State-Sponsored Digital Surveillance and Privacy Threats through Covert Software: A Visible Challenge to Privacy

Submitted: 17 August 2025
Reviewed: 7 January 2026
Revised: 19 January 2026
Accepted: 1 February 2026

Showkat Ahmad Wani*
https://orcid.org/0009-0009-0240-9073
Sheikh Inam Ul Mansoor**
https://orcid.org/0000-0001-8636-4769
Renuka Jaggi***

Article submitted to peer blind review

DOI: https://doi.org/10.26512/lstr.v18i2.59311

Abstract

[Purpose] This study investigates the global proliferation of privacy-infringing commercial surveillance technologies, such as Pegasus spyware, and examines the resulting concerns over state-sponsored privacy violations, abuse of telecommunications infrastructure, and breaches of international legal norms. It aims to clarify the legal responsibilities of states for facilitating or using spyware and to highlight the gaps in existing international law governing cross-border digital surveillance.

[Methodology/Approach/Design] Using a doctrinal qualitative methodology, the paper analyses treaties, customary international law, UN Human Rights Committee interpretations, state practices, jurisprudence, and scholarly commentary. It focuses on issues of state responsibility, digital sovereignty, attribution, due diligence, and extraterritorial liability in the context of cyber surveillance and spyware deployment.

[Findings] The research demonstrates that international law remains ambiguous and weak in regulating spyware markets and determining state liability. It highlights the failure of mechanisms such as the Wassenaar Arrangement and export control regimes to prevent misuse by both authoritarian and democratic states. National-level legal accountability remains inconsistent, with significant implications for judicial independence, rule of law, and privacy protection.

[Practical Implications] The paper underscores the urgent need for a robust multilateral framework to regulate state surveillance practices, ensure accountability within the spyware industry, and strengthen international enforcement tools to uphold privacy and human rights in the digital age.

*Associate Professor of Law, Alliance University, Bangalore, India. E-mail: showkat.wani@alliance.edu.in.
**Assistant Professor of Law, Symbiosis Law School, Hyderabad Campus, Symbiosis International (Deemed University), Pune, India. E-mail: sheikh.mansoor@slsh.edu.in.
***Senior Research Fellow, Himachal Pradesh National Law University (HPNLU) Shimla, India. E-mail: 215rjaggirenuka@gmail.com.

[Originality/Value] This study offers a comprehensive analysis of state responsibility for spyware-facilitated surveillance, bridging doctrinal legal research with contemporary concerns about digital sovereignty and privacy rights. By critically examining the misuse of Pegasus spyware and existing regulatory gaps, it contributes to policy discourse, comparative legal scholarship, and the development of actionable international norms.

Keywords: Spyware. State. Surveillance. Rule of Law. Accountability.

INTRODUCTION

Digital surveillance technologies have posed new challenges for the legal regimes that regulate privacy, telecommunications, and the responsibility of states under international law. Among these technologies, the most well-known and controversial one is the Pegasus spyware, which has been developed by the Israeli firm NSO Group. It was designed to circumvent security features and gain access to data on mobile phones, Pegasus has allegedly been used by governments to spy on political opponents, journalists, activists, and even presidents, raising serious questions about the legality, legitimacy, and control of such cyber-intrusion (Marczak et al., 2018; Amnesty International, 2021). C1

This is a serious threat to privacy rights and huge spyware scandal; it is a reflection on the emergence of an international surveillance apparatus whereby public actors collaborate with private actors to conduct extraterritorial, black-boxed, and partially unaccountable digital surveillance. An independent investigation project launched in 2021, the Pegasus Project, revealed a list of more than 50,000 potential surveillance victims, including more than 1,000 individuals from more than 50 countries (Kirchgaessner et al., 2021). These revelations place states not just as consumers of spyware but as customers in an international marketplace for intrusive technology thereby raising pressing questions regarding state responsibility under international law.

The issue is particularly complex in the Global South, where fragile rule-of-law institutions and few mechanisms for transparency optimise the danger of abusive surveillance (Sirohi, 2021). The use of Pegasus in India, Mexico, Rwanda, Saudi Arabia, and the United Arab Emirates is the quintessential example of how spyware would be used as a weapon against civil society in the guise of national security (George P. G., 2021). Meanwhile, European democracies like Poland and Hungary have not been accused of employing Pegasus for political purposes, and this underlines the attractiveness of spyware to regimes of all sorts and legal regimes (Marczak et al., 2021; Dumbrava, C., 2023).

Despite its global scope, the regulatory framework for spyware is appallingly weak. The absence of a multilateral convention that regulates cybersurveillance and the inadequacy of existing frameworks such as the International Covenant on Civil and Political Rights (ICCPR), the Wassenaar Arrangement, and export control measures to address the unique threat posed by spyware has created a legal vacuum (Riecke L., 2023). As a result, there are essential legal questions that needs an answer and solution; Is the use of spyware a breach of international human rights law? Do States become internationally responsible for the actions of private surveillance companies? What legal remedies are available to victims of snooping/spying?

This paper does a doctrinal qualitative analysis of the global Pegasus spyware scandal from the viewpoint of international law. The article critically evaluates the responsibilities of deploying and exporting states to maintain obligations related to privacy, telecommunications integrity, and prohibition of arbitrary surveillance. The study integrates concepts drawn from international human rights law instruments, theory of state responsibility, export control law, and cyber sovereignty law (Alubaidi A., 2023). The intrusion on civil liberties risks is very high due to lack of legally binding norms, spyware tools like Pegasus risk institutionalising mass surveillance and further eroding fundamental human rights such as dignity, autonomy, and freedom of expression (Coco, A. et al., 2021). This study aims to advance the early-stage debate on digital sovereignty and responsibility by conducting a rigorous legal scrutiny of the international surveillance framework and the obligations of states thereunder.

PEGASUS AND THE GLOBAL SPYWARE MARKET

The growing off-the-shelf availability of commercial surveillance technology has dramatically transformed the landscape of intelligence gathering and law enforcement. The most publicised and controversial of these tools is likely to be Pegasus spyware, developed by the Israeli cyber-intelligence firm NSO Group. Unlike traditional surveillance techniques based on physical proximity or cable tapping of telecommunication, Pegasus operates by utilizing zero-click exploits, allowing remote, undetectable access to mobile phones without user interaction (Marczak et al., 2021). Upon being installed, the spyware offers complete access to calls, messages, images, emails, and even encrypted communication programs such as Signal and WhatsApp, basically turning an individual device into a tool of live monitoring.

Pegasus has been considered as a counterterrorist and criminal investigation tool, but several investigations reveal its mass abuse targeting journalists, political activists, human rights defenders, academics, and judges (Amnesty International, 2021; Marczak et al., 2021). The Pegasus Project, a

global collaborative inquiry by Forbidden Stories with Amnesty International and over 80 journalists across the world, uncovered over 50,000 phone numbers as reportedly targeted for surveillance in over 50 nations (Lewis, P., 2021). The findings have made Pegasus shift from being a technological advancement to a 21st century indicator of digital authoritarianism.

The Technical Functionality and Capabilities of Pegasus

Pegasus makes use of sophisticated strategies of penetration which exploit vulnerabilities in popular mobile operating systems i.e., IOS and Android. The spyware requires no physical or user action to be installed, this is a zero-click attack trajectory, where the software can be installed through a missed call or an unsolicited push notification (NSO Group, 2021). Once it has penetrated into a device, Pegasus works silent real-time access to audio, camera, GPS location, and all stored data. It can also self-destruct or erase its traces, and this complicates forensic identification (Marczak et al., 2021).

NSO Group claims that it exports Pegasus to vetted government agencies solely for counterterrorism and crime investigations, and not to autocratic governments or commercial companies (NSO Group, 2021). However, the secret nature of these exports, combined with limited export controls or end-user responsibility, has facilitated misuse on a global scale (Deibert J.R., 2020).

Transnational Use and Abuses

The evidence also shows that Pegasus has been used in more than 45 countries, both democratic and nondemocratic, around the world. In Mexico, anti-corruption activists and journalists were targeted with the spyware rather than drug cartels (Ahmed A., 2017). In the UAE and Saudi Arabia, it is suspected to have been used against dissidents and women's rights activists. The software is also suspected of being used in the surveillance of Jamal Khashoggi's associates before and after his murder in the Saudi consulate in Istanbul (Amnesty International, 2021).

In Europe, Hungary was the first EU member state that had been found to have employed Pegasus against journalists and opposition politicians (Dumbrava C., 2023). The same applies to the Polish government, which has been accused of employing Pegasus in the 2019 election against its members of the opposition (Telford T., 2021; Walker S., 2024). The above instances make questionable the assertion that Pegasus is used solely for the purposes of combating terrorism or organized crime and bring to light its strategic application for political and electoral purposes.

Pegasus and the Private-Public Surveillance Nexus

The NSO Group lives in the gray zone between public interest and profit. Although it claims to obey Israel's Ministry of Defense export controls stringent regulations, with no multilateral supervision, NSO can virtually act like a sovereign when it comes to determining who its technology arrives at (Riecke, L., 2023). This is an international law issue since it turns the long-established principle on its head which presented surveillance operations as being the exclusive preserve of the state.

In addition, state contracting out of intelligence collection to non-state actors poses grave accountability issues. According to the International Law Commission's Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA), states can be held accountable if private actors are acting under their direction, control or instruction (International Law Commission, 2001). In the case of Pegasus, different governments have refused to confirm or deny their contractual relationship with NSO, thereby allowing them to deflect legal scrutiny and public scrutiny.

The Global Pegasus Market and the Surveillance Industrial Complex

The Pegasus spyware market is one illustration of the proliferation of a "surveillance industrial complex", the trend where states and corporations partner together in the large-scale manufacture and spread of intrusive digital technology. The loosely monitored market is also served by other corporations such as Candiru, FinFisher, and Hacking Team, selling spyware to democratic governments as well as to authoritarian governments (Jaffe A., 2023). What distinguishes Pegasus is its unparalleled technical sophistication and worldwide extent of application (De Gregorio G., 2022).

Without internationally enforceable treaties or norms on regulating the spyware market, export controls like the Wassenaar Arrangement are toothless. Although Wassenaar has dual-use technologies like intrusion software under its ambit, it does not bind non-signatory states or private parties and is unenforceable (Riecke L., 2023). Pegasus thus finds itself in a legal void where neither producer states nor end-user states are held accountable for its use or impact.

Consequences for Digital Rights and Rule of Law

The use of Pegasus has severely undermined digital rights, primarily the right to privacy, freedom of expression, and protection of journalistic sources (Penney J., 2017). Chilling effect of internet surveillance is no fiction; once people sense they are being watched, they alter their behavior, self-censor, and back away from dissent (Tufekci, 2015). Where Pegasus has been used to target applications

in elections or political uprisings, the spyware has been linked to electoral manipulation, harassment by law, and empowering opposition parties.

Such comprehensive deployment of spyware represents a dangerous slide towards digital authoritarianism even in ostensibly democratic administrations. It erodes judicial independence, undermines the watchdog roles of civil society, and dissolves public trust in democratic institutions (De Gregorio G., 2022). Any viable legal assessment, therefore, must account not just for the technical details of spyware, but for the political and normative implications of its application.

Telecommunication and Privacy in International Law

With the onset of the digital age, the right of privacy specifically in relation to telecommunication surveillance has become quite likely the most contentious field in international law. The right of privacy was once accepted traditionally in the post–World War II, international legal order as a foundation for human rights. Nowadays, privacy is threatened by advanced technologies that provide silent, real-time, and mass-scale intrusion (Humble K. P., 2021). Pegasus spyware that breaks encryption and gets access to confidential messages assaults the inviolability of this right directly and invokes the obligations of states under international human rights law. This analysis considers how international law conceptualizes the right of privacy, how telecommunication is protected from arbitrary interference, and how these norms are enforced against the threat of contemporary surveillance (Alexander A., et al., 2022).

Right of Privacy under International Human Rights Law

The right to privacy is enshrined in several binding international human rights treaties. Article 17 of the International Covenant on Civil and Political Rights (ICCPR) provides that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence," and that "everyone has the right to the protection of the law against such interference or attacks" (United Nations, 1966). Similarly, Article 12 of the Universal Declaration of Human Rights recognizes the individual's right to privacy against arbitrary intrusion (United Nations, 1948).

The Human Rights Committee, the ICCPR's interpreting treaty body, specified in General Comment No. 16 (1988) that "correspondence should be delivered to the addressee without interception and without being opened or otherwise read." It emphasized that states must enact legislative and institutional protection against both public and private sector interception (Human Rights Committee, 1988). More recently, in General Comment No. 34 (2011), reaffirmed that freedom of expression also entails protection against unlawful surveillance

and hacking, especially targeting journalists and human rights defenders (Human Rights Committee, 2011).

Pegasus violates these standards in direct ways. It's quiet, systematic form of surveillance crosses the norms of lawfulness, necessity, and proportionality, which international human rights law dictates for any limitation on privacy (Kuner C., 2021). Furthermore, the unaccountable and secretive application of spyware cannot be said to meet the criterion of "provided by law," since the application and delivery of the software lie beyond the realm of open legal process or independent monitoring (Milanović, M., 2022).

Telecommunications as a Site of Legal Protection

While privacy assurances in general in telecommunications are increasingly becoming ingrained as a distinct entity due to the commonality of digital communication in modern life. In its resolution 68/167 (2013), the United Nations General Assembly reaffirmed that "unlawful or arbitrary surveillance and/or interception of communications constitute a highly intrusive act and violate the right to privacy" (United Nations General Assembly, 2014).

This was echoed by the UN Special Rapporteur on the Right to Privacy, who commented in his 2021 report that contemporary spyware like Pegasus not only intrudes on privacy but "undermines the infrastructure of democratic societies" by targeting journalists, legislators, and civil society actors (UNHRC, 2021). Given that modern communication is becoming more practiced over encrypted messaging platforms, the right to use anonymous and encrypted technologies is now seen as part of the freedom of expression and right to privacy (UNHRC, 2018). It is important to understand that telecommunications privacy protections have two obligations; one is called Negative obligations in which States are obligated not to participate in illegal intrusions. Whereas the Positive obligations emphasis that there is a responsibility for states to protect individuals against third-party monitoring, including from private entities like NSO Group. The failure of states to prohibit, regulate, or even disclose their use of Pegasus defies such double obligations. In the majority of reports published, there was no enabling legislation, no judicial warrant obtained, and no remedy to the target (Bhandari V., et al., 2020).

Regional Human Rights Courts and Surveillance Jurisprudence

Regional courts plays a crucial role in delineating the law regarding digital surveillance. In the landmark case of Roman Zakharov v. Russia (2015), the European Court of Human Rights (ECtHR) ruled that general and secret surveillance techniques, particularly those that fall outside judicial review's umbrella, violate Article 8 of the European Convention on Human Rights (right

to private life). The Court highlighted the point that even threat of surveillance constitutes a violation of privacy in the absence of protection measures (European Court of Human Rights, 2015).

In Szabó and Vissy v. Hungary (2016), the ECtHR denounced surveillance law allowing state powers of uncontrolled interception without sufficient legal definition or independent monitoring. This ruling is especially relevant considering that Hungary was subsequently a known user of Pegasus (European Court of Human Rights, 2016).

The Inter-American Court of Human Rights, in its Escher et al. v. Brazil (2009) judgment, held that surveillance should be in conformity with legality, legitimate purpose, necessity, and proportionality. The Court emphasised the state's obligation to investigate and disclose unauthorized surveillance, especially when fundamental rights such as political participation and freedom of association are concerned. These developments provide a uniform set of standards by the judiciary. It is a clear signal that legislative requirement is imperative, independent oversight and adequate remedies to protect civil liberties particularly privacy rights of human beings. Pegasus deployment in secret, often without warrant or judicial supervision, violates all these conditions and places using states in violation of their regional human rights responsibilities (Inter-American Court of Human Rights, 2009).

Telecommunication Integrity under International Telecommunication Law

Besides human rights law; international telecommunication regimes also have a further layer of legal regulation. According to Article 40 of the ITU Constitution, the International Telecommunication Union (ITU), a UN specialized agency, mandates the "protection of telecommunications against harmful interference" (International Telecommunication Union, 1992). Although not directly focused on spyware, the ITU regime encourages states to join forces in blocking technology misuse and secure communication facilities. The Budapest Convention on Cybercrime in 2001, which is in the main focused on criminal cooperation, exhorts states to transpose interception into law that is illegal. Its reach does not extend, however, to state surveillance, and this has led to the call for a more powerful tool addressing cyber espionage and spyware specifically (Gascón M. A., 2024).

The Challenges of Enforcement and Extraterritorial Application

There is an inherent flaw in the application of international law to Pegasus surveillance due to extraterritorial deployment. The modern treaties and conventions, most notably the ICCPR require some threshold of jurisdiction for obligations to come into play. The Human Rights Committee has affirmed in

General Comment No. 36 that states must respect rights "where they exercise effective control," including through cyber technologies (Human Rights Committee, 2019). Milanovic and others support a functional definition of jurisdiction that recognises the cross-border nature of surveillance and propose it especially where spyware is applied remotely by a state to reach targets in another. Without such an interpretative modification, international human rights law may remain inadequately oblique towards regulating digital watchdog across borders/jurisdictions (Milanović, M., 2011).

Attribution of Responsibility Under International Law

The international law paradigm of attributing wrongful act to states is the central doctrine of state responsibility. The paradigm fits where the wrongful act is perpetrated by non-state actors or private individuals with implicit or express backing from the state. Use and deployment of the Pegasus spyware, which is a military-grade surveillance software constructed by a private entity, poses difficult questions in attribution under international legal norms. This part analyses how states can be held legally responsible in case the use of such spyware either directly by state agents or indirectly by non-state actors under state control or direction. Attribution is presently governed by the International Law Commission's Draft Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA), adopted by the United Nations General Assembly in 2001, which establishes principles of attribution, breach, and reparation (International Law Commission, 2001).

Article 4 of ARSIWA provides that an act performed by any organ of a state, legislative, executive, judicial, or administrative, is an act of that state if the organ is acting in the exercise of that power (Brown C., 2024). The case is particularly relevant when a government intelligence agency like India's Research and Analysis Wing (RAW) or Israel's Shin Bet explicitly uses spyware like Pegasus. The fact needs to be understood that a state organ's action is attributed to the state itself (International Law Commission, 2001). Amnesty International and The Guardian, for example, have all named different state organs in a variety of states from Morocco to Hungary to India and Saudi Arabia as direct beneficiaries or users of Pegasus spyware (Amnesty International, 2021; Kirchgaessner et al., 2021).

The more complex scenario arises under Article 8 of ARSIWA, addressing conduct by private actors "acting on the instructions of, or under the direction or control of, the state." This article is particularly pertinent to considering instances where the NSO Group, a private Israeli company, supplies Pegasus to government agencies (Brown C., 2024). The "effective control test", which has been set by the International Court of Justice (ICJ) in Nicaragua v. United States, mandates that

the state must have directed or enforced specific operations of wrongful conduct (International Court of Justice, 1986). The same test was applied in Bosnian Genocide (2007), in which the ICJ refused to attribute the acts of the Bosnian Serbs to Serbia for absence of specific operational control. In Pegasus cases, unless the spyware is employed under transparent government control with evidence of state coordination, attribution may struggle under this low standard.

However, the "effective control doctrine" has been criticised as dogmatic and unrealistic in cyber operations. The experts have actually encouraged the "overall control test", as formulated by the International Criminal Tribunal for the former Yugoslavia (ICTY) in Tadić, that exacts a lower threshold of control i.e., whether the state possesses the ability to co-ordinate or assists the overall military or intelligence activities of non-state forces (International Criminal Tribunal for the former Yugoslavia, 1997). If adhered to, this test would broaden attribution in the Pegasus model, particularly where it is evident that state officials have commissioned, funded, or encouraged NSO Group to facilitate specific spyware activities.

Complicating this further is Article 11 of ARSIWA, which addresses instances where the state acknowledges and claims private activity as its own (International Law Commission, 2001). This particularly comes into play in the case of states when, accused of employing Pegasus for cyber spying, they fail to refute it or back the practice through public declarations or in-court hearings. For instance, in India, no affidavit was submitted by the government of denial or exoneration of the use of Pegasus in the proceedings of the Supreme Court and thereby left room for legal speculation about veiled acknowledgment (Bapat K., 2021).

Another path of attribution is through the escalation of speech regarding due diligence failure as an implied state conduct. Though due diligence is generally viewed as a secondary obligation, if states are not preventing private spyware abuse within their control or jurisdiction from occurring, such failures could conceivably be defined as wrongful acts per se (Milanović M., 2015). For instance, Israel's Ministry of Defense export licensing system permits the export of Pegasus but not in a transparent and post-export accountable manner, thereby implicating the state in potential misuse of its sanctioned technologies (Deibert J.R., 2020).

Besides, as per Tallinn Manual 2.0, which embodies evolving norms of cyber operations, a state can be held responsible for failure to prevent its territory from being utilised to conduct wrongful cyber operations if it possesses actual or constructive knowledge of the activities (Schmitt M. N., 2017). If Israel, as the country of licensing, continues to issue licenses for Pegasus exports to tyrannical

governments or where there have been historical abuses, it may be held liable not for use, but for enabling the actions by inaction.

The global proliferation of the Pegasus spyware also raises implications of indirect or derivative responsibility in co-operations through collective operations or inter-state cooperation. As per Article 16 of ARSIWA, a state which aids or assists another state to commit an internationally wrongful act is also internationally responsible if it is aware of the circumstances of the wrongful act and if the act would be wrongful if it were to be committed by it (International Law Commission, 2001). This provision might be invoked where a government actively facilitates another state's unlawful surveillance for example, by supplying decryption keys, hosting command-and-control servers, or subsidising the production of spyware and thereby becomes hostile.

The global extent of Pegasus deployment erases territorial boundaries, and jurisdictional and applicable law issues are raised. International law still falls behind the facts of digital surveillance and its penetrable implications. Courts and treaty bodies are not entirely unanimous in recognising the extraterritorial character of privacy rights, but growing jurisprudence, such as that of the European Court of Human Rights (ECtHR) in Big Brother Watch v. United Kingdom (2021), suggests that bulk surveillance of foreign nationals can be seen to engage European Convention on Human Rights obligations (Zalnieriute M., 2022).

International law responsibility in Pegasus cases requires subtle application of both established doctrines and evolving cyber principles. The ARSIWA framework provides a firm basis, but its practical constraints notably in the assignment of private corporate activity necessitate supplementary instruments and interpretative ingenuity. In a state-private partnership-led digital surveillance economy, global legal frameworks must evolve to ensure accountability becomes inevitable, hinder impunity, and uphold the inherent human rights of the targeted individuals through advanced spyware tools.

Due Diligence and Export Control Failure Obligations

For a very long time, states have been obligated under international law to make sure that activities within their jurisdiction do not harm other states or violate the human rights of individuals outside their jurisdiction. This obligation of due diligence, while having its origins in environmental law and transboundary harm doctrines historically, has been reaffirmed and extended to the cyber space by international courts, treaty organs, and commentators (Schmitt M.N., 2017). In the scenario of spyware such as Pegasus, there is a duty of diligence under which a state that knowingly allows a foreign state or a private company to employ intrusive surveillance software that has been exported from its state, or does not

regulate its exportation, can be held internationally accountable for ensuing privacy, data protection, and human rights infringements.

The International Law Commission's Draft Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA) clearly articulates that a state is not only responsible for positive action but also for inaction i.e., where it fails in the exercise of due diligence to prevent third-party abuse. Article 2 of the ARSIWA lays down wrongful acts to encompass action which is attributable to a state and constitutes a violation of an international obligation (International Law Commission, 2001). In Pegasus, the responsibility of the exporting state, Israel, and the deploying or buying states like India, Hungary, and Saudi Arabia is augmented by the dual-use character of spyware and its complete potential to undermine basic civil liberties (Milanović M., 2015). Pegasus's ability to steal everything from a smartphone without the need for user interaction and send it to command-and-control servers has caused intense concerns that such technology, left without constraint, transforms mere surveillance into a threat to existent democratic liberties (Deibert J.R., 2020).

In general, international law, and more particularly in sources such as the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, the rule of due diligence requires a state not to knowingly allow its territory to be used for purposes that infringe the rights of another state or of individuals covered by international human rights law (Schmitt M.N., 2017). The Israeli government's approved export process for Pegasus, handled by the Ministry of Defense, is not publicly transparent and independently audited. Though, the NSO Group claims to export Pegasus to only supervised governments for counter-terrorism and law enforcement reasons, the product has reportedly been utilised within highly repressive political settings against journalists, dissidents, and civil society (Marczak et al., 2021). Despite widespread reporting by organizations such as the United Nations and the European Parliament, there is no concrete accountability framework to measure whether Israel is fulfilling its due diligence obligations under international human rights law and export control standards (Dumbrava, C., 2023).

Also, the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, while seemingly created to regulate cross-border technology transfers, has failed to effectively regulate the proliferation of cyber spying tools. The Arrangement does encompass intrusion software, including Pegasus-type spyware, in its export control list, but its voluntary and non-binding character limits its effectiveness. Furthermore, its lack of a central enforcement agency or public reporting framework reduces any true deterrence effect (Riecke L., 2023). National security exceptions are generally

employed by states in order to bypass export controls, thereby creating a non-transparent and impunity-driven global spyware market.

Scholars noted that the legal gap results in "regulatory arbitrage," in which companies relocate activities or reroute transactions among jurisdictions with low control levels, thereby avoiding accountability. Failing to carry out effective due diligence by states that facilitate or agree in the Pegasus raises severe legal concerns for complicity and indirect responsibility under Article 16 of the ARSIWA, which deals with giving of aid or assistance to the commission of an internationally wrongful act. A government knowingly allowing surveillance activities to violate the rights enshrined in the International Covenant on Civil and Political Rights (ICCPR), including Article 17's privacy right, could be held responsible both for lack of prevention but also for assistance in human rights violations (Human Rights Committee, 1988).

Additionally, the private status of spyware manufacturers makes it harder to enforce. However, the state responsibility doctrine is not pre-empted by the fact that the perpetrator is a non-state actor. In fact, the European Court of Human Rights (ECtHR) has consistently held that states have positive obligations to protect individuals against rights abuse by private individuals, including through regulatory and preventive measures (ECtHR, 2008). Consequently, failure to institute strict licensing, ineffective export control transparency, and refusal to investigate credible claims of abuse put exporting states at risk of international legal responsibility.

At the receiving end, the sending states are also required to exercise due diligence by making sure that they use surveillance technologies in accordance with proportionality, necessity, and legality tests under international human rights law. Failing to enact judicial remedies, grant redress to the victims, or give parliamentary or independent checks may be deemed violations of not just domestic constitutional norms but also extraterritorial human rights agreements (Penney J. W., 2021). The Indian Supreme Court, in the Pegasus Case, attempted to enforce such standards by constituting a technical committee to probe allegations of illegal surveillance. But prosecutorial failure to follow up and public delay undermined the utility of such oversight (Manohar Lal Sharma v. Union of India, 2021).

The Pegasus spyware scandal reveals a blatant gap in global governance of cyber surveillance technology. States failure to fulfil their obligation of due diligence to authorise, export, or utilize such technology contradicts the intention and reason of international law. Without the legally binding instruments, accountability mechanisms, and normative comprehension of cyber surveillance, the global market for spyware will remain a place where due care is taken lightly and privacy rights are consistently being breached.

The application of Pegasus spyware beyond the country's borders to monitor individuals beyond the territorial domain of a state raised definitive issues regarding the extraterritorial application of international human rights commitments. The important question arises whether states are internationally responsible for their surveillance activities, which aim against individuals in other states because Pegasus operates without the physical presence of state agents in the targeted territory, it challenges traditional notions of jurisdiction that underpin international human rights regimes.

Article 17 of the ICCPR guarantees individuals against "arbitrary or unlawful interference" with privacy, family, home, or correspondence. The United Nations Human Rights Committee (UNHRC) has clarified, notably in General Comment No. 16 and more recently in General Comment No. 36, that the right to privacy applies to communications and surveillance in the digital sphere. Nevertheless, the issue of extraterritorial application was more thoroughly addressed in General Comment No. 31, where the Committee emphasised that the state is obliged to respect and ensure ICCPR rights to "all persons within their territory and subject to their jurisdiction" (United Nations Human Rights Committee, 2004).

Double requirement of presence on the territory and jurisdiction has been an object of legal discussion. For long-distance cyber monitoring, control over territory will probably be absent, but jurisdiction may be present where a state exercises effective control over the digital behavior influencing the rights of an individual. Where a state employs technology to interfere with private communications of foreign nationals, has noted that in cyberspace, control can thus be understood functionally (Milanović M., 2015). This has been supported yet again by the United Nations High Commissioner for Human Rights in their 2014 report, reaffirming that extraterritorial surveillance must be consistent with human rights standards (Human Rights Watch, 2014).

The Snowden revelations of 2013, and more recent news on Pegasus use, provide real examples where surveillance technology was used in an extraterritorial manner (MacAskill E. & Dance G., 2013). Its use by some governments to track journalists, activists, and foreign officials based abroad proves there is cross-border surveillance activity (Amnesty International, 2021; Deibert J.R., 2020). The Israeli NSO Group has marketed Pegasus to multiple state clients who have used it outside their borders, especially to track phones registered in other countries, activating potential extraterritorial liability (Riecke L., 2023).

International jurisprudence concerning extraterritorial extension of human rights law prefers a functional doctrine of jurisdiction. The European Court of Human Rights (ECtHR) held that the state's human rights obligations under the

European Convention on Human Rights (ECHR) may bear an extra-territorial scope of application when the state exercises effective control over individuals. Although the judgment proper concerned physical occupation (Al-Skeini v United Kingdom, 2011). Later cases, such as (*Carter v. Canada 2015)* demonstrate an emerging understanding that jurisdiction in the digital age does not necessarily require physical location.

This development is particularly relevant when one views Pegasus, where a state can invade an individual's private domain anywhere in the world by accessing digital hardware. The ECtHR in (Zakharov v. Russia 2015) also held that secret surveillance, even if there is no physical invasiveness involved, will be subject to human rights law and legal safeguards, and therefore cross-border abuses would require scrutiny accordingly (European Court of Human Rights, 2015).

Moreover, the Inter-American Court of Human Rights has established that states are obligated to respect and guarantee rights to individuals "within their authority and effective control," a rule encompassing distant conduct which far-reaches and considerably affects rights (Inter-American Court of Human Rights, 2017). It is important to note if injury is caused by spyware of a state against individuals beyond its borders, it has functional authority sufficient to initiation its human rights obligation.

The notion of "digital sovereignty" has also emerged in international law to contend that cyberspace operations, however distant, will have to be sensitive to the sovereignty and right to life of other countries and their peoples (Chatinakrob T., 2024). The invasion through spyware is hence not only a breach of privacy but could also be a breach of another country's sovereign rights, and therefore legal as well as diplomatic consequences start increasing.

Despite this, enforcement remains elusive. Victims of extraterritorial surveillance have limited avenues of remedy. Domestic courts often lack jurisdiction, while international remedies are disconnected. Although cases such as Schrems II have limited the scope of intercontinental data transfers on the basis of privacy (Court of Justice of the European Union, 2020), they do not address surveillance conducted by way of secret tooling like Pegasus. Legal accountability is further frustrated by the confidentiality of state surveillance processes, national security justifications, and the veil of incorporation shielding producers of spyware (Stahl B. C., et al., 2023).

Exporter states and users of Pegasus can therefore be violating not only the privacy of foreign nationals but also undermining the global order that governs the protection of human rights in cyberspace. Extraterritorial human rights obligations should be rethought to encompass the digital realities of transborder

surveillance, where jurisdiction arises from control of the data space and effects on rights, rather than presence.

To make someone accountable, it is essential that more specific norms are created within the United Nations and regional contexts regarding extraterritorial application of privacy rights. Efforts such as the proposed UN Cybercrime Convention and Human Rights Council debates are steps towards codification of responsibility in an interconnected digital world. The Pegasus case demonstrates the necessity for a more active comprehension of extraterritorial obligations that acknowledges and regulates the real practices of states within the surveillance economy.

Case Study – India's Pegasus Controversy and Domestic Legal Accountability

India's Pegasus spyware scandal is arguably one of the most controversial contemporary examples of alleged state-sponsored surveillance, which raises profound issues about democratic governance, civilian rights, and state institution accountability. In July 2021, a global collaborative investigative story pioneered by Forbidden Stories and Amnesty International's Security Lab revealed that several Indian citizens, including journalists, political opponents, activists, lawyers, and even constitutional authorities, were victims of the Pegasus spyware developed by Israeli firm NSO Group (Amnesty International, 2021; Project Pegasus, 2021). These findings resulted in widespread political and legal debate on the legality of surveillance operations and the role of the state to deliver transparency and accountability in democratic societies.

Despite the fact that the Indian government neither refuted nor confirmed the use of Pegasus, it evaded direct answers to questions posed by parliament and to the demand for explanations by the public (Bapat, 2021). The silence of the government regarding whether it purchased or used the spyware is a sign of insufficient openness and the lack of proper checks on the executive surveillance powers. This silence also worsened popular apprehensions regarding abuse of power, especially since most of the people targeted were not only politically dissenting against the governing government but were additionally engaged in constitutionally safeguarded activities like journalism and legal activism (Naithani P., 2021). These actions strike at the heart of India's constitutional framework, which safeguards fundamental rights to privacy, free speech, and protection from arbitrary action by the government.

The Supreme Court of India stepped in after petitions were filed by prominent citizens, including journalists and public intellectuals. In its landmark order dated October 27, 2021, the Court directed an independent expert committee to probe the allegations based on upholding the rule of law and protecting

fundamental rights (Manohar Lal Sharma v. Union of India, 2021). The judgment emphasized the sanctity of the right to privacy as defined in Justice K.S. Puttaswamy v. Union of India, and the requirement of judicial oversight in the case of potential abuse of surveillance technology (Paranjoy, 2024). Even though the last report submitted by the expert committee was made public in 2022, the lack of prosecution or official acknowledgment by the Indian government shows a deficiency in accountability.

India's existing legal framework on surveillance is mainly governed by the Indian Telegraph Act, 1885, and the Information Technology Act, 2000, which are not transparent enough, lack enough judicial review, and lack rights-based safeguards (Bhatia G., 2021). Both laws grant excessive powers of surveillance to the executive without any need for independent or parliament approval. Although India does have data protection legislation but is not sufficient to deal with alleged cases of spyware. The Digital Personal Data Protection Act, 2023, has wide exceptions for government departments which would become a path of exploitation and a further dilution of privacy protections (Kumar R., 2025).

The Pegasus case also highlights the complexity of legal liability when there are foreign companies and dark Cross border cyber operations involved. The NSO Group has claimed that it sells its spyware only to governments in order to fight terrorists and proclaimed criminals, but very little verifiable evidence exists to support these assertions (Marczak et al., 2021). The Indian case points to the absence of any effective national mechanism to screen procurement of such surveillance technology, let alone consider conformity with international human rights standards.

The failure to articulate clear legal liability and remedies in Pegasus cases is not only an internal accountability deficit but threatens to normalise executive overreach in electronic surveillance. To India, democratic institutions and the judiciary need to be at the forefront to ensure that new technology is not ahead of legal frameworks created to safeguard citizens rights.

Comparative Jurisdictional Analysis – Israel, the EU, and the U.S.

The Pegasus spyware affair has again raised issues of state surveillance, export control, and privacy legislation across jurisdictions. A comparative analysis of legal responses and regulatory frameworks in Israel, the European Union (EU), and the United States (U.S.) illustrates divergence in degrees of responsibility, control, and respect for human rights in regulating surveillance technology.

Israel: Prioritizing National Security and Export Controls

Israel, NSO Group's home nation, has had a defence-export control regime since ages under the Defense Export Control Law (2007). Export licensing of defence and dual-use cyber products, including Pegasus, is within the jurisdiction of the Israeli Ministry of Defense (IMOD). While Israeli authorities claim that they conduct rigorous end-use assessments before issuing licenses, there has been recent evidence to suggest that licenses were issued to governments with human rights abuses, including Saudi Arabia, Rwanda, and Azerbaijan (Kotliar D. M., et al., 2024).

After global outcry over NSO's role in human rights violations, Israel reduced the number of countries allowed to purchase offensive cyber weapons from 102 to 37 toward the end of 2021 (Bromley M., 2024). However, the secrecy surrounding the license process and absence of public checks and balances have been condemned by human rights groups and global organizations. In addition, Israeli courts have long been accommodating to export surveillance cases except where national security exceptions apply, de-facto providing corporations like NSO a near-immunity from serious judicial scrutiny (Rosen Zvi R., 2023).

European Union: A Human Rights-Centric Framework

The European Union boasts a robust legal regime on surveillance and privacy, grounded in the Charter of Fundamental Rights of the European Union (2000), the General Data Protection Regulation (GDPR), and the European Convention on Human Rights (ECHR). The Pegasus exposes several investigations across EU member states, spearheaded most notably in Poland, Hungary, and Spain, where opposition politicians and journalists are reported to have been targeted. The European Parliament established the PEGA Committee in 2022 to investigate the use of Pegasus and other spyware within the EU. The Committee's 2023 report called for greater controls, an immediate prohibition on using such spyware, and co-ordinated standards across member states for intelligence surveillance according to Articles 7 and 8 of the EU Charter (European Union, 2000). In addition, the European Data Protection Supervisor (EDPS) has also expressed concerns that spyware like Pegasus necessarily violates the spirit of the right to data protection and privacy since it is invasive, clandestine, and indiscriminate in nature (European Data Protection Supervisor, 2022).

The European Court of Human Rights (ECtHR) has also crafted strong jurisprudence in decisions like Szabó and Vissy v. Hungary (2016), where it ruled that secret surveillance systems must have adequate protection against the danger of abuse and emphasized the need for prior judicial approval (European Court of

Human Rights, 2016). These principles are increasingly shaping surveillance accountability discussions in the EU.

United States: National Security vs. Civil Liberties

The United States is a dual-track regime of oversight on surveillance, focused on national security and civil liberties protections. The Foreign Intelligence Surveillance Act (FISA) of 1978 and amendments, the USA PATRIOT Act and the USA FREEDOM Act, offer legislative safeguards for domestic and overseas surveillance by federal agencies. But these acts have been accused numerous times of allowing mass surveillance with little transparency and little judicial oversight (MacAskill E., et al., 2013).

Unlike in the EU, there is no blanket federal data protection law like the GDPR in the U.S. But the U.S. government took action against NSO Group in November 2021 by adding it to the Entity List under the U.S. Department of Commerce for conduct against U.S. foreign policy and national security interests (U.S. Department of Commerce, Bureau of Industry and Security, 2021). It marked a major change in U.S. policy, symbolising a broader commitment to address abuse of surveillance technology.

American courts have generally left it to the executive on matters involving national security, but contemporary case law shows a shifting of the balance in the direction of concerns. In United States v. Moalin case, the Ninth Circuit Court held that the NSA's bulk collection of telephone metadata was unconstitutional under the Fourth Amendment and most likely illegal under FISA (United States v. Moalin, 2020). Nevertheless, unlike the EU, whose legal structures attach a high value to privacy as a fundamental right, U.S. surveillance law is lower in rights orientation and higher in governmental prerogative and procedural legitimacy.

This comparative analysis identifies the international divergence of legal responses to the Pegasus spyware scandal. Israel's national security-oriented export model, the EU's human rights-based legal principles, and the U.S.'s executive-led surveillance regulation are all varied constitutional and legal principles. But the commonality is that there is a growing recognition that the lack of regulation on the use of spyware will undermine democratic accountability and human rights and calls for better domestic laws and multilateral regulatory strategies.

International Legal Framework on Spyware Governance

The basis of spyware technologies like Pegasus in current use makes it more important than ever to have an enforceable, harmonised, and globally accepted legal framework that oversees their development, deployment, and

extraterritorial impact. Normative and ethical arguments against digital surveillance notwithstanding, international law remains grey, reactive, and not competent to deal with the extraterritorial and cross-sectoral dimensions of spyware trade and use (Wagner B., 2012). The existing instruments such as the International Covenant on Civil and Political Rights (ICCPR), the Budapest Convention on Cybercrime, and the Wassenaar Arrangement are as helpful as they may be but fall short of having complete coverage or surveillance tools that can get the rapidly expanding spyware industry into line (De Gregorio G., 2022).

One of the major limitations is the absence of a binding treaty or protocol specifically addressing spyware or state-sponsored cybersurveillance. Whereas Article 17 of the ICCPR establishes the right to privacy, their enforcement devices like the general comments and concluding observations of the Human Rights Committee are lacking the binding character to regulate sovereign action in cyberspace (UN Human Rights Committee, 2018). Furthermore, the territorial limit of such conventions complicates effective remedies for victims of foreign surveillance agents, thereby exacerbating a legal vacuum.

The efforts of the United Nations to codify norms on state activities in cyberspace through, most prominently, the UN Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) have also resulted in soft law outcomes that remain aspirational and non-binding (Tsagourias N., et al., 2021). These State efforts at diplomacy have caused states to act "responsibly" in cyberspace but have failed to set their commitment on intrusive spyware exports and extraterritorial surveillance activities. The EU has also turned to regulatory examination, for example, a planned anti-spyware directive, in response to the Pegasus scandal, but these remain developing and restricted to domestic jurisdictions (European Parliament, 2023).

Wassenaar Arrangement, a multilateral export control regime, covers dual-use cyber monitoring items on its control lists, but the list-based control style is not transparent and is usually poorly enforced by member states (Broeders D., et al., 2020). For instance, NSO Group, an Israeli firm, selling Pegasus software for export to various governments engaged in human rights abuses occurred when Israel is a Wassenaar regime member. This shows the inherent failure of export controls to prevent misuse and implies the need for standardized standards, monitoring, and sanctions across jurisdictions (Kaster S. D., et al., 2022).

Furthermore, the challenge is also being complicated by the growing reach of private actors that are beyond the control of traditional state-driven regulatory structures. Private surveillance technology exploitation has blurred legal accountability and thus complicated state attribution, due diligence, and reparation in international law (United Nations Human Rights Council, 2011). Thus, there is mounting academic and policy agreement on the need to develop a

legally binding multilateral treaty regulation of spyware technology. Such a proposed model needs to be anchored in prevailing human rights standards but should also be sensitive to the specific features of the digital landscape.

Several guiding values should inform such a framework; firstly, a human rights one that gives precedence to individual autonomy, consent, and dignity; secondly, evident prohibitions on the use of spyware against journalists, political activists, and human rights defenders; thirdly, an effective mechanism and administrative or judicial body with the mandate to investigate, review, and sanction states and corporations; and fourthly, binding transparency obligations on procurement, deployment, and reporting of activities for spyware (Marczak et al., 2021; De Gregorio et al., 2023).

Finally, if it is to be effective, any future global legal instrument will have to draw on an intersectional framework that considers the digital divide and the disproportionate weight of surveillance borne by the Global South. Without equitable representation of countries from different regions and levels of technology, spyware regulation risks reflecting structural imbalances in digital sovereignty and accountability (Ball K., et al., 2020).

While the Pegasus scandal uncovers the full scope of existing legal and ethical challenges in question, the necessity of an international treaty or binding instrument on spyware control is no longer a matter of discussion but a necessity. Such a framework should be conceived against the backdrop of the advanced, transnational, and hybrid nature of spyware markets, balancing national interests with the inviolable rights of individuals in the digital age.

CONCLUSION

The proliferation of state-authorized digital surveillance, as illustrated by the Pegasus spyware, reveals profound legal, ethical, and policy vulnerabilities within the global telecommunications and human rights context. This study has carried out a doctrinal qualitative examination to demonstrate the ways in which current legal instruments both international and national miss the distinctive challenges posed by transnational markets for spyware, the secret nature of surveillance exports, and the resulting loss of privacy, dignity, and democratic participation. More particularly, Pegasus worldwide capabilities coupled with the opacity of export regulation and state interference highlight a systemic deficiency of balancing surveillance practice with global human rights norms.

From an international law standpoint, specifically attribution rules, due diligence, and extraterritorial human rights obligations, the present paper has established that Pegasus surveillance system constitutes a legal loopholes which erodes the protected framework envisioned under international instruments such as the International Covenant on Civil and Political Rights (ICCPR), the Universal

Declaration of Human Rights (UDHR), and the UN Guiding Principles on Human Rights (UNGPs). In this case, state responsibility is not limited to the exporting state, for instance, Israel, but also to the buying states like India that fail to meet transparency, judicial oversight, or zealous parliamentary oversight. The Indian case study reveals an established tradition of executive secrecy enabled by old laws such as the Indian Telegraph Act of 1885 and the Information Technology Act of 2000. Confronted with judicial encroachment, including the Supreme Court's formation of an expert committee to probe the Pegasus charges, indigenous legal accountability is rare. At the same time, EU and U.S. comparative practices show comparatively more dynamic mechanisms for control, export control, and openness, albeit with challenges persisting.

Some normative recommendations based on these findings follow. First, a binding international legal regime is a pressing need to oversee the surveillance software market. This could be in the form of an UN-sponsored treaty that defines the legal parameters of the use of spyware, mandates judicial warrant, and puts exporters and importers under human rights due diligence obligations. Such a treaty should also include mandatory reporting, third-party audit, and penalties for non-adherence. Second, existing mechanisms like the Wassenaar Arrangement must be transformed into binding agreements with enforceable norms rather than voluntary regimes, allowing for greater transparency and responsibility in surveillance exports. Third, legal systems of countries, especially countries like India, must be altered to include autonomous parliamentary watchdog committees, enforceable privacy provisions, and timely judicial review mechanisms for surveillance authorization and redress.

Finally, civil society, the media, and digital rights organizations must assume a larger responsibility for global norm-setting, particularly in the Global South where state institutional protection is weaker. Transparency in surveillance reports, whistleblower protections laws, and digital literacy programs can create a public sphere less vulnerable to state abuse. The Pegasus scandal, in its transnational nature and democratic dimension, has made it clear that there is an imperative for a transnational response that is rooted in law, rights, and accountability. If governments do not accept joint, open, and human rights-based regulation of surveillance technologies, the risk of misuse will only grow and threatening not just individual freedoms but the constitutional and international order itself.

REFERENCES

Ahmed, A., & Perlroth, N. (2017, June 19). *Using texts as lures, government spyware targets Mexican journalists and their families*. *The New York*

Times. https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html

Alexander, A., & Krishna, T. (2022). *Pegasus Project: Re-Questioning the legality of the cyber-surveillance mechanism*. *Laws, 11*(6), 85. https://doi.org/10.3390/laws11060085

Al-Skeini and Others v. United Kingdom, App. No. 55721/07, Grand Chamber, European Court of Human Rights, Judgement delivered July 7, 2011.

Alubaidi, A. (2023). Challenges to implementing the international digital law to protect digital rights. *Journal of Law and Sustainable Development, 11*(5). https://doi.org/10.55908/sdgs.v11i5.554

Amnesty International. (2021, July 19). *The Pegasus Project: Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally*. https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/

Ball, K., & Webster, W. (Eds.). (2020). *Big Data and surveillance: hype, commercial logics and new intimate spheres*. *Big Data & Society*. (SAGE). https://doi.org/10.1177/2053951720925853

Bapat, K. (2021, August 16). *MEITY filed a limited affidavit in Supreme Court without confirming or denying if the Government used Pegasus*. Internet Freedom Foundation https://internetfreedom.in/meity-filed-a-limited-affidavit-in-supreme-court-but-did-not-confirm-or-deny-if-the-government-used-pegasus/#:~:text=Govt's%20affidavit%20in%20SC%20doesn,Government%20used%20the%20Pegasus%20Spyware

Bapat, K. (2021, August 16). *MEITY filed a limited affidavit in Supreme Court without confirming or denying if the government used Pegasus*. Internet Freedom Foundation. https://internetfreedom.in/meity-filed-a-limited-affidavit-in-supreme-court-but-did-not-confirm-or-deny-if-the-government-used-pegasus/

Bhandari, V., & Lahiri, K. (2020). The surveillance state: Privacy and criminal investigation in India—Possible futures in a post-Puttaswamy world. *University of Oxford Human Rights Hub Journal, 3*(2), 15–45. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3580630

Bhatia, G. (2021, October 12). *"The yes or a no": The court must ask about Pegasus*. *The Hindu*. https://www.thehindu.com/opinion/lead/the-yes-or-a-no-the-court-must-ask-about-pegasus/article36953053.ece

Broeders, D., & van den Berg, B. (2020). *Governing cyberspace: Cyber norms and responsible state behavior in cyberspace*. Bloomsbury Publishing.

Bromley, M. (2024, March 8). *Export controls and cyber-surveillance tools: Five suggestions for the Summit for Democracy*. Stockholm International

Peace Research Institute. https://www.sipri.org/commentary/2024/export-controls-cyber-surveillance-summit-democracy

Brown, C. (2024). *Article 4 of the ARSIWA: Conduct of organs of a State*. In A. Kulick & M. Waibel (Eds.), *General International Law in International Investment Law: A Commentary* (pp. 104–113). Oxford University Press. https://doi.org/10.1093/law/9780192849922.003.0018

Brown, C. (2024). Article 8 of the ARSIWA: Conduct of organs of a State. In A. Kulick & M. Waibel (Eds.), *General international law in international investment law: A commentary* (Chapter 17). Oxford University Press. https://doi.org/10.1093/law/9780192849922.003.0022

Carter v. Canada (Attorney General), 2015 SCC 5, [2015] 1 S.C.R. 331. Supreme Court of Canada.

Chatinakrob, T. (2024). Interplay of international law and cyberspace: State sovereignty violation, extraterritorial effects, and the paradigm of cyber sovereignty. *Chinese Journal of International Law, 23*(1), 25–72. https://doi.org/10.1093/chinesejil/jmae005

Coco, A., & de Souza Dias, T. (2021). *"Cyber due diligence": A patchwork of protective obligations in international law*. *European Journal of International Law, 32*(3), 771–806. https://doi.org/10.1093/ejil/chab056

Court of Justice of the European Union. (2020). *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems (Schrems II), Case C-311/18*.

De Gregorio, G. (2022). *Digital constitutionalism in Europe: Reframing rights and powers in the algorithmic society*. Cambridge University Press.

Deibert, R. J. (2020). *Reset: Reclaiming the internet for civil society* (CBC Massey Lectures). House of Anansi Press.

Dumbrava, C. (2023, June). *Investigation of the use of Pegasus and equivalent surveillance spyware* (At a Glance, PE 747.923). European Parliamentary Research Service, European Parliament. https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA%282023%29747923

European Court of Human Rights. (2015). *Roman Zakharov v. Russia*, No. 47143/06.

European Court of Human Rights. (2016). *Szabó and Vissy v. Hungary*, No. 37138/14.

European Data Protection Supervisor. (2022, February 15). *Preliminary remarks on modern spyware*. *Complex Discovery*. https://complexdiscovery.com/spyware-revelations-edps-remarks-on-modern-spyware/

European Parliament. (2023, May 8). *Report of the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA)*. https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/PEGA/DV/2023/05-08/REPORTcompromises_EN.pdf

European Union. (2000). *Charter of Fundamental Rights of the European Union.* (Article 7 & 8).

Gascón Marcén, A. (2024). *The Budapest Convention and the UN Cybercrime Convention negotiations*. In *Global Cybersecurity and International Law* (pp. 174–192). Routledge.

George, P. J. (2021, July 25). *Explained: Pegasus and the laws on surveillance in India*. *The Hindu.* https://www.thehindu.com/news/national/explained-pegasus-and-the-laws-on-surveillance-in-india/article61437972.ece

Human Rights Committee. (1988). *General Comment No. 16: The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (Art. 17)*. https://www.refworld.org/legal/general/hrc/1988/en/27539

Human Rights Committee. (2011). *General Comment No. 34: Freedoms of opinion and expression*. UN Doc. CCPR/C/GC/34. https://www.refworld.org/legal/general/hrc/2011/en/83764

Human Rights Committee. (2019). *General Comment No. 36 (2018) on Article 6 (Right to Life) of the International Covenant on Civil and Political Rights* (CCPR/C/GC/36). United Nations.

Human Rights Watch. (2014, July 17). *United Nations: Rein in mass surveillance.* Human Rights Watch. https://www.hrw.org/news/2014/07/17/united-nations-rein-mass-surveillance#:~:text=In%20the%20report%2C%20Pillay%20reaffirmed,some%20national%20laws%20currently%20provide.

Humble, K. P. (2021). *International law, surveillance and the protection of privacy*. *The International Journal of Human Rights, 25*(1), 1–25. https://doi.org/10.1080/13642987.2020.1763315

Inter-American Court of Human Rights (IACtHR). (2017). *Advisory Opinion OC-23/17*.

Inter-American Court of Human Rights. (2009). *Escher et al. v. Brazil*, Series C No. 200

International Court of Justice. (1986). *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits*, ICJ Reports 1986, 14.

International Criminal Tribunal for the former Yugoslavia. (1997, May 7). *Tadić case: the verdict.*

International Law Commission. (2001). *Draft articles on responsibility of states for internationally wrongful acts, with commentaries* (Art. 6) (Supplement No. 10, A/56/10, ch. IV.E.1). United Nations. https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf

International Law Commission. (2001). *Draft articles on responsibility of states for internationally wrongful acts, with commentaries* (Art. 11) (Supplement No. 10, A/56/10, ch. IV.E.1). United Nations. https://www.refworld.org/legal/otherinstr/ilc/2001/en/20951

International Law Commission. (2001). *Draft articles on responsibility of states for internationally wrongful acts, with commentaries* (Chapter IV, Article 16). United Nations.

International Telecommunication Union. (1992). *Constitution and Convention of the International Telecommunication Union* (Article 40). Geneva: ITU.

Jaffe, A. (2023). *Global Surveillance* (CQ Researcher). CQ Press.

Kaster, S. D., & Ensign, P. C. (2022). Privatized espionage: NSO Group Technologies and its Pegasus spyware. *Thunderbird International Business Review, 65*(3), 355–364. https://doi.org/10.1002/tie.22321

Kirchgaessner, S., Lewis, P., Pegg, D., Cutler, S., Lakhani, N., & Safi, M. (2021, July 18). *Revealed: leak uncovers global abuse of cyber-surveillance weapon*. *The Guardian*. https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus

Kotliar, D. M., & Carmi, E. (2024). Keeping Pegasus on the wing: legitimizing cyber espionage. *Information, Communication & Society, 27*(8), 1499–1529. https://doi.org/10.1080/1369118X.2023.2245873

Kumar, R. (2025, January 12). *How the Data Protection Act will impact you personally*. *The New Indian Express*. https://www.newindianexpress.com/explainers/2025/Jan/12/how-the-data-protection-act-will-impact-you-personally

Kuner, C. (2021). The path to recognition of data protection in India: The role of the GDPR and international standards. *National Law Review of India, 33*(1), 1–23. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3964672

Lewis, P. (2021, July 18). *Huge data leak shatters the lie that the innocent need not fear surveillance*. *The Guardian*. https://www.theguardian.com/news/2021/jul/18/huge-data-leak-shatters-lie-innocent-need-not-fear-

surveillance#:~:text=The%20data%20leak%20is%20a,entered%20on%20to%20a%20system.

MacAskill, E. & Dance, G. (2013, November 1). *NSA files: Decoded—What the revelations mean for you* [Interactive feature]. *The Guardian.* https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

MacAskill, E., & Dance, G. (2013, November 1). *NSA Files: Decoded – decoding Snowden's surveillance revelations* [Interactive report]. *The Guardian.* https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

Manohar Lal Sharma v. Union of India, AIR 2021 SC 5396.

Marczak, B., Scott-Railton, J., McKune, S., Abdul Razzak, B., & Deibert, R. (2018, September 18). *Hide and seek: Tracking NSO Group's Pegasus spyware to operations in 45 countries* (Research Report No. 113). The Citizen Lab. https://nsarchive.gwu.edu/document/27613-6-citizen-lab-report-pegasus-spyware

Milanović, M. (2011). *Extraterritorial application of human rights treaties: Law, principles, and policy*. Oxford University Press.

Milanović, M. (2015). Human rights treaties and foreign surveillance: Privacy in the digital age. *Harvard International Law Journal, 56*, 81–112. https://www.ilsa.org/Jessup/Jessup16/Batch%202/MilanovicPrivacy.pdf

Milanović, M. (2022). Surveillance and cyber operations. In M. Gibney, et al. (Eds.), *The Routledge handbook on extraterritorial human rights obligations* (pp. 366–378). Routledge.

Moalin, *United States v. Moalin*, 973 F.3d 977 (9th Cir. 2020).

Naithani, P. (2021, December 4). *Pegasus and the law*. *Letters*, *Economic and Political Weekly, 56*(49). https://www.epw.in/journal/2021/49/letters/pegasus-and-law.html

NSO Group Technologies Ltd. (2021, June). *Transparency and responsibility report 2021* [PDF]. NSO Group. https://www.nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf

Paranjoy. (2024, December 8). *Indian use of Pegasus*. *Centre for the Study of Organized Hate*. https://www.csohate.org/2024/12/08/indian-use-of-pegasus/

Penney, J. (2017). Internet surveillance, regulation, and chilling effects. *Internet Policy Review*, 6(2). https://doi.org/10.14763/2017.2.692

Penney, J. W. (2021). Cybersecurity, human rights, and empiricism: The case of digital surveillance. In P. Cornish (Ed.), *The Oxford Handbook of Cyber Security* (Chapter 56). Oxford University Press

Project Pegasus: How Phones of Journalists, Ministers, Activists May Have Been Used to Spy on Them. (2021, July 18). *The Wire*. https://thewire.in/rights/project-pegasus-journalists-ministers-activists-phones-spying

Riecke, L. (2023). Unmasking the term "dual use" in EU spyware export control. *European Journal of International Law, 34*(3), 697–720. https://doi.org/10.1093/ejil/chad039

Rosen Zvi, R. (2023, January 30). *Managing Risky Business – The international regulatory framework of spyware companies: Where it is lacking and where it is heading*. *Center on Transnational Business and the Law Blog, Georgetown Law.* https://www.law.georgetown.edu/ctbl/blog/managing-risky-business-the-international-regulatory-framework-of-spyware-companies-where-it-is-lacking-and-where-it-is-heading/

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

Sirohi, N. (2021, August 7). *Pegasus in the Room: Law of surveillance and national security's alibi* [Commentary]. Observer Research Foundation. https://www.orfonline.org/expert-speak/pegasus-in-the-room-law-of-surveillance-and-national-securitys-alibi

Stahl, B. C., Schroeder, D., & Rodrigues, R. (2023). Surveillance capitalism. In *Ethics of artificial intelligence* (pp. 39–52). Springer. https://doi.org/10.1007/978-3-031-17040-9_4

Telford, T. (2021, December 28). *Claims Polish government used spyware is 'crisis for democracy', says opposition*. *The Guardian.* https://www.theguardian.com/world/2021/dec/28/poland-pegasus-spyware-donald-tusk

Tsagourias, N., & Buchan, R. (Eds.). (2021). *Research Handbook on International Law and Cyberspace* (2nd ed.). Edward Elgar Publishing.

Tufekci, Z. (2015). Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. *Colorado Technology Law Journal*, 13(1), 203–218. https://scholar.law.colorado.edu/ctlj/vol13/iss2/4/

U.S. Department of Commerce, Bureau of Industry and Security. (2021, November 4). *Commerce adds NSO Group and other foreign companies to Entity List for malicious cyber activities.* https://www.bis.gov/press-release/commerce-adds-nso-group-other-foreign-companies-entity-list-malicious-cyber-activities

UN Human Rights Committee. (1988). *General comment No. 16: Article 17 (Right to privacy)*. UN Doc. HRI/GEN/1/Rev.9.

United Nations General Assembly. (2014, December 18). *The right to privacy in the digital age* (A/RES/68/167). United Nations Digital Library. https://digitallibrary.un.org/record/764407?ln=en&v=pdf

United Nations Human Rights Committee. (2004, May 26). *General comment No. 31 [80]: The nature of the general legal obligation imposed on States Parties to the Covenant* (CCPR/C/21/Rev.1/Add.13). Refworld.

United Nations Human Rights Council. (2011). *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*. United Nations Office of the High Commissioner for Human Rights.

United Nations. (1948). *Universal Declaration of Human Rights*, Article 12.

United Nations. (1966). *International Covenant on Civil and Political Rights*, Article 17.

Wagner, B. (2012). Exporting censorship and surveillance technology. *Netherlands: Humanist Institute for Co-operation with Developing Countries.* PP. 1-19. https://www.academia.edu/2133607/Exporting_Censorship_and_Surveillance_Technology

Walker, S. (2024, April 1). *Poland launches inquiry into previous government's spyware use*. *The Guardian.* https://www.theguardian.com/world/2024/apr/01/poland-launches-inquiry-into-previous-governments-spyware-use

Zalnieriute, M. (2022). *Big Brother Watch and Others v. the United Kingdom*. *American Journal of International Law, 116*(3), 585–592.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET