INTERNATIONAL JOURNAL OF SOCIAL SCIENCES BULLETIN
ISSN: (E) 3007-1917 (P) 3007-1909
Volume 4, Issue 5, 2026

VPN USE IN EMERGENCY SITUATIONS: A STUDY OF PRIVACY RIGHTS UNDER THE CONSTITUTION OF PAKISTAN AND INTERNATIONAL HUMAN RIGHTS LAW

Noor Ul Huda Afzal[*1], Adeeb Afzal[2], Kainat Afzal[3]

[*1]*LL.B (Hons) Scholar, School of Law, Bahria University, E-8 Campus, Islamabad, Pakistan*
[2]*LL.B (Hons), University of the Punjab; LL.M Human Rights Law Scholar, Department of Law, International Islamic University, Islamabad, Pakistan*
[3]*BS Sociology, School of Sociology, Quaid-i-Azam University, Islamabad, Pakistan*

[*1]noorulhudaafzal2005@gmail.com, [2]adib56afzal@gmail.com, [3]afzalkainat302@gmail.com

Corresponding Author: *
Noor Ul Huda Afzal
DOI: https://doi.org/10.5281/zenodo.20047715

Received	Accepted	Published
11 March 2026	21 April 2026	06 May 2026

ABSTRACT

In an increasingly digital world, protecting privacy, access to information, and freedom of expression during emergencies—such as armed conflict, political unrest, and climate-related disasters—has become a key legal challenge. This study examines the role of Virtual Private Networks (VPNs) within Pakistan's constitutional framework (Articles 19 and 19A) and under international human rights law, including the ICCPR and UDHR, while also assessing the regulatory role of the Pakistan Telecommunication Authority (PTA). Using a doctrinal approach, the study analyzes legal frameworks, PTA practices, and relevant international best practices in digital governance. It finds that while VPNs are important tools for bypassing censorship and ensuring secure communication, their effectiveness is limited by state restrictions, technical blocking, and corporate compliance pressures.The study highlights that international law requires any restriction to meet the principles of legality, necessity, and proportionality, yet blanket VPN bans and internet shutdowns often fail these standards and cause disproportionate harm during emergencies. It concludes that VPNs alone cannot ensure digital rights protection. Accordingly, it recommends clear, proportionate, and transparent regulation, judicial oversight of PTA actions, protection of internet access as critical infrastructure, stronger corporate accountability, and improved international coordination. Ultimately, safeguarding digital rights during emergencies is essential for democratic resilience and effective crisis response.

Key Words: *VPN, Emergency Situations, Legal Framework, Privacy, Access, Legal Framework, Digital Rights, and UDHR.*

Introduction:

This study, titled "VPN Use in Emergency Situations: A Study of Privacy Rights under the Constitution of Pakistan and International Human Rights Law," explores the growing significance of Virtual Private Networks (VPNs) in protecting digital rights during times of crisis. VPNs have emerged as critical tools that enable individuals to safeguard privacy, maintain secure communication, and access information in environments characterized by censorship, surveillance, or infrastructure disruption. The study situates this issue within the constitutional framework of Pakistan—particularly Articles 19

and 19A—and the broader protections guaranteed under international instruments such as the International Covenant on Civil and Political Rights and the Universal Declaration of Human Rights, both of which affirm the fundamental rights to privacy and freedom of expression.

The research is guided by key questions addressing the extent to which VPNs protect privacy and access to information during emergencies, the legality of government-imposed restrictions under international human rights standards, the technical and legal mechanisms used to block VPNs, and the broader impact of such restrictions on freedom of expression, digital security, and civic participation. It also explores policy alternatives that can balance state security concerns with the protection of digital rights. These questions collectively highlight the central tension between national security imperatives and the preservation of fundamental freedoms in digital spaces, particularly during crises such as armed conflict, political unrest, and climate-related disasters.

The analytical framework of this study is grounded in a doctrinal legal methodology, drawing upon constitutional provisions, statutory instruments, judicial precedents, and international human rights law. It incorporates principles of legality, necessity, and proportionality as developed under Article 19 of the ICCPR, alongside interpretative guidance from bodies such as the United Nations Human Rights Council and the Office of the United Nations High Commissioner for Human Rights. The study further integrates soft-law frameworks, including the UN Guiding Principles on Business and Human Rights, and examines comparative state practices and case studies to evaluate how digital restrictions operate in real-world emergency contexts.

Finally in conclusion, this study underscores the urgent need for a balanced and rights-based approach to digital governance during emergencies. While states possess legitimate authority to ensure security and public order, such powers must be exercised within the limits of constitutional guarantees and international human rights obligations. The study recommends the adoption of clear legal frameworks, judicial oversight, and proportionate, time-bound measures in regulating VPN use. It also highlights the importance of corporate responsibility and international oversight in safeguarding digital rights. Ultimately, protecting privacy and access to information during emergencies is not only a legal obligation but a prerequisite for democratic resilience and effective crisis response.

Key Words: VPN, Emergency Situations, Legal Framework, Privacy, Access, Legal Framework, Digital Rights, and UDHR

Virtual Private Networks (VPNs)

A Virtual Private Network (VPN) is a technology used to create a secure, encrypted "tunnel" over a public network, such as the internet. By establishing this logical connection, devices can communicate as if they were on the same private network, ensuring that sensitive data is protected from eavesdropping or manipulation by unauthorized third parties.

A VPN is a networking technology that uses the Internet to connect one or more computers to a private network. These networks are used by businesses to permit their workers to remotely access corporate resources that they would not otherwise be able to from their homes, hotels, etc. (Chávez, 2020).

A VPN can be described as “an encrypted connection over the Internet from a device to a network” (CISCO, 2022). The encrypted connection assists in ensuring the safe transmission of sensitive data. It checks unapproved people from “eavesdropping on the traffic” and permits the user to perform work from a remote location. VPN technology is commonly utilised in corporate settings (CISCO, 2022).

The NIST (NIST, no date) provides the following definitions of VPN:

- “Protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line.”
- “A virtual network built on top of existing networks that can provide a secure communications mechanism for data and IP information transmitted between networks.”

- "A restricted-use, logical (i.e., artificial or simulated) computer network constructed from the system resources of a relatively public physical network (such as the Internet), often using encryption and tunneling."
- "A virtual network built on top of existing physical networks that provides a secure communications mechanism for data and IP information transmitted between networks or nodes."

VPNs safeguard communications over public and private networks (e.g., Internet, fibre networks, MPLS networks). VPNs provide confidentiality, integrity, replay protection, data origin authentication, and access control (Barker et al., 2020).

Network Layer Security (IPsec)

Internet Protocol Security (IPsec) is a group of "open standards" for safeguarding private communications over public networks. IPsec is the most commonly used security control at the network layer and is generally utilised to encrypt IP traffic and generate a VPN.

IP networking is a global standard used for communication across networks. It operates through four layers:

- **Application Layer:** Handles DNS, web (HTTP/HTTPS), and email (SMTP/IMAP)
- **Transport Layer:** Uses TCP (reliable) and UDP (unreliable)
- **Network Layer:** Uses IP, ICMP, and IGMP for routing
- **Data Link Layer:** Uses Ethernet and WiFi (IEEE 802.11)

Each layer adds information as data moves downward and removes it when moving upward. Security at one layer is not sufficient for full protection.

At different layers, security controls include S/MIME and SSH (application), TLS/DTLS (transport), and IPsec (network). Among these, IPsec is most effective for VPNs because it protects all applications without requiring modification.

IPsec Protocol

IPsec provides multiple security services including: confidentiality, integrity, peer authentication, replay protection, traffic protection, access control, perfect forward secrecy (PFS), and mobility.

- Confidentiality ensures data cannot be read by unauthorized users through encryption.
- Integrity ensures data is not modified using message authentication codes (MAC).
- Peer authentication verifies identity of endpoints.
- Replay protection prevents duplicate transmission attacks.
- Tunnel mode hides communication patterns.
- PFS frequently changes session keys.
- Mobility allows network switching without breaking connections.

VPN as Implementation of IPsec

VPNs are the most common implementation of IPsec.

A VPN is a "virtual network built on top of existing physical networks that can provide a secure communications mechanism for data and IP information transmitted between networks or between different nodes on the same network" (Barker et al., 2020).

VPNs are cost-effective compared to private leased lines and are widely used to securely transmit sensitive data over the Internet.

VPN architectures include:

- **Gateway-to-Gateway VPN:** Connects two networks such as headquarters and branch office.
- **Remote Access (Host-to-Gateway VPN):** Connects individual users to organizational networks for secure access to internal services such as email and servers.

Primary Types of VPNs

The video identifies two main categories for implementing these tunnels:

Site-to-Site VPNs:

Purpose: These are used to connect two separate network locations (such as a corporate headquarters and a branch office) so that they function as if they were part of the same internal infrastructure.

Implementation: The connection is established directly between the firewalls at both locations. This type of connection typically utilizes the IPsec (Internet Protocol Security) suite for robust, end-to-end encryption.

Remote Access VPNs:
Purpose: Designed for individual users (like employees working from home or traveling) who need to access internal corporate resources securely.

Web-based/Portal Access: This method uses a web browser as the tunnel endpoint. While convenient, it is often more restricted in terms of the types of data or applications an employee can interact with. These setups frequently use SSL/TLS encryption.

Software Client: This approach involves installing specialized software on the user's device. It creates a "full tunnel" experience, effectively making the remote computer appear as if it is directly connected to the internal corporate network. These clients can be configured to use either SSL/TLS or IPsec to secure the connection.

Key Benefits:
Enhanced Security: Essential for protecting your data on public Wi-Fi networks, which are often vulnerable to cyber threats.

Access to Restricted Content: VPNs allow you to bypass geographical restrictions and censorship, granting access to websites or content that may not be available in your current region.

Comparison of Top VPN Services
The video identifies three top-tier providers, each catering to different user needs:
1.ExpressVPN:

Best Overall: Recommended for those prioritizing reliability and ease of use.

Key Feature: Boasts a highly credible, real-life stress-tested no-logs policy.

Device Limit: Supports up to 5 simultaneous connections.
2.NordVPN:

Best Value: A well-rounded choice that offers high performance along with bonus security tools.

Key Feature: Includes "Threat Protection" to block ads, malware, and harmful files.

Device Limit: Supports up to 6 simultaneous connections.
3.Surfshark:

Best Budget Option: Ideal for large families or users who want to secure many devices at a low cost.

Key Feature: Allows unlimited simultaneous connections and includes advanced options like "No Borders" mode and rotating IPs.

Device Limit: Virtually unlimited connections per account.
VPNs protect data by creating a secure, encrypted tunnel, which prevents unauthorized parties from eavesdropping or manipulating sensitive information in transit. By using encryption protocols like IPsec or SSL/TLS, the VPN ensures that even if traffic is intercepted, it remains unreadable without decryption keys.

Research questions :
1. **To what extent does VPN use during emergencies protect individuals' right to privacy and access to information?**
2. **How do government-imposed VPN restrictions during emergencies align with international human rights standards (legality, necessity, proportionality)?**
3. **What are the technical and legal mechanisms used by internet service providers to block VPNs, and how effective are they?**
4. **How does restricting VPN access impact freedom of expression, digital security, and civic participation during crises?**

5. **What policy alternatives can balance state security concerns with the protection of privacy and digital rights during emergencies?**

Research Methodology

This study adopts a qualitative doctrinal (black-letter) approach to analyze the legality of VPN use in emergency situations, with particular focus on privacy rights under the Constitution of Pakistan, 1973 and international human rights law.

The research is analytical and descriptive, relying on the interpretation of primary sources, including constitutional provisions, statutes, and judicial precedents, as well as international instruments such as the International Covenant on Civil and Political Rights. Secondary sources include academic literature, journal articles, and legal databases such as Pakistan Code, PTA legal framework available on official websites, United Nations databases, ICJ case law, and domestic court decisions, as well as research platforms like Pakistan Law Site.

A qualitative content analysis is employed to interpret legal texts and identify gaps and inconsistencies in the existing legal framework. These gaps are then formulated into research questions, which guide the study's critical evaluation of whether restrictions on VPN use comply with constitutional and international privacy standards.

The methodology is limited to doctrinal analysis and does not include empirical data; however, it ensures a systematic and coherent legal examination, leading to reasoned conclusions and recommendations.

1. To what extent does VPN use during emergencies protect individuals' right to privacy and access to information?

In the digital environment, private companies play a dual and often contradictory role in shaping access to information and privacy, particularly during emergency situations. On one hand, internet service providers and technology companies may act as agents of restriction by complying with state directives to block websites, filter online content, or disable access to communication platforms. Such practices are often justified under national security or public order laws but may result in over blocking and disproportionate interference with lawful expression. This raise concerns under international human rights law, particularly Article 19 of the International Covenant on Civil and Political Rights, which protects freedom of expression and access to information.

The same concerns are reflected in digital rights interpretations by the United Nations Human Rights Council, which emphasizes that states must ensure that private actors do not arbitrarily restrict online freedoms. In Pakistan, such restrictions must also be assessed in light of fundamental rights guaranteed under the Constitution of Pakistan, 1973, particularly Articles 19 and 19A, which protect freedom of speech and the right to information.

On the other hand, these companies also function as key facilitators of digital human rights by providing encryption services, secure communication tools, and Virtual Private Networks (VPNs), which help individuals maintain privacy and access information in restrictive or emergency environments. Academic literature highlights that VPNs serve as essential instruments of digital resilience, particularly where censorship, surveillance, or internet shutdowns occur (DeNardis, The Global War for Internet Governance, 2014; Freedom House, Freedom on the Net 2025).

Thus, the role of companies reflects a structural tension between state compliance and human rights protection, raising critical questions about corporate responsibility and their alignment with international digital rights standards, including the UN Guiding Principles on Business and Human Rights (2011).

Case Studies:

1.Internet connectivity in areas affected by armed conflict has been constrained by government pressure or by the risk calculations of service providers. As the two sides in Sudan's civil war destroyed the country's telecommunications infrastructure and imposed local service shutdowns, Sudanese people and aid groups turned to Starlink for emergency access to the internet. In April 2024, the company notified

Sudanese users that it would limit services in the country due to regulatory constraints. Civil society organizations raised concerns about the impact of further connectivity restrictions on local humanitarian efforts, and Starlink ultimately appeared to remain accessible throughout the coverage period. Starlink has reportedly faced similar dilemmas in Russian-occupied Ukrainian territories and Israeli occupied Palestinian territories, which are not covered by Freedom on the Net.

2. ***India imposed one of the longest internet shutdowns in Kashmir,*** where access to communication platforms was heavily restricted. Users relied on VPNs to access information and communicate during emergencies, particularly for legal, medical, and educational needs.

3. Myanmar Military Coup (2021–Present) – VPN Dependency Under Digital Repression

After the military coup in Myanmar, authorities restricted social media platforms and imposed surveillance measures. Citizens widely adopted VPNs and encrypted tools to access blocked platforms and report human rights abuses.

The situation demonstrates how VPNs become essential tools for digital survival in emergency authoritarian contexts, but also how states attempt to criminalize their use.

4. Gaza Palestine

The situation in Palestine (Gaza and the West Bank) demonstrates how conflict and emergency conditions can severely disrupt digital communication infrastructure, including internet shutdowns, network damage, and restrictions on connectivity. In such circumstances, individuals increasingly rely on VPNs and encrypted tools to access information, communicate, and report human rights conditions.

The United Nations Human Rights Council and the Office of the High Commissioner for Human Rights have documented that communication disruptions in the Occupied Palestinian Territory significantly impact freedom of expression and access to information, and must comply with international human rights standards of necessity and proportionality.

These protections are grounded in Article 19 of the International Covenant on Civil and Political Rights, which safeguards the right to seek and receive information even during emergencies

Palestine illustrates that in conflict situations, VPNs become essential tools for maintaining privacy and access to information, while excessive communication restrictions raise serious concerns under UN human rights frameworks.

VPN use during emergency situations provides an important, but limited, safeguard for the rights to privacy and access to information. In contexts such as Sudan, Kashmir, Myanmar, and Palestine, VPNs enable individuals to bypass censorship, maintain secure communication, and access critical information despite internet shutdowns and surveillance. However, their effectiveness remains conditional, as states increasingly impose legal and technical restrictions on VPN usage, and private companies often face pressure to comply with state directives. This creates a structural tension between corporate obligations and human rights standards, raising concerns under Article 19 of the International Covenant on Civil and Political Rights and constitutional protections such as Articles 19 and 19A of the Constitution of Pakistan, 1973.

At the international level, oversight operates through a decentralized framework rather than a single binding authority. The United Nations Human Rights Council and the Office of the United Nations High Commissioner for Human Rights monitor and interpret state obligations, emphasizing that digital restrictions must meet the standards of legality, necessity, and proportionality. The UN Guiding Principles on Business and Human Rights impose a responsibility on companies to respect human rights, while initiatives such as the Global Network Initiative promote transparency and accountability. The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression further strengthens oversight by documenting violations and shaping normative standards.

In situations of armed conflict or widespread human rights violations, the International Criminal Court may also play an indirect but significant role. While the ICC does not regulate VPN use or digital governance per se, it can exercise jurisdiction over crimes where communication blackouts, suppression of information, or targeting of digital infrastructure form part of broader violations such as crimes against humanity or war crimes. In this sense, severe and systematic restrictions on access to information during conflicts may contribute to evidentiary findings before the Court, reinforcing accountability at the international level.

Therefore, while VPNs act as crucial tools of digital resilience, they cannot replace a rights-based legal framework. States must avoid blanket internet shutdowns and ensure that any restrictions are lawful, proportionate, and subject to judicial oversight. At the same time, companies should align with international human rights standards by resisting overbroad state demands, conducting due diligence, and safeguarding secure communication tools. Strengthening international oversight, including indirect accountability through mechanisms such as the ICC, remains essential to ensure that digital rights are effectively protected during emergencies.

2. How do government-imposed VPN restrictions during emergencies align with international human rights standards (legality, necessity, proportionality)?

Government-imposed restrictions on VPN use during emergencies must be assessed against the well-established tripartite test of **legality, necessity, and proportionality** under Article 19(3) of the International Covenant on Civil and Political Rights. While states may lawfully limit certain aspects of freedom of expression and access to information, such limitations are only permissible when they strictly comply with these cumulative standards.

Legality requires that any restriction on VPN use be grounded in clear, accessible, and predictable law. Vague or overly broad regulatory frameworks—often justified under national security or public order—fail to meet this requirement, particularly where they grant unfettered discretion to authorities or lack procedural safeguards. In many jurisdictions, emergency powers are invoked without transparent legal basis, raising serious concerns regarding arbitrariness and abuse.

Necessity demands that restrictions pursue a legitimate aim—such as national security or public safety—and that VPN limitations are demonstrably required to achieve that aim. However, blanket bans on VPNs or widespread internet shutdowns rarely satisfy this condition, as less intrusive measures (such as targeted content regulation or lawful surveillance with judicial oversight) are often available. Reports by the Office of the United Nations High Commissioner for Human Rights and resolutions of the United Nations Human Rights Council consistently affirm that sweeping digital restrictions are generally inconsistent with international human rights law.

Proportionality requires that the scope and impact of the restriction be balanced against the interest it seeks to protect. Measures that indiscriminately block VPN access—thereby restricting journalists, human rights defenders, and ordinary citizens from accessing information or communicating securely—are typically disproportionate. Such restrictions often produce broader harm than the risk they aim to mitigate, especially in emergency contexts where access to information can be vital for safety, humanitarian coordination, and accountability.

Moreover, under the UN Guiding Principles on Business and Human Rights, states must also ensure that private companies do not become instruments of disproportionate restrictions, and that any cooperation with state directives respects human rights standards.

While many states impose disproportionate VPN restrictions, a number of jurisdictions demonstrate more rights-compliant approaches consistent with Article 19 of the International Covenant on Civil and Political Rights.Germany allows unrestricted use of VPNs and strongly protects encryption under its constitutional framework and EU law. Surveillance measures are subject to strict judicial authorization, reflecting compliance with legality and proportionality.

There is no general prohibition on circumvention tools, even in security-sensitive contexts.

Estonia is widely regarded as a model digital state. It promotes secure internet access, supports encryption technologies, and avoids blanket restrictions. Emergency measures remain targeted and time-bound, with transparency and legal clarity—aligning closely with necessity and proportionality standards Also, Canada permits VPN use without restriction and ensures that any limitation on digital communication is subject to judicial review and Charter protections. Government surveillance powers are constrained by courts, ensuring that restrictions are necessary and proportionate. Sweden, under EU data protection regimes (such as GDPR), supports privacy-enhancing technologies including VPNs. Any restrictions must pass strict proportionality review, and users benefit from strong legal remedies against misuse of surveillance powers.

The Budapest Convention on Cybercrime provides an important legal framework for assessing VPN restrictions, particularly through Article 15, which requires that all cyber-related measures comply with principles of legality, necessity, proportionality, and adequate safeguards against abuse. While the Convention does not directly regulate VPNs, it emphasizes that state powers such as data access, surveillance, and interception (Articles 19–21) must be targeted, lawful, and subject to judicial oversight. This implies that broad or indiscriminate restrictions on VPN use during emergencies would be inconsistent with its standards, as the Convention favors precise and rights-based enforcement mechanisms over blanket limitations on digital tools.

VPN use during emergencies plays a meaningful but limited role in protecting the rights to privacy and access to information under Article 19 of the International Covenant on Civil and Political Rights. In situations such as Kashmir, Myanmar, Sudan, and Palestine, VPNs have functioned as essential digital resilience tools, enabling individuals to bypass censorship, maintain secure communication, and access information during internet shutdowns or conflict. However, their effectiveness is frequently constrained by state restrictions, criminalization, and compliance by private companies acting under government pressure. International human rights law, including Article 12 and 19 of the Universal Declaration of Human Rights and Article 19 of the ICCPR, establishes that any restriction on access to information must meet the strict tests of legality, necessity, and proportionality. In addition, frameworks such as the Budapest Convention on Cybercrime reinforce that state powers in cyberspace must remain targeted, lawful, and subject to judicial safeguards rather than blanket restrictions.

From an international governance perspective, there is currently no ICC-like court specifically for digital rights enforcement. However, accountability is dispersed across several institutions: the United Nations Human Rights Council and the Office of the United Nations High Commissioner for Human Rights monitor state compliance; the UN Special Rapporteur on freedom of expression investigates violations; and regional human rights courts (such as the European Court of Human Rights) adjudicate digital rights cases within their jurisdictions. Despite these mechanisms, enforcement remains fragmented and largely non-binding in urgent digital rights crises.

States should ensure that any restriction on VPNs or digital access tools during emergencies complies strictly with international human rights standards under the UDHR and ICCPR, particularly the principles of legality, necessity, and proportionality. Blanket internet shutdowns, indiscriminate VPN bans, and criminalization of circumvention tools should be avoided as they are generally incompatible with Article 19 rights. Instead, governments should adopt narrowly tailored, time-bound, and judicially supervised measures that address specific and demonstrable security risks.

At the corporate level, technology companies must comply with the UN Guiding Principles on Business and Human Rights by conducting human rights due diligence, resisting disproportionate state requests where feasible, and maintaining transparency regarding restrictions on VPN and encryption services.

At the international level, there is a growing need for a dedicated digital rights governance forum. This could take the form of a specialized global mechanism—similar in structure to the International Criminal Court (ICC)—but focused on digital rights violations. Such a body could:

Investigate large-scale internet shutdowns and VPN bans

Adjudicate serious violations of digital expression and access to information

Issue binding or quasi-binding rulings on state compliance

Coordinate with UN bodies, regional courts, and technical governance institutions

Until such a structure exists, stronger coordination between existing mechanisms—particularly the UN Human Rights Council, OHCHR, and regional courts—is essential to close the accountability gap in digital governance.

3. What are the technical and legal mechanisms used by internet service providers to block VPNs, and how effective are they?

Internet Service Providers (ISPs) use a combination of technical and legal mechanisms to detect and block Virtual Private Networks (VPNs), especially during emergencies such as political unrest, cybersecurity threats, and natural disasters (floods, climate-related crises). These practices are increasingly important because VPNs are widely used to secure communication and access information when normal infrastructure is disrupted. However, they also raise concerns under Article 19 of the International Covenant on Civil and Political Rights and Article 12 and 19 of the Universal Declaration of Human Rights, particularly when restrictions interfere with emergency communication, disaster response, and humanitarian coordination.

ISPs commonly use Deep Packet Inspection (DPI), IP address blocking, DNS tampering, port filtering, and traffic fingerprinting to detect VPN usage. Academic research confirms that DPI can identify encrypted VPN flows by analyzing packet size, timing, and protocol behavior even when content is encrypted (Akhavan Niaki et al., ICLab Internet Censorship Measurement Platform, 2019) . Similarly, studies show that VPN endpoints are frequently blacklisted through IP filtering, creating a "cat-and-mouse" dynamic between censors and VPN providers .

In emergency and disaster situations (such as floods, earthquakes, and climate-related crises), these mechanisms become particularly controversial. Reports on global shutdowns show that governments increasingly use throttling or filtering during crises and protests, which can unintentionally disrupt emergency communication systems . For example, internet disruptions during disaster or conflict situations may limit coordination between humanitarian agencies and affected populations. Research shows that shutdowns and filtering often occur during politically sensitive or crisis periods, despite claims of public safety justification . Technically, while VPN blocking is partially effective, users often bypass restrictions using obfuscation tools and encrypted tunneling protocols, making enforcement inconsistent.

International law does not prohibit regulation of VPNs but requires strict compliance with legality, necessity, and proportionality. The UN Human Rights framework emphasizes that internet restrictions must not undermine access to information, particularly in emergencies. The United Nations Human Rights Council has repeatedly stated that blanket shutdowns and broad censorship measures are generally incompatible with human rights obligations.

Technical censorship methods such as DPI and IP blocking are widely documented in censorship research, including studies on global filtering systems and surveillance infrastructures (Deibert et al., Citizen Lab research on internet control systems). Similarly, obfuscation research shows that censorship and circumvention operate in an ongoing technological arms race, where encryption and traffic masking evolve in response to blocking techniques (Dixon et al., 2016, Network Traffic Obfuscation and Automated Internet Censorship)

Best practice frameworks such as the Budapest Convention on Cybercrime reinforce that any cyber enforcement—including monitoring or restriction of encrypted traffic—must be targeted, proportionate, and subject to judicial safeguards

(Article 15). Similarly, the UN Guiding Principles on Business and Human Rights require ISPs and technology companies to avoid contributing to disproportionate restrictions, especially where access to communication tools is essential during humanitarian emergencies.

ISPs possess highly advanced technical capabilities to detect and block VPN traffic, particularly through DPI-based surveillance, IP filtering, and protocol fingerprinting. However, these mechanisms remain only partially effective due to rapid technological adaptation in VPN obfuscation tools. More importantly, their use during emergencies—especially floods, climate disasters, and conflict situations—raises serious concerns under international human rights law. Evidence shows that network restrictions often occur during crises, where access to communication is most essential, thereby creating a tension between state security objectives and humanitarian needs.

States should ensure that ISP-level VPN restrictions are strictly limited, lawful, and subject to judicial oversight, particularly during emergencies such as floods, climate disasters, and humanitarian crises. Blanket blocking, DPI-based mass surveillance, and internet shutdowns should be avoided where they interfere with emergency response and access to life-saving information.

ISPs must operate under transparent regulatory frameworks aligned with the ICCPR, UDHR, and technical safeguards recommended in the Budapest Convention. They should avoid indiscriminate filtering and instead apply narrowly tailored, rights-respecting measures. International oversight should be strengthened through the Office of the United Nations High Commissioner for Human Rights, the UN Human Rights Council, and cyber governance frameworks that monitor digital restrictions in crisis contexts.

Finally, states and companies should recognize that in disasters and climate emergencies, internet access is not optional infrastructure but a life-saving utility, and any VPN or network restriction must be evaluated against its humanitarian impact as well as its security justification.

4. How does restricting VPN access impact freedom of expression, digital security, and civic participation during crises?

Restricting VPN access during crises significantly affects freedom of expression, digital security, and civic participation, particularly in emergency environments such as political unrest, floods, and climate-related disasters. VPNs are widely used to bypass censorship and secure communication, and their restriction directly limits access to information protected under Article 19 of the ICCPR and Articles 12 and 19 of the UDHR. During emergencies, such restrictions become more severe as digital communication is essential for humanitarian coordination, disaster response, and civic awareness.

VPN restrictions directly reduce freedom of expression by preventing individuals from accessing blocked platforms and expressing dissenting views online. According to Freedom House, governments increasingly target VPNs and censorship circumvention tools as part of broader internet control strategies, especially during political unrest and crisis situations.[1] The Freedom on the Net 2025 report highlights that restrictions on anonymity tools, including VPNs, "pose a direct threat to online privacy, free expression, and access to information."[2] During emergencies, such as floods or protests, this can result in citizens being unable to access real-time information, emergency updates, or independent news sources, thereby weakening informational freedom.

VPN restrictions also weaken digital security, exposing users to surveillance, data interception, and cyber risks. Research shows that encrypted communication tools are essential for protecting users in environments where monitoring is widespread.[3] In crisis contexts—such as natural disasters or conflict situations—this becomes particularly critical, as citizens, journalists, and humanitarian workers rely on secure communication channels. Freedom House notes that governments often justify restrictions under "security or misinformation control," but such measures frequently have the unintended effect of limiting civic participation and suppressing digital mobilization.[4] For example, during emergencies

or unrest, blocking VPNs can prevent coordination of relief efforts, civic reporting, and public accountability.

International human rights law requires that any restriction on VPN use must meet the standards of legality, necessity, and proportionality under Article 19(3) ICCPR. The United Nations Human Rights Council has consistently emphasized that states should maintain internet access during emergencies and avoid arbitrary restrictions that undermine civic freedoms.[5] The Freedom on the Net 2025 report further recommends that governments should not impose blanket bans on communication tools and should instead use targeted, transparent, and lawful regulatory measures.[6] In disaster and climate emergency contexts, maintaining open access to information is considered essential for saving lives and ensuring effective governance.

In conclusion, VPN restrictions during crises significantly undermine freedom of expression, weaken digital security, and limit civic participation, particularly in emergencies such as floods, climate disasters, and political unrest. While states may justify such measures on security grounds, international standards and empirical evidence suggest that broad restrictions are disproportionate and harmful to public welfare. Governments should ensure that any limitations are narrowly tailored, time-bound, and subject to judicial oversight. ISPs and private actors should comply with human rights due diligence obligations under the UN Guiding Principles on Business and Human Rights, while states should prioritize maintaining open communication channels during emergencies to protect both civic space and humanitarian response capacity.

5.What policy alternatives can balance state security concerns with the protection of privacy and digital rights during emergencies?

Balancing state security concerns with the protection of privacy and digital rights during emergencies has become a central issue in contemporary legal and policy discourse. Emergencies such as terrorism, armed conflict, and political unrest often lead governments to adopt extraordinary digital measures, including surveillance expansion, internet shutdowns, and restrictions on communication technologies. While these measures are frequently justified as necessary for maintaining public order, they directly implicate fundamental human rights, particularly the right to privacy and freedom of expression as guaranteed under International Covenant on Civil and Political Rights (Arts. 17 & 19) and Universal Declaration of Human Rights (Arts. 12 & 19). According to the United Nations Human Rights Council, the same rights people enjoy offline must also be protected online, even during emergencies (UNHRC Resolution 32/13, 2016).

From the state's perspective, digital restrictions are often considered essential tools for ensuring national security and crisis management. Governments argue that enhanced surveillance allows intelligence agencies to detect and prevent terrorist activities and cyber threats in real time. During emergencies, the rapid spread of misinformation on digital platforms can incite panic and destabilize societies, thereby justifying temporary restrictions. For instance, Freedom House notes that governments increasingly impose platform restrictions and connectivity disruptions during crises to control information flows (Freedom House, Freedom on the Net 2025, p. 17). Additionally, states justify regulating encrypted tools such as VPNs on the grounds that such technologies may be exploited by criminal or extremist actors to evade law enforcement.

However, these justifications are counterbalanced by serious concerns regarding rights violations. One of the most significant risks is the expansion of mass surveillance, which often exceeds the limits of necessity and proportionality required under international law. The Office of the United Nations High Commissioner for Human Rights has emphasized that surveillance measures must not be arbitrary and should be strictly necessary and proportionate (OHCHR, The Right to Privacy in the Digital Age, 2018). Moreover, emergency powers are frequently misused to suppress dissent, targeting journalists, activists, and political opponents under the guise of national security. This undermines freedom of expression and democratic accountability.

Internet shutdowns, in particular, have been widely criticized for their disproportionate impact, disrupting economic activity, education, and access to essential services. Reports indicate that such shutdowns cause significant economic losses and harm digital inclusion (Freedom House, 2025; Access Now, #KeepItOn Report, 2024).

To reconcile these competing interests, several policy alternatives have been proposed that emphasize a rights-based approach to digital governance. Central to these alternatives is the principle of proportionality, which requires that any restriction on rights be lawful, necessary, and narrowly tailored. Instead of blanket shutdowns, governments can implement targeted and time-bound measures to address specific threats. Judicial and parliamentary oversight is also critical to ensure accountability; surveillance and digital restrictions should require prior authorization and be subject to independent review. Transparency further strengthens legitimacy, as governments should clearly disclose the legal basis, scope, and duration of any restrictions imposed during emergencies (OHCHR, 2018).

Another important policy alternative is the strengthening of data protection frameworks and the regulation—rather than prohibition—of encryption technologies and VPNs. The European Union provides a strong example through its General Data Protection Regulation (GDPR), which emphasizes user consent, accountability, and strict limitations on data processing. Similarly, countries like Germany demonstrate the importance of constitutional safeguards and judicial scrutiny in limiting surveillance powers, while Estonia offers a model of transparent and secure digital governance. At the international level, the United Nations has consistently affirmed that blanket internet shutdowns are incompatible with international human rights law and should be avoided.

In conclusion, while states have a legitimate duty to protect national security during emergencies, this objective must be pursued within the framework of human rights and the rule of law. Overbroad digital restrictions risk undermining democratic institutions, economic stability, and public trust. A balanced approach—grounded in legality, necessity, proportionality, transparency, and accountability—is essential to ensure that security measures do not erode fundamental freedoms.

Accordingly, several key recommendations emerge. States should enact clear legal frameworks defining the scope and limits of emergency digital powers in line with international obligations under the ICCPR. Independent oversight mechanisms, particularly judicial authorization for surveillance, must be strengthened. Blanket internet shutdowns should be prohibited in favor of targeted, evidence-based interventions. Governments should also promote the lawful use of encryption and VPNs while ensuring appropriate regulation. Finally, a multi-stakeholder approach involving civil society, private sector actors, and international organizations should be adopted to create a resilient digital governance framework that protects both security and fundamental rights.

Key References (for citation use)

Freedom House, Freedom on the Net 2025: An Uncertain Future for the Global Internet (Washington, DC: 2025) 17.

Office of the United Nations High Commissioner for Human Rights (OHCHR), The Right to Privacy in the Digital Age (2018).

United Nations Human Rights Council, Resolution 32/13 (2016).

Access Now, #KeepItOn: Internet Shutdowns Report 2024.

European Union, General Data Protection Regulation (GDPR), 2016.

Cases :

1.2025 P Cr. L J 233 [Lahore] Before Tariq Saleem Sheikh, J NASIRA ASHFAQ--Petitioner Versus DIRECTOR GENERAL SAFE CITIES AUTHORITY, PUNJAB and 6 others-- - Respondents Writ Petition No. 78006 of 2023, decided on 30th April, 2024.

Facts

The petitioner sought access to electronic data, including CCTV footage and call records, maintained by the Punjab Safe Cities Authority.

The request was grounded in the fundamental right to information under Article 19A of the Constitution of Pakistan. However, instead of following the prescribed procedure under the PSCA Electronic Data Regulations (EDR-16), the petitioner claimed direct access as a constitutional entitlement, arguing that denial of such access violated both domestic and international guarantees of freedom of information.

Holding (Decision)

The Lahore High Court dismissed the petition. It held that although the right to information is a fundamental right, it is not absolute and must be exercised in accordance with the law. The Court found that the PSCA Act 2016 and related regulations validly regulate access to electronic data. Since the petitioner failed to follow the legally prescribed procedure, no infringement of Article 19A was established.

Laws / Legal Principles

The Court reaffirmed that the right to information is recognized both domestically and internationally, including under instruments such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, which guarantee the freedom to seek and receive information. Within Pakistan, Article 19A elevates access to information to a fundamental right, obligating the State to provide information on matters of public importance.

However, the Court emphasized that this right is subject to two key limitations: it applies only to matters of "public importance," meaning issues affecting the public at large rather than private individuals, and it is subject to "reasonable restrictions" imposed by law. Such restrictions must be lawful, proportionate, non-arbitrary, and serve legitimate objectives like public safety, law enforcement, and protection of sensitive information.

The Court further held that under the PSCA framework, electronic data is collected primarily for investigation, prosecution, and maintenance of law and order, and access to such data is restricted to authorized persons through a specific procedure (EDR Form). Applying the principle of procedural exclusivity, the Court ruled that where a statute provides a particular method for obtaining relief, that method must be strictly followed.

The judgment establishes that the right to information under Article 19A is enforceable but procedurally regulated, and individuals must comply with statutory mechanisms to access restricted data.

2.JUDGMENT SHEET. IN THE ISLAMABAD HIGH COURT, ISLAMABAD. W.P. No.3720/2022 Pakistan Telecommunication Authority Versus Pakistan Information Commission, etc.

Facts

The case arose from a dispute between the Pakistan Telecommunication Authority and the Pakistan Information Commission regarding the interpretation of the right to information under Article 19A of the Constitution of Pakistan. The key issue revolved around whether only "citizens" (natural persons) could exercise this right, or whether corporate entities (such as companies or statutory bodies) could also qualify as applicants under the law. The Constitution uses different terms—"citizen" and "person"—for different fundamental rights, raising a question of interpretation.

Holding (Decision)

The Islamabad High Court held that although the Constitution distinguishes between "citizen" and "person," the right to information under Article 19A can be extended to corporate entities. Through a harmonious and liberal interpretation, the Court concluded that a company or incorporated body, being a legal person, can exercise the right to seek information. Therefore, such entities are entitled to make requests under the relevant information laws.

Laws / Legal Principles

The Court clarified that the Constitution deliberately uses different terms—"citizen" and "person"—and ordinarily, "person" has a broader meaning, including legal entities such as corporations, while "citizen" refers to natural persons as defined under the Pakistan Citizenship

Act, 1951. However, constitutional interpretation is not rigid. Courts adopt a broad, dynamic, and purposive approach, recognizing the Constitution as a living document.

The judgment emphasized that even where rights are granted specifically to citizens, courts have, through judicial precedent, extended such rights to corporate entities. This is partly because companies represent the interests of natural persons behind them, and denying rights to the entity may indirectly violate the rights of individuals. In appropriate cases, courts may also lift the corporate veil to ensure justice.

Applying the principle of harmonious interpretation, the Court noted that statutory terms like "citizen" and "applicant" (which includes "person") should be read together to avoid contradictions. Relying on precedents such as Mirza Shaukat Baig v. Shahid Jamil and Combined Investment (Pvt.) Ltd. v. Wali Bhai, the Court affirmed that legal provisions must be interpreted in a way that promotes rights rather than restricts them.

The judgment establishes that the right to information under Article 19A, though textually granted to "citizens," can be extended to corporate entities through liberal and purposive interpretation, enabling them to seek information as legal persons.

3. Case: Roman Zakharov v. Russia, Application No. 47143/06, European Court of Human Rights (Grand Chamber), Judgment of 4 December 2015.

Facts (Relevance to VPN Context)

In *Roman Zakharov v. Russia*, the applicant challenged Russia's **SORM surveillance system**, which allowed intelligence agencies to access telecom communications directly from service providers without strong judicial control. The system enabled large-scale interception of private communications, raising concerns about digital privacy in modern communication networks. In today's digital environment, users often rely on tools like **VPNs (Virtual Private Networks)** to protect themselves from similar forms of state or third-party surveillance.

Holding

The European Court of Human Rights held that Russia's surveillance framework **violated Article 8 of the ECHR** because it permitted disproportionate and potentially arbitrary interference with private communications. The Court emphasized that surveillance laws must include strict safeguards, judicial oversight, and effective remedies to prevent abuse. Importantly, the Court accepted that individuals may challenge surveillance systems even without proof of direct monitoring if the system itself creates a real risk of privacy intrusion.

Law Points (Connected to VPN Use)

The principles from this case directly relate to why VPNs are widely used today:

- **Right to privacy in digital communications (Article 8 ECHR):** The case confirms that electronic communications (calls, messages, internet traffic) are protected under privacy law. VPNs are used to strengthen this protection by encrypting internet traffic.
- **Need for safeguards against mass surveillance:** The Court criticized systems that allow broad, unchecked access to communications. VPNs act as a technical safeguard by making it harder for third parties to monitor user activity.
- **Transparency and lawful interception:** The judgment stressed that surveillance must be clearly regulated and not arbitrary. VPNs respond to concerns of unclear or excessive surveillance by creating encrypted tunnels that limit visibility of user data.
- **Risk of state or ISP-level monitoring:** The case highlights how telecom systems can enable hidden surveillance. VPNs are often used to reduce exposure to ISP monitoring or interception at network level.
- **Balance between national security and privacy:** The Court accepted surveillance for legitimate aims but required proportionality. Similarly, VPNs represent a user-driven response to maintain

privacy while accepting that lawful monitoring may still exist under strict legal standards.

The *Roman Zakharov v. Russia* judgment reinforces that mass or unchecked digital surveillance violates fundamental privacy rights under Article 8 ECHR. In modern practice, VPNs are widely used as a **technological response to the same privacy risks identified in this case**, helping users encrypt and protect their communications from potential surveillance or interception.

4. Cases:Szabó and Vissy v. Hungary (2016) – Link with VPN

Facts (Relevance to VPN Context)

In Szabó and Vissy v. Hungary, the applicants challenged Hungary's counter-terrorism laws that allowed the Counter-Terrorism Centre (TEK) to conduct secret surveillance, including interception of communications, without sufficiently strict judicial control. The concern was that such broad surveillance powers could expose citizens' online activity, messages, and digital communications to state monitoring. In today's digital environment, where most communication happens online, similar risks are often discussed in relation to internet monitoring and data interception, which is why tools like VPNs (Virtual Private Networks) are widely used.

Holding:

The European Court of Human Rights held that Hungary violated Article 8 of the European Convention on Human Rights. It found that the surveillance regime granted overly broad powers to security agencies without adequate safeguards, making it disproportionate and insufficiently controlled in a democratic society.

Law Points (Connected to VPN Use)

The principles from this case help explain the modern privacy concerns that lead many people to use VPNs:

Need for strict safeguards in digital surveillance:

The Court stressed that secret monitoring of communications must be tightly controlled. VPNs are used as a technical tool to reduce exposure of internet traffic to monitoring by encrypting data.

Protection of electronic communications:

The judgment confirms that online messages, browsing activity, and digital communication fall under Article 8 protection. VPNs function as a privacy layer for these communications.

Risk of broad and unchecked state access:

The Court criticized laws that give wide discretion to security agencies. VPNs are commonly used to limit visibility of user data at ISP or network level, reducing the impact of such broad surveillance possibilities.

Requirement of proportionality:

Even for national security, surveillance must be proportionate. VPN usage reflects a user-level response to maintain proportional privacy and security in digital communication.

Need for effective oversight:

The Court emphasized independent control over surveillance powers. In practice, VPNs do not replace legal oversight but act as a technological safeguard where users cannot rely solely on institutional protection.

Conclusion

Szabó and Vissy v. Hungary strengthens the principle that mass or overly broad surveillance of digital communications violates Article 8 ECHR unless strict safeguards exist. In the modern digital context, VPNs are often used as a privacy-enhancing tool to protect individuals from the kind of unchecked monitoring risks identified in this case.

Szabó and Vissy v. Hungary, Applications Nos. 37138/14, European Court of Human Rights (Second Section), Judgment of 12 January 2016.

5.Case Name: Film Production Companies v. LiquidVPN (USA, Federal Court – Florida)

Key Source: TFilm Production Companies v. LiquidVPN (USA, Federal Court – Florida)

Facts of the Case

A group of independent film production companies filed a lawsuit against VPN provider LiquidVPN, alleging that the service facilitated copyright infringement by its users. The plaintiffs argued that the company not only enabled piracy

but also promoted its service as suitable for torrenting and bypassing restrictions. The court ultimately issued a default judgment of approximately $15 million after the defendant failed to respond to the legal proceedings. Following the judgment, the company became defunct, and the owner reportedly did not satisfy the damages awarded.

Legal Issue

The central issue was whether a VPN provider can be held liable for copyright infringement carried out by its users, particularly in situations where the provider is alleged to have encouraged or facilitated such activity and failed to participate in court proceedings.

Holding / Court Action

The court granted a default judgment against the VPN-related entities, establishing civil liability. Subsequent enforcement efforts included attempts to seize assets and compel payment. The plaintiffs also pursued contempt of court motions, seeking measures such as possible detention of the owner to enforce compliance. These actions represent civil enforcement mechanisms rather than criminal prosecution for piracy.

Legal Principles Involved

The case involves several key legal principles, including secondary liability for copyright infringement, the inducement theory (where encouraging infringement can establish liability), enforcement of default judgments, and the use of contempt of court powers to ensure compliance with judicial orders.

China Reference (Related but Different Context)

In contrast, China has pursued separate cases involving piracy and VPN-related activities under stricter legal frameworks. These include criminal prosecutions of individuals operating piracy platforms and actions against unauthorized VPN services used to bypass state internet controls. While these cases involve similar subject matter, they differ significantly from the LiquidVPN case in their reliance on direct criminal enforcement.

Key Takeaway

The LiquidVPN case in the United States illustrates how VPN providers may face civil liability, financial penalties, and enforcement actions if they are found to have facilitated or encouraged copyright infringement and fail to comply with court proceedings. By comparison, cases in China demonstrate a more direct criminal enforcement approach toward piracy and unauthorized VPN operations. Freak reporting / US District Court filings (Florida)

Landscape of Vpn Access and Restrictions of Different Countries:

(VPNs) have sparked intense debate regarding their legal status across various nations. On the surface, the question of whether VPNs qualify as legal may seem clear-cut. However, in practice, their classification proves nuanced, fluctuating substantially depending on geographic location and political climate.

In a majority of Western countries, utilizing VPN software remains fully lawful. The United States and the United Kingdom serve as prominent examples, upholding VPNs as legitimate tools for residents aiming to secure their digital privacy and bypass content geo-restrictions.

But the picture differs dramatically under authoritarian-leaning regimes. Both Russia and China have instituted outright bans on non-state-sanctioned VPN services as integral parts of their extensive internet censorship and surveillance apparatuses. Citizens of these countries face prosecution for unsanctioned VPN access.

The legal conversation grows even more complex considering how VPN use intersects with other potential infractions. Even in localities where virtual private networks are legal, they may shield illicit activities like hacking and copyright infringement. The VPN itself does not inherently violate the law but becomes an instrument for unlawful behaviors.

America:

Using a VPN does not in itself lead to legal consequences, and it can contribute to online privacy and security. VPN services are widely

available and can be downloaded from provider websites or app stores.

Some providers are based in the US, including Private Internet Access and IPVanish.

Research indicates that the US VPN market was valued at approximately $17.88 billion in 2024 and is projected to exceed $20 billion in 2025. Estimates suggest that around 43% of Americans use a VPN, with potential for further growth.

There have been discussions in some states regarding restrictions on "circumvention tools." For example, lawmakers in Michigan have proposed measures as part of a "public morals" bill. At present, widespread prohibition of VPNs in the US appears unlikely, though legislative developments continue to be monitored.

Although VPN use is not illegal, certain activities may violate the terms of service of online platforms. One example involves streaming services such as Netflix, which attempt to restrict access to region-specific content. Circumventing these restrictions may breach platform policies, potentially resulting in account limitations, though not criminal penalties.

Some websites or services may not function properly when accessed through a VPN. Platforms like YouTube and certain online banking systems may limit access or performance. In many cases, switching servers or adjusting settings can resolve these issues.

VPNs do not make illegal activities legal. Actions that are unlawful without a VPN remain unlawful when using one. While authorities may request data from VPN providers, the extent of available information depends on company policies, such as no-logs practices and transparency reporting.

VPNs are often used for privacy and security purposes. For example, they can help protect data on public Wi-Fi networks by encrypting internet traffic. They may also be used to bypass network-level restrictions in workplaces or educational institutions, subject to relevant policies.

In addition, various US states have introduced age-verification laws requiring identity checks to access certain online content. These processes may involve sharing personal data with third parties, raising concerns about data security. Regulatory approaches vary by state, and user responses—including the use of VPNs to change apparent location—may differ accordingly.

In summary, VPNs are legal in the United States and widely used for legitimate purposes. However, their use does not exempt individuals from legal responsibilities or compliance with service agreements.

In essence, VPN legality hinges greatly on the motivations of national governments. Some regard unchecked VPN use as a threat to centralized control, while others champion virtual private networks as a vital pathway to online liberties. With the internet fracturing into varying grades of openness, understanding the true legal landscape for VPNs demands recognition of these deeper political undercurrents worldwide.

Virtual private networks (VPNs) face mounting restrictions or comprehensive bans under a growing list of authoritarian-leaning governments worldwide. As these regimes continue tightening controls over online activity, the legal status of VPNs remains in constant flux. Here are examples of regimes where VPN use is illegal or regulated.

China

In China, no formal law prohibits VPN usage outright. However, the government actively blocks access to major VPN providers through sophisticated firewall systems. Approved VPNs must contain backdoors granting state agencies access to traffic data.

Periodic crackdowns also target non-approved services. Fines for using unapproved VPNs crop up erratically. According to a recent analysis, China blocks VPN websites over 73% of the time – more than any other country.

Still, the unlikely prospect of a total Chinese ban on VPNs persists due to reliance on the tools by international corporations.

Russia

Russia stands as another prime example of an authoritarian state wielding VPN restrictions as a censorship tool. Though technically legal, Russian VPN policies have grown increasingly prohibitive over recent years.

The state telecommunications watchdog routinely strong-armed major providers into blocking

banned websites, rendering unauthorized options the only way for citizens to access banned content. And following Russia's invasion of Ukraine in February 2022, the nation saw a massive surge in VPN use along with intensified crackdowns.

By March 2022, prominent services like ExpressVPN and Nord VPN had been blocked entirely from the Russian market due to mounting government pressures causing them to abandon Russian servers. Still, Russian journalists, protestors, and other activists accept the risks of unauthorized VPN usage as a needed shield against state scrutiny.

Belarus

The Belarusian regime has spearheaded harsh restrictions against virtual private networks (VPNs) as part of systematic efforts to limit online freedoms since 2015.

Beyond directly obstructing VPN traffic, authorities have compelled internet service providers to retain users' browsing data for government surveillance. Accusations have also emerged regarding the state's use of advanced monitoring systems to identify and disrupt VPN connections.

In a bid to suppress political dissent and restrict free speech, Belarus has concurrently enacted bans on secure messaging services like Telegram and Signal. Combined with VPN blocking, this denies citizens access to encrypted communication tools and the anonymizing protection of virtual private networks.

North Korea

North Korea stands alone as the most extreme case globally of VPN prohibition under an isolationist dictatorship. Virtual private networks remain expressly illegal within the country's borders. The regime maintains strict control over all internet access, restricting citizens to only a tightly monitored national intranet called Kwang Myong. Through pervasive censorship and surveillance measures, North Korea completely prevents external information flows. The government regards any attempt to circumvent its firewalls using VPNs or other tools as a punishable crime threatening its totalitarian control. Allowing citizens to access outside news constitutes an ideological threat in the state's eyes.

As a result, North Korean law threatens harsh penalties for anyone caught utilizing virtual private networks or similar circumvention technology. The VPN ban represents just one component in the regime's vast apparatus aimed at propagandizing the populace and eliminating foreign influences. Along with restrictions on outside telephone lines, North Korea's VPN prohibition further isolates citizens from the global community.

Legal Considerations When Using VPNs to Access Restricted Content:

As earlier mentioned, the legal implications of using VPNs for these purposes remain ambiguous across various nations. As such, those seeking to access prohibited content via VPN must carefully evaluate associated risks and laws.

You must also consider laws governing VPN server locations. Connecting to countries with minimal censorship raises fewer legal concerns compared to regions where authoritarian regimes tightly control nets. Restrictive states increasingly punish VPN access as a direct threat to their ideological control.

Furthermore, while VPNs may be legal, they can still shield illegal activities like piracy. Access copyrighted material without proper permissions, and you risk harsh penalties. Tread carefully regarding the type of content you access via VPN across all jurisdictions.

As technology progresses and the internet becomes increasingly integral to economics, politics, and society, navigating the legal landscape around tools like VPNs grows in complexity. On one hand, we can hope that the recognition of digital privacy as a human right becomes more widespread, leading more democratic nations to legalize and protect virtual private networks.

However, authoritarian regimes seem equally determined to prohibit VPN access as online censorship and surveillance rise globally. Additionally, factors like escalating cyber warfare and shifts in copyright law enter the mix, raising new questions around VPN usage even in traditionally open societies. There may be

pressures to restrict access in the name of national security or corporate interests.

In essence, the legal status of virtual private networks remains highly volatile across the world – subject to the pushing and pulling between demands for digital liberties versus desires for control. The coming years will determine which forces gain the upper hand in key region.

Domestic Legislative Frame work regard VPN (Privacy, VPNs & Emergency Situations)

1.Pakistan Telecommunication (Re-organization) Act, 1996

The Pakistan Telecommunication (Re-organization) Act, 1996 establishes the core regulatory structure governing telecommunications services in Pakistan, including those relevant to VPNs. Section 21 introduces a mandatory licensing regime, providing that no person may offer telecommunication services without obtaining a licence from the Pakistan Telecommunication Authority (PTA). This is reinforced by Section 5(2)(c), which grants PTA the authority to issue, renew, and revoke licences, while Section 5(2)(a) empowers it to regulate telecommunication systems and services more broadly. Together, these provisions give PTA wide discretion in controlling digital communication infrastructure.

Section 23 further strengthens this framework by allowing PTA to impose licence conditions, including technical requirements, operational limitations, and security compliance obligations. Enforcement is addressed under Section 31, which makes unlicensed operation a legal offence and permits penalties such as service blocking or other regulatory action. These provisions collectively form the statutory basis through which digital services—including VPN-related activities—can be controlled within Pakistan.

Direct Regulatory Framework Applied to VPNs

Within this legal structure, VPNs are treated as part of data communication services. Under the regulatory framework, the scope clause explicitly includes data transmission services, bringing VPNs within the ambit of telecom regulation. As a result, any entity providing VPN services is required to obtain a relevant licence—typically a class licence—making licensing the primary legal route for lawful VPN operation.

Security and compliance obligations are central to this framework. Providers must adhere to lawful access requirements and cooperate with authorities when legally mandated, reflecting the state's emphasis on surveillance and national security considerations. Enforcement provisions allow PTA to suspend or revoke licences and take action against violations, ensuring regulatory compliance.

Overall, this framework demonstrates that VPN regulation in Pakistan is not governed by a single explicit law on VPNs but is instead derived from broader telecommunications legislation, which subjects such technologies to licensing, monitoring, and enforcement mechanisms.

2. Class License for the Provision of Data Services in Pakistan

Class Licensing and Registration Regulations, 2007 with latest amendment, 2025

It gives mechanism for vpn service licensing.

3.Prevention of Electronic Crimes Act, 2016

Section 37 Allows authorities to:

- regulate or restrict digital services when necessary . Supports the regulatory control environment for encrypted services like VPNs

4.Critical Telecom Data and Infrastructure Security Regulations, 2025,

1. Chapter VI (Access Control), Clause (g)(i) of Sub-regulation (2) of Regulation 27;
2. Clause (g) and Clause (c) of Sub-regulation (5) (Remote Access Security) of Regulation 27;
3. and Clause (g) of Sub-regulation (2) of Regulation 40.

5. CVAS Information Memorandum in web page of PTA.

It give detailed schedules, agreements format, general conditions Class Value Added Licensed Services(CVALS) and key definition include "VPN" and two system data and voice system :/Users/DELL/AppData/Local/Temp/ad87ac56-f493-4b48-bc83-bd029c777016_2024-07-19-revised_cvas_im_070319.zip.016/revised_cvas_im_070319.pdf

International Legal & Technical Framework (Privacy, VPNs & Emergency Situations)

1. Core International Human Rights Law

Core international human rights law provides a clear foundation for the protection of privacy, even in times of crisis. The Universal Declaration of Human Rights establishes, under Article 12, that no one should be subjected to arbitrary interference with their privacy, family, home, or correspondence, laying an important—though non-binding—global standard. This principle is given binding legal force through the International Covenant on Civil and Political Rights, to which Pakistan is a party. Article 17 of the Covenant guarantees the right to privacy and permits restrictions only when they are lawful, necessary, and proportionate. Furthermore, Article 4 of the ICCPR allows states to temporarily derogate from certain obligations during a public emergency threatening the life of the nation, but such measures must meet strict conditions of necessity, remain non-discriminatory, and cannot undermine the core essence of fundamental rights. Together, these instruments establish that even in emergencies, state actions—such as restricting digital tools like VPNs—must be carefully justified within a robust human rights framework.

2. United Nations Digital Rights Framework

The United Nations Human Rights Council has affirmed the principle that the same rights people enjoy offline must also be protected online, as recognized in its 2016 resolution. This principle extends key protections to the digital sphere, including the right to privacy, freedom of expression, and access to information. Complementing this, the UN Special Rapporteur on Freedom of Expression has taken a strong position in favor of encryption and anonymity tools—within which VPNs are generally understood to fall—emphasizing that such technologies are essential for safeguarding secure communication and protecting users from unlawful surveillance. The Special Rapporteur has consistently argued that states should refrain from imposing arbitrary or blanket bans on these tools. This position is further reinforced in the 2022 report of the Office of the United Nations High Commissioner for Human Rights, Internet Shutdowns: Trends, Causes, Legal Implications and Impacts on a Range of Human Rights (A/HRC/50/55), which highlights that restrictions on digital access and tools must comply with strict human rights standards, particularly the principles of legality, necessity, and proportionality (para. 51).

3.European Human Rights Framework

The European Convention on Human Rights provides a robust regional framework for protecting fundamental rights in both offline and online contexts. Article 8 guarantees the right to privacy, while Article 10 protects freedom of expression; any restrictions on these rights must meet strict conditions of legality, necessity, and proportionality. Building on this, the Council of Europe, through Recommendation CM/Rec(2016)5, emphasizes the importance of maintaining internet freedom, explicitly opposing blanket blocking of online services and supporting the use of secure communication tools. Further strengthening this framework, Convention 108+ establishes advanced standards for data protection, requiring states to implement safeguards against unlawful data processing and intrusive surveillance. Together, these instruments reinforce the principle that even in digital environments and emergency situations, limitations on technologies such as VPNs must be carefully justified and aligned with fundamental rights protections.

Roman Zakharov v. Russia

- Condemned mass surveillance systems
- Set strict safeguards for interception

Szabó and Vissy v. Hungary

- Surveillance must be strictly necessary and proportionate

4. Cybersecurity & Internet Governance Standards (Technical Layer)

At the technical layer, cybersecurity and internet governance standards play a crucial role in shaping how digital tools like VPNs operate within legal and security frameworks. The Budapest

Convention on Cybercrime, the first international treaty addressing cybercrime, establishes cooperation mechanisms and criminalizes acts such as illegal access and data interception, while allowing states to regulate cyber tools subject to appropriate legal safeguards. Alongside this, the Internet Engineering Task Force develops and maintains essential internet security protocols, including IPsec, which forms the backbone of many VPN systems, and TLS encryption, both of which ensure secure and private communication across networks. Complementing these technical standards, ISO/IEC 27001 provides a globally recognized framework for information security management, emphasizing the protection of confidentiality, integrity, and the overall security of data systems. Together, these instruments demonstrate that while cybersecurity requires regulation, it also fundamentally depends on strong encryption and secure communication technologies that underpin privacy and trust in the digital environment.

Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights Report of the Office of the United Nations High Commissioner for Human Rights(A/HRC/50/55) : VPN blockage by internet services providers internally.

Comment no 51. Disruptions, in particular the targeted blocking of access to platforms, often require the use of additional technology to monitor traffic and disrupt access to specific channels. In particular, researchers have documented the frequent use of deep packet inspection technology to conduct surveillance and block access to communications channels in support of repressive measures. Even if those tools may be used for legitimate purposes, such as restricting access to illegal content, abuses of deep packet inspection for conducting surveillance and implementing shutdowns are well documented, 81 with some tools being marketed explicitly with indications on their effectiveness in selectively blocking access to applications such as virtual private networks or social media.82 Technology companies should reflect such concerns in their human rights and other policies.

Conclusion:

VPN use during emergencies plays a significant yet inherently limited role in safeguarding the rights to privacy, access to information, and freedom of expression. Across diverse contexts—including conflict zones, political unrest, and climate-related disasters—VPNs function as critical tools that enable individuals to bypass censorship, maintain secure communication, and access essential information. However, their effectiveness is constrained by increasing state regulation, technical blocking mechanisms, and pressures placed on private companies to comply with restrictive legal frameworks.

International human rights law, particularly Article 19 of the International Covenant on Civil and Political Rights (ICCPR) and Articles 12 and 19 of the Universal Declaration of Human Rights (UDHR), establishes that any restriction on digital access must meet the cumulative requirements of legality, necessity, and proportionality. Evidence from global practice demonstrates that blanket VPN bans, internet shutdowns, and indiscriminate surveillance measures rarely satisfy these standards and often produce disproportionate harm, especially during emergencies when access to information is essential for safety, humanitarian coordination, and civic participation.

At the same time, the role of private actors—including internet service providers and technology companies—reveals a structural tension between compliance with state directives and the responsibility to respect human rights under frameworks such as the UN Guiding Principles on Business and Human Rights. While technical mechanisms such as deep packet inspection and IP blocking enhance state capacity to restrict VPN usage, they remain only partially effective due to ongoing technological adaptation and raise serious concerns regarding mass surveillance and overreach.

From a governance perspective, international oversight remains fragmented. Institutions such as the United Nations Human Rights Council and the Office of the United Nations High Commissioner for Human Rights provide normative guidance but lack binding enforcement

powers. Although the International Criminal Court may indirectly address extreme cases involving communication suppression in conflict settings, there is no dedicated global mechanism specifically tasked with enforcing digital rights.

Overall, the analysis demonstrates that while VPNs contribute to digital resilience, they cannot substitute for a comprehensive, rights-based legal and policy framework. Ensuring the protection of digital rights during emergencies requires coordinated action by states, private actors, and international institutions grounded in human rights principles.

Recommendations:

- **State Responsibilities:**

States should ensure that any restriction on VPN use or digital communication tools strictly complies with international human rights standards, particularly the principles of legality, necessity, and proportionality. Blanket internet shutdowns and indiscriminate VPN bans should be avoided, especially during emergencies such as conflicts, political unrest, floods, and climate-related disasters. Instead, governments should adopt narrowly tailored, time-bound measures supported by clear legal frameworks and subject to independent judicial oversight.

- **Protection of Access During Emergencies:**

Governments should recognize internet access as a critical infrastructure during emergencies. Policies should prioritize maintaining connectivity to support humanitarian response, disaster coordination, and access to life-saving information. Any limitations imposed must be carefully assessed against their humanitarian impact.

- **Corporate Responsibility and Accountability:**

Technology companies and internet service providers should align their operations with the UN Guiding Principles on Business and Human Rights. This includes conducting human rights due diligence, resisting disproportionate or unlawful state requests where possible, and ensuring transparency in how restrictions on VPNs and communication tools are implemented.

- **Strengthening Legal and Regulatory Frameworks:**

States should develop clear and predictable legal frameworks governing digital restrictions, including safeguards against abuse. Regulation of VPNs and encryption technologies should focus on lawful oversight rather than prohibition, ensuring that privacy-enhancing tools remain accessible for legitimate use.

- **Enhancing International Oversight:**

There is a need to strengthen coordination among international mechanisms, including the United Nations Human Rights Council, the Office of the United Nations High Commissioner for Human Rights, and regional human rights courts. Consideration may also be given to developing a specialized global framework or institution dedicated to digital rights governance and accountability.

- **Promoting Transparency and Multi-Stakeholder Governance**

States should ensure transparency regarding the scope, duration, and legal basis of any digital restrictions imposed during emergencies. A multi-stakeholder approach involving governments, private sector actors, civil society, and international organizations should be adopted to ensure balanced and accountable digital governance.

- **Technical Safeguards and Proportional Enforcement**

Technical measures such as traffic monitoring or VPN regulation should be applied in a targeted and proportionate manner, avoiding mass surveillance practices. Frameworks such as the Budapest Convention on Cybercrime should guide the implementation of safeguards, ensuring that enforcement actions remain lawful and rights-compliant.

REFERENCES:

Reji Kurien Thomas, VPN Solutions: Balancing Productivity and Security for Business (DBA diss., Swiss School of Business and Management Geneva, 2023), 42–48.

Freedom House, Freedom on the Net 2025: An Uncertain Future for the Global Internet (Washington, DC: Freedom House, 2025), 17.

UN Special Rapporteur on Myanmar Reports (2021–2024). And Access Now. Digital Repression in Myanmar, 2022–2024.

United Nations Human Rights Council and Office of the High Commissioner for Human Rights, Reports on the Situation in the Occupied Palestinian Territory, 2022–2025.

Computer Science > Cryptography and Security [Submitted on 9 Jul 2019 (v1), last revised 10 Jul 2019 (this version, v2)]ICLab: A Global, Longitudinal Internet Censorship Measurement Platform Arian Akhavan Niaki, Shinyoung Cho, Zachary Weinberg, Nguyen Phong Hoang, Abbas Razaghpanah, Nicolas Christin, Phillipa Gill

Wendzel, Steffen & Volpert, Simon & Zillien, Sebastian & Lenz, Julia & Rünz, Philip & Caviglione, Luca. (2025). A Survey of Internet Censorship and its Measurement: Methodology, Trends, and Challenges. 10.48550/arXiv.2502.14945.

Letcher, Terry, and Andria Hayes-Birchler. "Is Remote Measurement a Better Assessment of Internet Censorship than Expert Analysis? Analyzing Tradeoffs for International Donors and Advocacy Organizations of Current Data and Methodologies." Data & Policy 5 (2023): e9. https://doi.org/10.1017/dap.2023

Leonie Maria Tanczer, Ronald J Deibert, Didier Bigo, M I Franklin, Lucas Melgaço, David Lyon, Becky Kazansky, Stefania Milan, Online Surveillance, Censorship, and Encryption in Academia, International Studies Perspectives, Volume 21, Issue 1, February 2020, Pages 1–36, https://doi.org/10.1093/isp/ekz016

George Phillips. Staff Writer at Tom's Guide, covering VPNs, privacy, and cybersecurity news, with a focus on digital rights and censorship and their relationship with politics. Chicago: Tom's Guide. Interests include music, Star Wars, and karate.

https://www.legalreader.com/legality-of-virtual-private-networks-vpn/.

Office of the United Nations High Commissioner for Human Rights, Internet Shutdowns: Trends, Causes, Legal Implications and Impacts on a Range of Human Rights, A/HRC/50/55 (United Nations, 2022), para. 51.