://doi.org/10.1111/1758-5899.12620

Manor, I. (2026). From digital diplomacy to AI-driven diplomacies? Mapping the potential impact of AI on diplomacy. *Communication and the Public.* Advance online publication. https://doi.org/10.1177/20570473261438571

" and the securing of nationals in a citizen-centric world. *Global Affairs, 2*(3), 321–330. https://doi.org/10.1080/23340460.2016.1239381

Mitev, L., & Anichienco, V. (2025). Digital diplomacy: Transforming consular services through technology. In *Universitas Europaea: Spre o societate a cunoaşterii prin europenizare şi globalizare* (pp. 555–560). Editura ULIM. https://doi.org/10.54481/uekbs2025.91

Pamment, J. (2013). *New public diplomacy in the 21st century: A comparative study of policy and practice*. Routledge. https://doi.org/10.4324/9780203121221

Pérez, F. J. P. (2026). Public diplomacy's communication management through digital platforms: The case of Spanish embassies. *Place Branding and Public Diplomacy, 22*(1), 1–15. https://doi.org/10.1057/s41254-024-00390-1

Rashica, V. (2026). The evolution of digital diplomacy: The impact of technological advancements on diplomatic practice. *Masaryk University Journal of Law and Technology, 20*(1), 33–57. https://doi.org/10.5817/MUJLT2026-40703

Robinson, N., Kask, L., & Krimmer, R. (2019). The Estonian data embassy and the applicability of the Vienna convention: An exploratory analysis. In *Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance* (pp. 391–396). ACM. https://doi.org/10.1145/3326365.3326417

Romero Vara, L. (2021). Digital diplomacy and COVID-19: An exploratory analysis of consular activities. *Comunicación y Sociedad, 2021*, Article e7960. https://doi.org/10.32870/cys.v2021.7960

Romero, L. D. (2026). Digital diplomacy: The transformative role of technology in international relations. In J. Lüdert & M. Wählisch (Eds.), *The Palgrave handbook of science diplomacy* (pp. 109–129). Springer Nature. https://doi.org/10.1007/978-3-032-29473-9_7

Sakamoto, T. (2024). How different are offline and online diplomacy? A comparative analysis. *Global Policy, 15*(2), 230–245. https://doi.org/10.1111/1758-5899.13245

Sevin, E. (2016). *Understanding digital diplomacy: The performance of foreign ministries on Twitter*. Palgrave Macmillan. https://doi.org/10.1057/978-1-137-57468-8

Wekesa, B. (2021). Introduction to the special issue: Digital diplomacy in Africa. *South African Journal of International Affairs, 28*(3), 335–339. https://doi.org/10.1080/10220461.2021.1961606

Williams, R. (2022). Communication between the United States and Iran: The virtual embassy experience. *The Thinker, 1*(1), 117–130. https://doi.org/10.25159/2767-1798/1171

Zhahira, T., & Christianti, D. F. (2023). The establishment of a virtual embassy according to the 1961 Vienna Convention on Diplomatic Relations: The case of Barbados' metaverse embassy. *Jurnal Bina Mulia Hukum, 8*(1), 106–127. https://doi.org/10.23920/jbmh.v8i1.1336

Zhou, Z. Y. (2026). Air pollution after the shutdown of US embassy monitoring. *Proceedings of the National Academy of Sciences, 123*(1), Article e2605467123. https://doi.org/10.1073/pnas.2605467123