

UDC: 342.7; 004.056
DOI: <https://doi.org/10.30546/2521-6341.2025.01.017>

PROTECTION OF PERSONAL DATA WITHIN THE UNITED NATIONS SYSTEM

Nusrat GULIYEV

*The Department of Public and Municipal Administration of Faculty of Economics and Management
of Baku Engineering University
Baku, Azerbaijan
nquliyev@beu.edu.az, 0000-0001-5007-2932*

ARTICLE INFO	ABSTRACT
Article history Received: 2025-04-21 Received in revised form:2025-05-29 Accepted:2025-06-03 Available online Keywords: Personal Data Protection, Data Protection Frameworks, Data Privacy, Cybersecurity, Global Data Governance JEL CODES: K24; K33	<i>This article analyzes the role and activities of the UN in the field of personal data protection in cyberspace. The article examines the documents, initiatives and calls adopted within the framework of the UN's statutory bodies, the General Assembly and the Economic and Social Council. The article reviews the contributions of specialized agencies such as UNESCO and ITU in the field of basic human rights in the field of information and the establishment of an ethical framework in this field, as well as technical standards. UNESCO supports the implementation of the UN General Principles on the Protection of Personal Data and implements projects aimed at increasing knowledge of data protection in the fields of education, science and culture. ITU, on the other hand, seeks to strengthen the protection of personal data by increasing the capacity of states in the field of cyber security and developing technical and legal measures. In this context, efforts to harmonize normative approaches to the protection of personal data in global cyberspace are evaluated.</i> <i>As a result of our research, we find that the existing mechanisms for the protection of personal data in the UN system are fragmented and there is a lack of institutional coordination between different structures. Although UNESCO's initiatives in the field of information ethics and ITU's technical standardization are important, their scope of application is limited and enforcement mechanisms are weak. At the same time, problems remain in the voluntary adoption and practical implementation of some normative frameworks by states. In some cases, problems such as the weakness of national legislation in states, inefficiency in the implementation of measures, lack of capacity in the field of cyber security, and weakness of mechanisms for controlling the use of personal data are noted. In addition, the limited legal mechanisms for combating data protection and the lack of independent supervisory authorities in some states create serious difficulties in the protection of personal data.</i> <i>The article also touches on future prospects in this area. Predictions are made such as strengthening national legislation, increasing capacities in the field of cyber security, strengthening cross-border cooperation models, increasing institutional coordination in the UN system, and initiating a global convention on the protection of personal data. In this context, recommendations are made for the UN to operate more systematically and normatively, and the need to form a new legal architecture for the protection of human rights in the digital era is emphasized. In this regard, it is predicted that activities aimed at the protection of personal data in the UN system will be more effective and productive in the future.</i>

I. INTRODUCTION

The acceleration of digitalization on a global scale has made the protection of personal data in cyberspace one of the main challenges of the international legal and human rights system. The development of information technologies imposes new and complex obligations on states and international organizations. In this context, the issue of forming unified and effective mechanisms for the protection of personal data within the UN system remains relevant. Although the UN's statutory bodies, the General Assembly and the Economic and Social Council, UNESCO and ITU, have put forward various initiatives in this area, their inadequacy is noticeable in terms of legal force, scope and implementation mechanisms. The study shows that there is a serious institutional fragmentation and normative inconsistency in approaches to personal data protection within the UN system. The study found that despite international measures taken in the field of personal data protection, significant obstacles and legal gaps exist. These include the insufficient level of national legislation, the weakness of control mechanisms of state authorities and companies, the lack of effective means to protect the rights of individuals, and the slow progress of the process of harmonization at the international level. Thus, in many countries, there are no mechanisms through which individuals can easily take action in cases of misuse of personal data, and legal protection processes are complex and inaccessible. While UNESCO's promotion of ethical principles on the one hand, and ITU's proposal of technical security measures on the other hand, are commendable, the synergy and legal coordination between these activities is weak. At the same time, the lack of a universal and binding legal instrument on the protection of personal data within the UN normative framework creates a serious legal gap. This gap limits the possibilities of states to exchange information and cooperate in cyberspace, and creates uncertainty in the provision of individual rights.

To solve the problem, it is necessary to develop unified and legally binding norms and mechanisms within the UN system. To solve the problem, it is important to integrate international standards and principles developed by the UN and its specialized agencies into national legislation, increase the responsibility of states and companies, inform individuals about their rights, and create effective legal protection mechanisms. To this end, improving the existing normative and institutional structure, strengthening functional cooperation between various agencies, as well as adopting a new international convention on the protection of human rights in cyberspace can be put forward as a perspective. Such measures will strengthen the protection of personal data in cyberspace and expand the prospects for international cooperation in this area. Such an approach can both strengthen the legal foundations of personal data protection at the global level and strengthen the leadership role of the UN in this area.

The object of this article is the existing institutional and normative approaches to the protection of personal data in the UN system. The subject of the study is the analysis of the activities and initiatives of the UN statutory bodies, such as the General Assembly and the Economic and Social Council, as well as specialized agencies such as UNESCO and ITU, in the field of personal data protection in cyberspace, the effectiveness of these activities, limitations and development prospects. The study examines the role of international law and cybersecurity policy in the protection of personal data in cyberspace. The study used legal document analysis, comparative legal method, institutional approach and foresight analysis methods. The aim is to assess the legal basis and practical results of efforts to protect personal data in the UN system and to identify opportunities for the formation of unified and effective approaches in this area on a

global scale. At the same time, the study also attempts to reveal the extent to which the relevant bodies of the UN system act adequately and flexibly in ensuring the inviolability of personal life against the background of the rapid development of information technologies.

II. THE UN's STATUTORY BODIES AND SPECIALIZED AGENCIES

A. THE UN's STATUTORY BODIES

1. The UN's General Assembly

The General Assembly, one of the UN's statutory organs, plays an important role in promoting human rights, including privacy and the protection of personal data, globally. The resolutions adopted by the General Assembly on the protection of personal data in cyberspace are a clear indication of the growing attention paid to this issue. These resolutions, on the one hand, call on States to strengthen national and international legal mechanisms in this area, and on the other hand, pave the way for coordinated action by other bodies of the UN system. Resolution A/RES/68/167 (2013)¹, "The right to privacy in the digital age". This resolution adopted in response to concerns about mass surveillance, this landmark resolution highlighted the importance of the right to privacy in the context of new technologies. It reaffirmed that the same rights that people have offline must be protected online, including privacy. Resolution A/RES/69/166 (2014)², "The right to privacy in the digital age". This resolution follow-up to resolution A/RES/68/167 (2013), highlighted the importance of preventing violations of the right to privacy, particularly through surveillance. It called on States to review their procedures and legislation to ensure compliance with human rights obligations, particularly with regard to the collection, storage and dissemination of data. Resolution A/RES/73/179 (2018)³, "The right to privacy in the digital age" expanded on previous ones to address new data protection issues, including artificial intelligence, big data and the use of technology by both States and corporations. It called for transparency, accountability and oversight of data collection practices, particularly with regard to personal data. These resolutions have played a critical role in shaping global debates on the protection of personal data and the right to privacy, particularly in an era of rapid technological advances.

Those resolutions were adopted in the wake of revelations about global electronic surveillance systems and is one of the first UN documents aimed at preventing unlawful interference by states with personal data. The resolutions highlighted the threats posed by mass and individual surveillance measures implemented through the Internet and other digital technologies in terms of human rights, in particular the right to privacy, and called on states to adhere to a lawful, necessary and proportionate approach in this area. The important aspect of these resolutions is that they do not only reinterpret the classical human rights framework in the digital context, but also provide states with specific behavioral models for the protection of personal data. This contributes to the formation of transparent and reliable data protection standards in international law. On the other hand, the fact that these resolutions are not legally binding raises problems with their implementation. In most cases, states are slow to implement the provisions of these documents in their domestic legislation, and sometimes introduce exceptions that weaken their essence for reasons of national security and sovereignty. In addition, the lack of mechanisms for

¹ <https://docs.un.org/en/A/RES/68/167>

² <https://docs.un.org/en/A/RES/69/166>

³ <https://docs.un.org/en/A/RES/73/179>

monitoring and accountability for the implementation of General Assembly resolutions also negatively affects their effectiveness.

However, the fact that these documents influence international public opinion, strengthen civil society, and guide the normative activities of other international organizations, including regional institutions, increases their practical importance. In the future, the General Assembly is expected to come up with more systematic and legally strengthened initiatives in this area. Thus, the fact that recent resolutions have already separately addressed the issues of artificial intelligence, big data analytics, and digital identity in the context of personal data protection is an indication of this development. Those resolutions adopted by the General Assembly are legally advisory in nature leads to the weakness of their implementation mechanisms. These resolutions are not normative legal acts and their implementation depends on the political will of the states. Also, the lack of definition of specific legal obligations in the resolutions and the lack of clear formulation of legal criteria for transparent and accountable behavior in cyberspace is criticized. On the positive side, these resolutions of the General Assembly play an encouraging role in shaping global public opinion and in bringing national legislation of states into line with international standards. These resolutions also provide a political and normative basis for other UN bodies – the Human Rights Council, the Office of the High Commissioner for Human Rights and the specialized agencies. As a result, the UN General Assembly has made a significant contribution to the formation of global legal awareness on the issue of personal data protection in the digital era. However, in order to increase the real impact of this contribution, it is necessary to support the adopted resolutions with legally enforceable mechanisms and to define specific legal obligations.

2. The UN's Economic and Social Council

The Economic and Social Council, one of the UN's statutory bodies, performs the function of coordinating economic, social and humanitarian issues on a global scale and formulating policies in these areas. The Council's activities in the field of personal data protection are mainly based on coordinating the work of related specialized agencies (e.g. UNESCO, ITU, etc.) and contributing to the definition of international policy in this area. The number of resolutions adopted by the Council directly related to the protection of personal data is limited.

However, the issue of personal data protection in the context of digital transformation, information society, sustainable development goals (SDG 16.10)⁴ and human rights has been repeatedly addressed in the advisory documents and forums of this Council, and the importance of privacy and personal data protection during the acquisition and use of data has been particularly emphasized within the framework of the High-level Political Forum on Sustainable Development (HLPF)⁵.

The strengths of the Economic and Social Council include its multisectoral and inclusive nature, its broad participation by civil society organizations, and its joint analysis of the social, economic, and legal aspects of digital issues. This allows for the integration of personal data protection with broader goals such as human rights, development, gender equality, and poverty reduction. However, the weaknesses are that the Council's decisions are not legally binding, and in some cases, the documents adopted are too general and principled. The complexity of the Council's structure and bureaucratic mechanisms mean that some initiatives have little practical impact.

⁴ <https://sdgs.un.org/goals/goal16>

⁵ <https://hlpf.un.org/>

B. THE UN's SPECIALIZED AGENCIES

1. The International Telecommunication Union (ITU)

ITU, one of the specialized agencies of the United Nations, plays an important role in the development of global information and communication technologies, as well as in the field of personal data protection and information security in cyberspace. ITU's activities in this area are mainly focused on the preparation of normative and technical documents, promotion of international cooperation and strengthening the technical potential of developing countries. The World Summits on the Information Society (WSIS), held in 2003⁶ and 2005⁷ under the leadership of ITU, were an important stage in the formation of a global agenda for the development of the information society and the protection of personal data. The documents adopted within the framework of WSIS promoted the principle of personal data protection in national and international policies.

ITU's initiatives are not limited to technical documents. The organization seeks to strengthen the cybersecurity capabilities of countries through various international forums and programs. ITU-T is the telecommunications standardization sector of the organization, a specialized organization engaged in the development of technical standards in the field of telecommunications and information and communication technologies on a global scale. This organization is engaged in the development of global standards in mobile communications, Internet protocols, network security, data exchange and other technical areas. In addition, the organization develops technical norms that ensure the interoperability of technologies from different countries and manufacturers. ITU-T develops advisory documents in the field of cyber security and personal data protection. Among the technical standards developed by ITU, documents X.1058 and X.1205 are of particular importance⁸. Document X.1058 provides recommendations for the formation of a national information security management structure and the establishment of competent authorities in this area by states. On the other hand, document X.1205 (formerly X.805) explains the cybersecurity architecture and lays out the technical foundations of personal data protection. These documents include risk-based protection of personal data and technological approaches to detecting cyber threats. However, the lack of legal binding force of these technical standards and the weakness of their integration into national legislation cause some problems. Initiatives such as the Global Cybersecurity Agenda⁹ and the Global Cybersecurity Index provide an opportunity to assess and improve the current situation of member states in terms of legislation and technical infrastructure in the field of personal data protection. In addition, ITU programs such as Child Online Protection¹⁰ include personal data protection initiatives aimed at specific risk groups.

However, there are some shortcomings in the activities of the ITU in this area. First of all, the standards adopted by the ITU are of a recommendatory nature and their mandatory application is not ensured. This makes it difficult for states to comply with these standards in practice. On the other hand, the activities of the ITU in the field of legal protection of personal data are limited, and more active cooperation and coordination are needed to develop legal mechanisms in this direction. In the future, harmonization of the ITU's technical standards with legal

⁶ <https://dig.watch/actor/world-summit-information-society>

⁷ <https://dig.watch/resource/tunis-agenda-for-the-information-society?utm>

⁸ <https://www.itu.int/rec/T-REC-X.1205-200804-I/en>; <https://www.itu.int/rec/T-REC-X.1058-201703-I/en>

⁹ <https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx>

¹⁰ https://www.itu.int/en/cop/pages/about_cop.aspx?utm

frameworks, as well as strengthening interregional information security cooperation, should be one of the important priorities. The lack of sufficient attention paid to the protection of personal data in the context of human rights in the activities of the ITU and the weakness of coordination with other UN bodies in this area are criticized. In the future, it seems necessary to more closely coordinate the technical expertise of the ITU with legal mechanisms within the framework of human rights.

2. The United Nations Educational, Scientific and Cultural Organization (UNESCO)

UNESCO is actively involved in the development of normative and ethical frameworks for the protection of personal data for the fair and inclusive development of the information society. One of the main reference documents of the organization in this area is the “UNESCO Recommendation on the Ethics of Artificial Intelligence”¹¹. This document provides recommendations on ethical principles, human rights and prevention of data misuse in the processes of collection, storage and processing of personal data. The document provides a roadmap for states and technology manufacturers to ensure that data is used without harming the privacy and autonomy of the individual.

UNESCO also takes technical and legal initiatives in the field of information ethics and regulation of cyberspace. The “Internet Universality ROAM-X Indicators”¹² framework is of great importance in this regard. Among these indicators, the “Privacy” component occupies a special place and assesses the level of legal and institutional readiness of states in the field of transparency, accountability and protection of personal data in the information space. This approach provides countries with measurable criteria for making human rights-based decisions in cyberspace policy.

In addition, UNESCO carries out educational and methodological activities on personal data protection through a number of global initiatives, including the World Summit on the Information Society (WSIS)¹³ and the Information for All Programme (IFAP)¹⁴. These platforms encourage the sharing of best practices on ethical and legal regulation of data for Member States and civil society. However, UNESCO's advisory and non-binding legal status limits the organization's influence. In the future, it seems important for UNESCO to take more active initiatives on the development of legally binding standards between technology manufacturers and states.

III. OBSTACLES AND LEGAL GAPS

A. OBSTACLES

The United Nations (UN), as a global organization, faces a number of obstacles and legal gaps in promoting effective international cooperation. Some of the obstacles are:

1 Diverging national interests. Member states often prioritize national agendas over collective goals, leading to conflicts in decision-making processes. Member states insist on priorities that suit their own economic, political, or security interests, while pushing global or collective concerns to the background. Diverging views on conflicts such as civil wars or regional tensions lead to paralysis in the UN Security Council (Docksey and Propp, 2023).

¹¹ <https://digitallibrary.un.org/record/4062376?v=pdf>

¹² https://unesdoc.unesco.org/ark:/48223/pf0000370288_eng

¹³ <https://www.unesco.org/en/wsisis>

¹⁴ <https://www.unesco.org/en/ifap/programme>

2 Inequality among Member States. Unequal distribution of power, particularly between developed and developing countries, limits fair participation in global governance. Some countries have veto power, allowing them to block resolutions even if they are supported by a majority of other members (inequality in voting power). Richer countries contribute more financially to the UN and, as a result, often have more influence over its programmes and initiatives (United Nations, 2021).

3 Geopolitical tensions. Conflicts between major powers prevent consensus on important issues such as climate change, disarmament, and human rights. The UN Security Council is often paralyzed by the vetoes of the permanent members. These countries often use their veto to block resolutions that run counter to their strategic or geopolitical interests (Security Council deadlocks). Major powers often engage in proxy wars, using smaller states as battlegrounds for their rivalries. These conflicts complicate UN peacekeeping efforts and humanitarian missions (proxy conflicts) (United Nations, 2019).

4. Resource constraints. Insufficient funding and resources for UN programmes limit their effectiveness in addressing global challenges. The UN budget is financed by Member States through assessed contributions and voluntary contributions. Late or non-payment by Member States, including major contributors, creates funding gaps that disrupt operations. This dependence makes the UN vulnerable to the priorities and conditionalities set by donor countries (over-reliance on voluntary contributions). UN peacekeeping missions are often underfunded, understaffed and under-equipped (United Nations, 2023).

5 Bureaucratic inefficiencies. Complex administrative processes can delay or hinder timely responses to global crises. Lengthy approval, procurement, and recruitment procedures slow down programme implementation and crisis response (complex administrative processes). Different UN bodies and specialized agencies often have overlapping responsibilities leading to duplication of effort and wasted resources (overlapping mandates). A lack of clear communication and cooperation between UN entities leads to fragmented and incoherent approaches to global problems (Yves Schemeil, (2021).

6. Lack of enforcement mechanisms. The UN often lacks the authority to enforce its resolutions and decisions, making implementation dependent on the willingness of Member States. Member States are not required to implement or adhere to these guidelines (non-binding nature of the guidelines). Many countries lack comprehensive data protection laws or have inconsistent regulations, making it difficult for the UN to promote a unified approach to personal data protection (fragmented national frameworks) (Solove and Hartzog, 2022).

B. LEGAL GAPS

The United Nations (UN), as a global organization, faces legal gaps in fostering effective international cooperation. Below are some legal gaps:

1. Lack of a binding framework. Unlike areas such as trade (WTO) or human rights (UN conventions), no single, universally binding international framework governs the protection of personal data. Existing frameworks, such as the EU GDPR, are regional and cannot impose obligations on non-member states (Lack of universally binding rules). Countries adopt very different data protection laws, reflecting their legal traditions, economic priorities, and cultural attitudes towards privacy (UN, 2024).

2 Inadequate cybersecurity laws. Cybersecurity laws vary widely across jurisdictions, reflecting differences in resources, priorities, and technological advances. The lack of a universal legal framework creates gaps and inconsistencies in regulation, making cooperation difficult (fragmented legal landscape). Many countries adopt cybersecurity laws in response to incidents, resulting in fragmented and incomplete coverage. Such laws often fail to take into account the global nature of cyber threats or do not provide robust protection for personal data (reactive rather than proactive measures) (UN CEB, 2018).

3. Weak regulation of non-state actors. Unlike states, non-state actors are not directly bound by international treaties unless they are explicitly integrated into national laws. The lack of global rules governing how non-state actors process personal data leads to inconsistent practices and enforcement (Lack of binding international standards for non-state actors). Many non-state actors operate across multiple jurisdictions, exploiting regulatory gaps and inconsistencies (United Nations Human Rights Office of the High Commissioner, (2021)).

4. Fragmented international law. International data protection law is heterogeneous and there is no single binding treaty setting universal standards. Existing agreements, such as the OECD Privacy Shield Guidelines or the Council of Europe Convention 108, are limited in scope and are not binding on many countries (Lack of a single global framework). Jurisdictions adopt different approaches to data protection, influenced by cultural, economic and political factors (Discrepancies in regional and national laws) (Kittichaisaree and Kuner, 2015).

5. Weaknesses in Environmental Law. Environmental governance increasingly relies on personal data, such as geolocation data, to monitor pollution, track resource use, and analyze human impacts on ecosystems. Technologies such as satellite imagery and IoT devices often collect personal data, raising privacy concerns (data-driven environmental decisions). Efforts to combat environmental crimes such as illegal logging or poaching often involve surveillance and data-sharing mechanisms that may violate privacy rights if not properly regulated (Schafer and Mazzega, 2019).

6. Protection of Human Rights. The right to privacy is enshrined in international instruments such as Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR). However, the interpretation and implementation of this right varies widely, with some countries prioritising economic or national security interests over the protection of privacy (inconsistent recognition of privacy as a human right). Although human rights treaties recognise privacy, their enforcement mechanisms are often weak or non-binding. Many states do not include robust privacy protections in their national legal frameworks, leaving gaps in the protection of personal data. (Torikul Islam, (2022)).

C. GAPS'S IMPLICATIONS. EFFORTS TOWARD SOLUTION

1. Absence of Binding Frameworks

Implications of the Gaps: Companies face regulatory fragmentation, requiring compliance with multiple, often conflicting, legal regimes. This complexity increases costs, slows innovation, and creates barriers to entry for small businesses (Barriers to Trade and Innovation). Inconsistent standards make individuals' data vulnerable in jurisdictions with weaker protections. Cross-border data transfers can expose personal data to misuse or surveillance without recourse (Weak

Protection for Individuals). Investigating cybercrime and enforcing data protection laws require cross-border cooperation.

Efforts Toward a Solution: Organizations such as the UN are advocating for a binding international data protection treaty. Such a treaty could establish minimum standards, dispute resolution mechanisms, and enforcement protocols (Proposals for a Global Framework). Regional initiatives such as the GDPR could inspire the development of global standards. Efforts to align national laws with GDPR principles, such as “adequacy decisions,” could promote greater harmonization (Developing Regional Frameworks). Multilateral bodies such as the OECD and the G20 could lead negotiations on binding agreements (Increasing the Role of Multilateral Organizations) (UN, 2024).

2. Inadequate Cyber security Laws

Implications of the Gaps: Inadequate laws make it difficult to investigate and prosecute cybercrime across borders. Mutual legal assistance treaties (MLATs) are often slow and cumbersome, failing to address the rapid nature of cyberattacks (Challenges in Cross-Border Enforcement). Differences in cybersecurity laws lead to mistrust between countries, preventing data-sharing agreements that are critical to cooperation. Concerns about inadequate protections in some jurisdictions exacerbate the problem (Barriers to Data Sharing). Weak cybersecurity structures in one country can expose data across the globe, especially in interconnected systems (Increased Vulnerability of Personal Data) (UN CEB, 2018).

Efforts Toward a Solution: The UN has repeatedly called for a unified approach to cybersecurity, recognizing its critical role in protecting personal data. Initiatives such as the UN Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security aim to build consensus on global norms (Promoting a Global Cybersecurity Framework). The UN assists Member States in developing and implementing cybersecurity laws through programmes such as the UNODC Global Programme on Cybercrime. These efforts aim to address capacity gaps and ensure that all countries can participate in international cooperation (Capacity-Building for Developing Countries)

3. Weak Regulation of Non-State Actors

Implications of the Gaps: The UN has highlighted the importance of holding non-state actors accountable for their role in data protection through initiatives such as the UN Guiding Principles on Business and Human Rights. These principles set out the responsibilities of businesses to respect human rights, including privacy, in all their operations (Promoting accountability through global norms). UN platforms such as the Internet Governance Forum (IGF) provide an opportunity for governments, private sector actors and civil society to discuss and agree on data protection norms.

Efforts Toward a Solution: Weak regulation of non-state actors in some jurisdictions creates mistrust between countries, preventing data-sharing agreements and other cooperative measures. States may impose data localization laws to protect their citizens’ data, further complicating international cooperation (undermining trust between states). Cybercriminal groups and rogue non-state actors exploit weak regulatory environments to commit data breaches, fraud, and identity theft. The lack of international consensus on how to combat such threats exacerbates vulnerabilities. (United Nations Human Rights Office of the High Commissioner, (2021).

4. Fragmented International Law

Implications of the Gaps: Businesses and governments face significant legal and logistical challenges when transferring data across borders. The lack of harmonized rules increases compliance costs, legal uncertainty, and the risk of enforcement action (Challenges to Cross-Border Data Flows). Disparate laws hinder international cooperation in investigating and prosecuting cybercrime related to personal data breaches. Inconsistent standards for sharing evidence and access to data delay responses to global threats (Barriers to Effective Law Enforcement). Inconsistent rules create gaps in the protection of individuals, particularly in jurisdictions with weak laws. (Weakened Individual Protection).

Efforts Toward a Solution: The UN has long emphasized the need for common global approaches to address transnational challenges, including data protection. Through initiatives such as the UN Conference on Trade and Development (UNCTAD), the UN encourages dialogue to harmonize national and regional data protection laws (Advancing Harmonization). The UN assists Member States, particularly in the Global South, in developing robust legal frameworks to protect personal data (Kittichaisaree and Kuner, 2015).

5. Environmental Law Deficiencies

Implications of the Gaps: The lack of clear legal protection for personal data in environmental initiatives can undermine trust between states, hindering cooperation in achieving common environmental goals. Countries may be reluctant to share data due to concerns about its misuse or inadequate protection (international trust deficit). Individuals' personal data collected for environmental purposes may be disclosed or misused, undermining trust in global environmental efforts. Diverging legal standards for data protection and environmental governance make it difficult to coordinate international efforts.

Efforts Toward a Solution: The UN can promote the inclusion of data protection provisions in environmental treaties and agreements, ensuring that personal data is protected in environmental management activities. Initiatives such as the UN Environment Programme (UNEP) can incorporate data privacy into their digital environmental strategies (integrating data protection into environmental frameworks). The UN helps countries develop comprehensive legal frameworks that address both environmental and data protection concerns, with a particular focus on developing countries to enhance their regulatory capacity (capacity building and technical assistance). (Schafer, B., & Mazzega P. (2019).

6. Human Rights Protections

Implications of the Gaps: Weak or inconsistent human rights protections undermine trust between states, making it difficult to enter into data-sharing agreements or cooperate on cross-border enforcement. Concerns about the misuse of shared data by states with poor privacy records hinder cooperation (Erosion of trust between countries). Inadequate human rights protections leave individuals vulnerable to data misuse, particularly in jurisdictions with weak legal frameworks.

Efforts Toward a Solution: The UN Human Rights Council (UNHRC) has highlighted the importance of privacy in the digital age through resolutions such as Resolution 68/167 on the right to privacy in the digital age. The Office of the High Commissioner for Human Rights (OHCHR) monitors and reports on state practices that impact the right to privacy (Promoting

privacy as a human right). The UN Special Rapporteur on the right to privacy investigates and reports on violations, advocating for stronger legal protection. These efforts aim to ensure that states comply with their human rights obligations, particularly in the digital context. (*Toriquul Islam, (2022).*

IV. CONCLUSION

1. The lack of a binding international framework for the protection of personal data creates a critical gap in promoting effective global cooperation. Addressing this challenge requires a concerted effort to establish legally binding rules that balance privacy, innovation, and sovereignty. A global compact, inspired by successful regional models and agreed in multilateral fora, could provide a comprehensive solution to this pressing issue.

2. Weak regulation of non-state actors is a significant legal gap in international cooperation on personal data protection. Addressing this challenge requires coordinated global action to establish binding frameworks, enforce standards, and promote cooperation between governments, private entities, and multilateral organizations. UN leadership is critical to building an inclusive and effective regulatory regime that ensures accountability and protects privacy globally.

3. Inadequate cyber security laws pose a significant obstacle to effective international cooperation on personal data protection. Addressing this legal gap requires a coordinated global effort to harmonize laws, strengthen enforcement mechanisms, and build capacity in resource-constrained countries. UN leadership is critical to helping create a universal, binding framework that ensures the protection of personal data in an increasingly interconnected world.

4. Fragmented international law is a critical obstacle to effective international cooperation on personal data protection. Addressing this challenge requires a unified approach, with the UN playing a central role in promoting harmonization, capacity building, and developing a binding global framework. A cohesive international legal system is essential to protect personal data, enable cross-border cooperation, and ensure that individuals' rights are protected in the digital age.

5. Deficiencies in environmental law create a legal gap that indirectly impacts international cooperation on personal data protection. As the use of personal data in environmental governance increases, integrating robust data protection standards into environmental agreements and policies becomes essential. UN leadership is critical to addressing this gap by promoting harmonized frameworks, facilitating dialogue, and supporting capacity-building efforts to ensure that both environmental objectives and privacy rights are protected globally.

6. Human rights protection is the cornerstone of effective international cooperation on personal data protection. The legal gap in recognizing and ensuring privacy as a fundamental human right weakens global efforts to protect personal data. UN leadership is essential to promote harmonization, strengthen accountability mechanisms, and advance privacy as a universal right. Bridging this gap will not only protect individuals, but also strengthen trust and cooperation among countries in the digital age. Inadequate integration of human rights protection into the legal framework for personal data protection represents a significant legal gap that hinders international cooperation.

REFERENCES

1. Schafer, B., & Mazzega P. (2019). Big Data Enters Environmental Law. *Transnational Environmental Law*, Volume 8, Issue 3, November 2019, pp.523-545. <https://www.cambridge.org/core/journals/transnational-environmental-law/article/abs/big-data-enters-environmental-law/929EEC51BB95947EF6A62538E21EBA6F>
2. Docksey, C., & Propp, K. (2023). Government Access to Personal Data and Transnational Interoperability: An Accountability Perspective. *Scandinavian University Press*, Volume 10, Issue 1, November 2023, pp.1-34. <https://www.studocu.com/row/document/university-of-nairobi/information-communication-technology/docksey-propp-2023-government-access-to-personal-data-and-transnational-interoperability-an-accountability-perspective/115253556>
3. Solove, D.J., & Hartzog, W. (2022). Narrowing Data Protection's Enforcement Gap. 74 *Maine Law Revue*, Issue 1 (2022). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3806880#
4. Kittichaisaree, K. & Kuner, C. (2015). **The Growing Importance of Data Protection in Public International Law. Blog of the European Journal of International Law.** <https://www.ejiltalk.org/the-growing-importance-of-data-protection-in-public-international-law/>
5. Union Nation System Chief Executives Board for Coordination, (2018). Principles on Personal Data Protection and Privacy, *United Nations CEB*. <https://unsceb.org/principles-personal-data-protection-and-privacy-listing>
6. Union Nation, (2024). Legal Safeguards for Personal Data Protection and Privacy in the Digital Age, *January 2024*. https://digitallibrary.un.org/record/4037316?utm_source=chatgpt.com&v=pdf
7. United Nations, (2021). Compendium of Data Protection and Privacy Policies, *United Nations Statistics Division*, November 2021. https://unstats.un.org/legal-identity-agenda/documents/Paper/data_protecton_%20and_privacy.pdf
8. United Nations, (2019). The New Geopolitics of Converging Risks: The UN and Prevention in the Era of AI, *United Nations University Centre for Policy Research*, 1 May 2019. <https://unu.edu/cpr/project/new-geopolitics-converging-risks-un-and-prevention-era-ai>
9. United Nations, (2023). UN Handbook on Privacy-Preserving Computation Techniques. <https://arxiv.org/abs/2301.06167>
10. **United Nations Human Rights Office of the High Commissioner, (2021). Thematic Report “Right to Privacy - Note by the Secretary-General”.** <https://www.ohchr.org/en/documents/thematic-reports/a76220-right-privacy-note-secretary-general>
11. *Torikul Islam*, (2022). A Brief Introduction to the Right to Privacy: An International Legal Perspective. New York University, 19 July, 2022. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4154695
12. Yves Schemeil, (2021). International Bureaucracy and the United Nations System: Introduction. *International Review of Administrative Sciences*, Volume 87 Issue 4, December 2021. <https://journals.sagepub.com/toc/rasb/87/4>
<https://docs.un.org/en/A/RES/68/167>
<https://docs.un.org/en/A/RES/69/166>
<https://docs.un.org/en/A/RES/73/179>
<https://sdgs.un.org/goals/goal16>
<https://hlpf.un.org/>
<https://dig.watch/actor/world-summit-information-society>
<https://dig.watch/resource/tunis-agenda-for-the-information-society?utm>
<https://www.itu.int/rec/T-REC-X.1205-200804-I/en>; <https://www.itu.int/rec/T-REC-X.1058-201703-I/en>
<https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx>
https://www.itu.int/en/cop/pages/about_cop.aspx?utm
<https://digitallibrary.un.org/record/4062376?v=pdf>
https://unesdoc.unesco.org/ark:/48223/pf0000370288_eng
<https://www.unesco.org/en/wsis>
<https://www.unesco.org/en/ifap/programme>