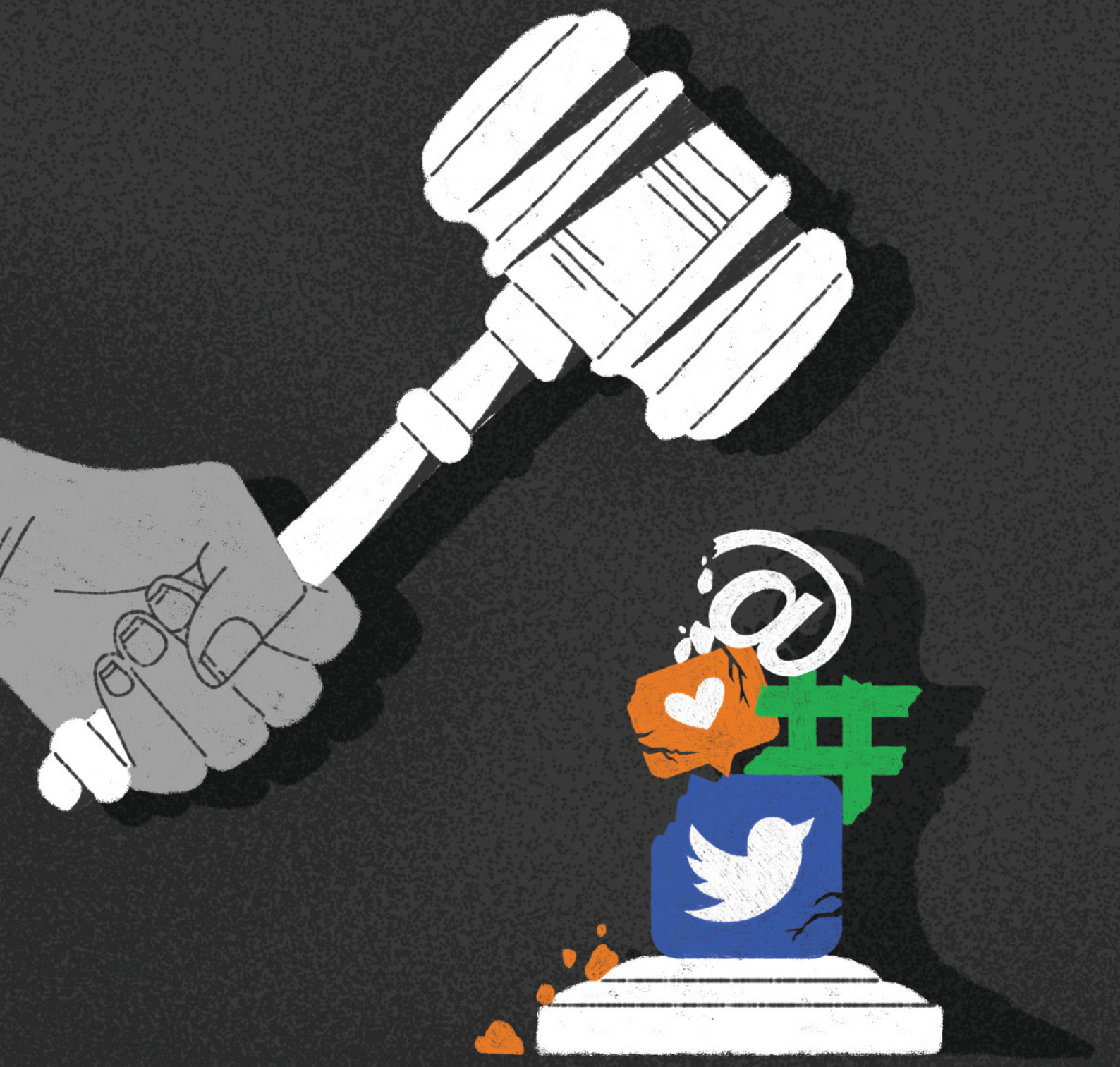
# Jurisprudence shaping digital rights in South Asia

CYRILLA APC



# JURISPRUDENCE SHAPING DIGITAL RIGHTS IN SOUTH ASIA

**Authored by**
Divya Srinivasan and Gayatri Khandhadai

**Proofread by**
Lawrence Garcia

**Designed by**
Kritika Trehan

Jurisprudence Shaping Digital Rights in South Asia
November 2020
ISBN 978-92-95113-36-7
APC-202011-CIPP-R-EN-DIGITAL-326

# INDEX

## Acknowledgements

The Association for Progressive Communications developed this research as part of the CYRILLA project[1] that seeks to provide comprehensive resources on global digital rights laws.

This research has been carried out by Divya Srinivasan[2] and Gayatri Khandhadai.[3] We are thankful to Chinmayi Arun for guiding the initial conception and methodology for undertaking the research. Ashwini Natesan and Rifat Khan provided key research assistance in locating relevant case laws from Sri Lanka and Bangladesh respectively.

Several experts from South Asia provided us their valuable time and inputs in helping identify and analyse the cases. We thank them for their work and support. Resources developed by organisations such as Media Matters for Democracy (Pakistan), Body and Data (Nepal), LIRNEasia (Sri Lanka), Internet Democracy Project (India), Software Freedom Law Centre (India) and Internet Freedom Foundation (India) were greatly helpful for understanding developments and the ecosystems in their countries.

We would also like to thank all the participants in the #DigitalLawsAsia Twitter Campaign organised by CYRILLA and the Association for Progressive Communications in June 2020 for their knowledgeable insights which guided our understanding and analysis of the issues involved.

Our work relies extensively on information relating to case laws on digital rights already available on the CYRILLA database on Global Digital Rights Law, as well as Columbia University's Global Freedom of Expression database.

We are also thankful to Lawrence Garcia for proofreading and editing the report. Kritika Trehan developed the art design and cover for the report.


[1] https://cyrilla.org/en/

[2] Divya Srinivasan is a human rights lawyer and activist. Her work focuses on issues relating to gender and free speech and she has worked as research consultant with the Association for Progressive Communications for mapping ICT laws in selected Asian countries as part of the CYRILLA project.

[3] Gayatri Khandhadai is a lawyer with a background in international law and human rights, international and regional human rights mechanisms, research and advocacy. She works with the Association for Progressive Communications as the Asia Regional Policy Coordinator.

## Abbreviations

CJI - Chief Justice of India

CrPC - Code of Criminal Procedure 1973 (India)

DoT - Department of Telecommunications, Government of India

DSA - Digital Security Act 2018 (Bangladesh)

FoE - Freedom of Expression

HRC - Human Rights Council

ICCPR - International Covenant on Civil and Political Rights

ICESCR - International Covenant on Economic, Social and Cultural Rights

ICT - Information and Communications Technology

ICT Act - Information and Communication Technology Act 2006 (Bangladesh)

IPC - Indian Penal Code

IT - Information Technology

NADRA - National Database and Registration Authority

PECA - Prevention of Electronic Crimes Act 2016 (Pakistan)

PTA - Pakistan Telecommunication Authority

PUBG - Player Unknown's Battle Grounds

UDHR - Universal Declaration of Human Rights

UIDAI - Unique Identification Authority of India

UN - United Nations

UNGA - United Nations General Assembly

WP - Writ Petition

## Overview and reflections

Jurisprudence developed by courts are central to the understanding, application and implementation of laws. Information and communication technologies (ICTs) have irreversibly impacted every walk of personal and public life, including how courts function and deliberate on rights. Given the number of ICT specific laws and policies that have developed, in some cases hastily, over the past decade, the views of courts are ever more important. The rise of the internet and its impact on governments and governance processes has caused states to ring in various laws and extend offline regulations to online spaces. We have been faced with challenges that existed in our societies prior to the internet, but now, the forms they take and the speed of proliferation of content is unimaginable.

This is further complicated in regions which are inhabited by large populations of diverse linguistic, ethnic and religious groups. South Asia, which shares a broad history of colonisation and current socio political and economic challenges, has much to contribute to the evolution of the internet and its governance. Therefore, the study focuses on the South Asian sub-region and explores selected cases relating to digital rights from Bangladesh, India, Nepal, Pakistan and Sri Lanka.

The objective of this report is to make available a resource that can be used by lawyers, policy experts and civil society to gauge the trajectory of judicial discourse on digital rights and use this as a tool to advocate for greater protections. This is not a compendium of all cases relating to the topics dealt with.

For studying the cases, the researchers developed a workbook[4] that collated decisions available in online databases including CYRILLA and the Columbia University's Global Freedom of Expression database. Resources developed by national groups on the state of digital rights in their countries provided critical guidance. The cases selected naturally fell into three categories of Access, Privacy and Freedom of expression. A key challenge faced, while developing this research, relates to collection of data. In many of the countries (except India), case laws are not easily available on free, open and searchable case law databases. Judgements and orders are often not available or are difficult to access on official court websites. In some countries, many of the decisions or orders relating to digital rights were not reported and thus were inaccessible. In a few instances, particularly for Nepal and Pakistan, some judgements were not available in English and reliance had to be placed on the analysis of the judgement provided by researchers with knowledge of the local language.

The countries selected share similar legal systems and challenges in the exercise and enjoyment of digital rights. Some of the issues covered by the report include discussions around access to the internet and its impact on other rights as well as network shutdowns. Judicial pronouncements in relation to privacy, surveillance, national identity programmes, data protection have been analysed across jurisdictions. A significant number of cases studied related to challenges surrounding freedom of expression.

Judgements on access to the internet indicate that there is some recognition of the central role the internet and connectivity play in the lives of all individuals. Cases discussed in this report include judgements relating to equitable telecast rights, instances where use of mobile phones were prohibited, providing limited internet access to prisoners, recognition of medium of information being protected and multiple cases on network shutdowns. However, judgements on internet shutdowns have varied in terms of decisions on procedural propriety, legality and ultimately in providing actual remedy to the people most affected by it. Despite the developing jurisprudence on network shutdowns, ground realities remain unchanged with repeated imposition of disruptions in the region.

Decisions relating to privacy dealt with fundamental questions of whether privacy is protected as a constitutional or fundamental right, validity and regulation of state surveillance mechanisms, data protection and privacy concerns relating to national identity programs. The cases examined included advisory opinions and pronouncements on the right to privacy as a fundamental right, disclosure of personal

[4] https://docs.google.com/spreadsheets/d/1hbolMtuQWTukQ-cw38W8uL2_4KVfUDR9xI6GcBunhHc/edit?usp=sharing

information, tapping of phone conversations, surveillance of voice and text messages in communications and the validity of the national identity programme in India.

While there is broad recognition for the principles evolved around freedom of expression, courts have largely ruled in favour of censorship and criminalisation. Even in cases where the courts have shunned state action, reparations have not been made available to petitioners in an adequate manner. Fear of uncertainty is pushing intermediaries to proactively takedown content that is under dispute. Cases discussed in the report relate to state powers and validity of blocking; restrictions and criminalisation of political, artistic and sexual expression; the use of blasphemy provisions to criminalise speech; actions to curb hate speech online; use of defamation and contempt of court provisions against speech online and directions on intermediary action or liability.

Overall, courts have been more deferential to state power and concerns of national security or public order over defending individual and fundamental freedoms. However, important jurisprudence has also emerged from the region limiting the power of governments to the imposition of network shutdowns, legality of vague provisions governing freedom of expression and the need for robust data protection mechanisms. South Asian courts have also developed strong jurisprudence delineating the scope of fundamental rights to privacy and freedom of expression and have made it clear that these constitutional protections apply to the online realm. It is hoped that these landmark cases are merely laying the groundwork for the development of robust jurisprudence upholding digital rights and holding states accountable for violating these rights.

While in several instances of litigants have referred to international developments and law on the subject, in few judgements courts have reflected on them. An over reliance on concerns relating to security have driven courts away from adopting a rights-based approach in deliberating on the issues. The protectionist approach of courts is particularly evident in orders relating to blocking and filtering which has had far reaching and, in some cases, undesirable consequences. Traditional jurisprudence on freedom of expression has been applied in some cases to render state action as illegal. However, the zeal for protecting offline freedoms is yet to be applied to online spaces.

There is inconsistency in the application of principles across jurisdictions nationally and within the region. For instance, the Indian Supreme Court rendered a landmark decision laying out the contours of the right to privacy, but failed to apply many of these very principles in its subsequent decision upholding the validity of the Aadhaar scheme. Despite progressive decisions in some cases, enforcement remains insufficient.

Key judgements, especially in relation to network shutdowns have remained mere recognition of a violation with elaboration of first principles with little remedy provided that could restore or provide reparations to the victims. Progressive jurisprudence within the region could play an important role in informing similar cases in other jurisdictions. However, this is yet to be evidenced.

While this report looks at developments in five countries in South Asia with a specific focus on access, privacy and freedom of expression, several other issues warrant attention. Laws and jurisprudence relating to intermediary liability, misinformation, anti-trust, algorithmic discrimination, community networks, taxation, information sovereignty, physical infrastructure, spectrum allocation, sharing and licensing and cross-border data transfers are swiftly evolving. Future studies could focus on these issues and adapt the study to other regions or countries.

Based on the analysis, the primary need relates to courts evolving a more consistent and rights based/friendly approach to the issues before them. Access to the internet requires a more holistic approach and recognition as a legal right, similar to other instances where courts have recognised rights derived from the guarantees in national constitutions. Network shutdowns require greater oversight from judicial bodies with a specific goal of ensuring that other alternatives, which are more appropriate are exhausted.

Jurisprudence relating to digital privacy and surveillance in South Asia is still at a very nascent stage. It is apparent that the jurisprudence of South Asian courts in relation to digital privacy needs to keep up with evolving threats proliferating from State and non-State actors, including the increasing use of extensive and sophisticated surveillance systems by States. There are currently cases pending before the Indian Supreme Court challenging the constitutional validity of electronic

surveillance framework,[5] before the Sri Lankan Supreme Court challenging a planned central database which would profile all citizens[6] and before the Lahore High Court regarding the alleged use of a digital spying tool (Finfisher) and digital surveillance by the State.[7] While it remains to be seen the extent to which courts will protect the right to digital privacy in these cases, the jurisprudence till date indicates that constitutional right to privacy has not been implemented in a manner which provides strong on ground protection for citizens.[8]

Courts could examine the impact of expansive orders for blocking or filtering of online content on the grounds of obscenity, blasphemy, religious harmony and the like which have been ordered in multiple instances. There is a palpable need for more transparency on the grounds for blocking and filtering and the means through which it is carried out.

International bodies, especially the Human Rights Council and special rapporteurs dealing with different thematic areas must pay greater attention and contribute to ongoing litigation on key issues to provide critical perspectives. Greater collaborations and dialogue among civil society and the legal professionals could ultimately result in understanding developments relating to digital rights jurisprudence and sharing of resources. Engaging with the judiciary on issues relating to digital rights perhaps requires to be an ongoing effort outside the courtroom too.

[5] https://internetfreedom.in/iff-files-rejoinder-in-pil-seeking-surveillance-reform/
[6] https://economynext.com/sri-lanka-supreme-court-petitioned-on-invasion-of-privacy-central-database-profiling-8526/
[7] https://ifex.org/despite-pakistani-concerns-over-digital-surveillance-snags-in-hearing-of-finfisher-case/
[8] Prasad, S.K & Aravindakshan, S. (2020). Playing catch up – privacy regimes in South Asia. *The International Journal of Human Rights (2020).* DOI:10.1080/13642987.2020.1773442

# List of cases

**Bangladesh**

● Abul Kalam Azad v. David Bergman 5 CLR (2017) 7 [International Crimes Tribunal of Bangladesh, 2014]

● State v. Md. Rafiqul Islam 69 DLR (2017) 18 [Supreme Court of Bangladesh (High Court Division), 2016]

**India**

● Anna Vetticad and Jack Dorsey v. State of Rajasthan S.B. Criminal Misc(Pet.) No. 2818/2019 [Rajasthan High court, 2020]

● Anuradha Bhasin v. Union of India 2020 SCC OnLine SC 25 [Supreme Court of India, 2020] (referred to as "Anuradha Bhasin")

● Ashutosh Dubey v. Netflix Inc I.A 3754/2020 [Delhi High Court, 2020]

● Banashree Gogoi v. Union of India 2019 SCC Online Gau 5584 [Guwahati High Court, 2019]

● Dhirendra Singh Rajpurohit v. State of Rajasthan D. B. Civil Writ No. 10304/2018 [Rajasthan High Court, 2018]

● Faheema Shirin v. State of Kerala 2019 (2) KHC 220 [Kerala High Court, 2019]

● Foundation for Media Professionals v. Union Territory of Jammu & Kashmir Writ Petition D. No. 10817 of 2020 [Supreme Court of India, 2020]

● Gaurav Sureshbhai Vyas v. State of Gujarat WP (PIL) No. 191 of 2015 [Gujarat High Court, 2015]

● In Re Prajwala (2018) 15 SCC 551 [Supreme Court of India, 2019]

● In Re Prashant Bhushan & Another Suo moto Criminal Contempt Petition No 1 of 2020 [Supreme Court of India, 2020]

● Justice K.S. Puttaswamy v. Union of India (2019) 1 SCC 1 [Supreme Court of India, 2018] (referred to as "Puttaswamy I")

● Justice K.S. Puttaswamy v. Union of India AIR 2017 SC 4161 [Supreme Court of India, 2017] (referred to as "Puttaswamy II")

● Kamlesh Vaswani v. Union of India W.P. (Civil) No. 177/2013 [Supreme Court of India, 2014, 2015] (referred to as "Kamlesh Vaswani")

● Khawar Butt v. Asif Nazir Mir CS(OS) 290/2010 [Delhi High Court, 2013]

● People's Union for Civil Liberties v. Union of India AIR 1997 SC 568 [Supreme Court of India 1997] (referred to as "PUCL")

● Registrar (Judicial) v. Secretary to the Government Suo moto WP No. 16668/2017 [Madras High Court, 2017]

● S. Muthukumar v. Telecom Regulatory Authority of India WP(MD) No. 7855 of 2019 [Madras High Court, 2019] (referred to as 'Muthukumar")

● Sabu Mathew George v. Union of India (2018) 3 SCC 229 [Supreme Court of India, 2018] (referred to as "Sabu Mathew George")

● Secretary, Ministry of Information and Broadcasting, Government of India v. Cricket Association of Bengal AIR 1995 SC 1236 [Supreme Court of India 1995]

● Sharat Babu Digumarti v. NCT of Delhi AIR 2017 SC 150 [Supreme Court of India, 2016]

● Shreya Singhal v. Union of India AIR 2015 SC 1523 [Supreme Court of India, 2015] (referred to as "Shreya Singhal")

● Sneha Kalita v. Union of India (2018)12 SCC 674 [Supreme Court of India, 2017]

● Suo moto PIL after gangrape incident WP PIL No. 158/2018 [Uttarakhand High Court, 2018]

● Swami Ramdev v. Facebook CS (OS) 27/ 2019 [Delhi High Court, 2019]

● Tehseen S. Poonawalla v Union of India (2018) 9 SCC 501 [Supreme Court of India, 2018]

● Vinit Kumar v. Central Bureau of Investigation

**Sri Lanka**

● Sunila Abeysekera v. Ariya Rubasinghe S.C. Application No. 994/99 [Supreme Court of Sri Lanka, 2000]

● Supreme Court Advisory Opinion, SC Reference No. 1 of 2008 [Supreme Court of Sri Lanka, 2008]

**Pakistan**

● A. Khalid Ansari v. Mir Shakil Ur Rahman PLD 2011 Karachi 484 [Sindh High Court, 2011]

● Asim Nawaz v The State 2019 P CrLJ 920 [Lahore High Court, 2018]

● Awami Workers Party v. Pakistan Telecommunication Authority Writ Petition no. 634/2019 [Islamabad High Court, 2019]

● Benazir Bhutto v President of Pakistan 1998 PLD 388 [Supreme Court of Pakistan 1998] (referred to as the "Benazir" case)

● Bolo Bhi v. Federation of Pakistan Writ Petition 4994/2014 [Islamabad High Court, 2014, 2015, 2018]

● Bytes For All v. Federation of Pakistan Writ Petition 958/2013 [Lahore High Court, 2013, 2014]

● CM Pak Limited v. Pakistan Telecommunication Authority 2018 PLD 243 Islamabad [Islamabad High Court, 2018]

● High Court Bar Association v. Government of Balochistan PLD 2013 Balochistan 75 [Balochistan High Court, 2012

● Islamic Lawyers Movement v. Federation of Pakistan 2012 CLC 1300 [Lahore High Court, 2012]

● Jamal Akram v. Federation of Pakistan 2011 PLD 377 [Lahore High Court, 2011] (referred to as "Jamal Akram")

● Justice Qazi Faez Isa v. The President of Pakistan & others C.P. No. 19/2019 [Pakistan Supreme Court, 2020]

● MD Tahir v. Director, State Bank 2004 CLD 1680 Lahore [Lahore High Court, 2004]

● Ministry of Information Technology and Telecommunications & Pakistan Telecommunication Authority v. CMPak Limited C.A 977 & 978/2018 [Supreme Court of Pakistan, 2020]

● Muhamad Ayoub v. Federation of Pakistan 2018 P Cr LJ 1133 [Lahore High Court, 2017

● Muhammad Abdul Rauf Siddiqui v SHO 2013 P CrLJ 70 [Sindh High Court, 2012]

● Proxima Beta Pte v Federation of Pakistan WP No 1788/2020 [Islamabad High Court, 2020]

● Salman Shahid v. Federation of Pakistan W.P. No. 739/2017 [Islamabad HC, 2017].

● Talal Ahmed Chaudhry v State 2019 SCMR 542 [Supreme Court of Pakistan, 2019]

**Nepal**

● Baburam Aryal v GoN, NKP (2017), N.S.C 9740 [Supreme Court of Nepal, 2017]

● Robert Ian Penner v Department of Immigration NKP (2018), N. S.C 10091 [Supreme Court of Nepal, 2018]

# Introduction and methodology

## Digital laws and jurisprudence

Instruments in the form of legislation, policy documents and directives have been used extensively to regulate the internet. This includes the development and governance of infrastructure and user experience relating to information and communication technologies (ICTs). With the exponential increase in the shift to digital mediums for a range of activities, states have been constantly grappling with evolving challenges. Initially traditional offline legislation in the form of penal, telegraph and broadcast regulations laws were being extended to the internet. Over time, internet and digital specific laws have evolved or are in the process of being enacted in the Asian region.

A 2017 study Unshackling Expression,[9] found that freedom of expression and opinion online is increasingly criminalised with the aid of penal and internet-specific legislation. It brought to light the problematic trends in the use of laws against freedom of expression in online spaces in Asia. This holds true of other rights in the digital space including privacy, right to information and perhaps access to the internet as such.

The study went on to conclude that offline regulations, typically in penal legislation, are applied to online spaces, to bolster internet-specific legislation. Legitimate expression on the internet is increasingly being redefined as cybercrime. States rely on legal provisions relating to public order, national security, decency and religion-based exemptions to crack down on legitimate forms of expression and dissent. Multiple legal provisions (including use of both offline and online specific laws) are used to target a "single offence" and harsher punishments are prescribed for the online realm as compared to offline. The study also found that some ICT laws in Asia disregard national and international jurisprudence on rights evolved over decades. ICT or digital laws impact various rights including freedom of expression, assembly and association, information, privacy, culture, health, gender equality, education and political participation. ICT laws have mushroomed in the last few years in the region drawing on models existing in other jurisdictions. Newer legislation seeking to address issues such as terrorism or national security, are also incorporating internet and digital specific provisions. Amendments are carried out to include internet specific provisions in existing legislation. While traditional offline laws are used to address the internet, multiple legislation have come into force to address a multitude of issues. These have typically addressed cybercrime, security, broadcasting and communication regulation or data protection. As this report is being developed, several bills are pending for approval in different jurisdictions.

Experts have pointed out that these laws and drafts carry vague or overbroad provisions that carry with them the possibility of being implemented arbitrarily completely disregarding constitutional guarantees or jurisprudence on the said subject matter which has evolved over decades.[10]

Ultimately, these laws or specific provisions and instances of arbitrary application are challenged before the courts. Their validity and legality is tested against the scheme of the enabling law or the contours of the constitution. The pronouncements or even the manner of treatment of these cases by the judiciary has significantly shaped and continues to shape the discourse, guarantees and boundaries relating to digital rights. Jurisprudence is particularly important since it sets the standards for rights guarantees and regulation, it has the ability to undo a law, water it down or in some cases even go completely against the spirit of protections enjoyed over the years. It remains as the ultimate platform for holding states accountable while reassuring citizens in some cases.

On the contrary, some judicial pronouncements also have the ability to embolden states compromising guarantees. Above all, judicial precedents and discourse sets the tone for the evolution of rights in the field, shaping future legislation. The courts remain as the last resort for individuals for asserting, defending and securing their rights, hopefully. Over the course of this research, we have found that oftentimes there is a lack of consistency in how courts decide and deliberate on digital rights.

[9] Association for Progressive Communications (2017). *Unshackling Expression: A study on laws criminalising expression online in Asia. Global Information Society Watch*. https://www.giswatch.org/2017-special-report-unshackling-expression-study-law-criminalising-expression-online-asia

[10] Association for Progressive Communications (2017). Op cit.

This could perhaps be attributed to the evolving challenges, severity of the situation before them, lack of technical understanding or implications of new technology. Online interactions or activities are treated differently by the courts as compared to offline spaces given the virality and exposure of content. Overall, the unpredictability in how the judiciary would deliberate on digital rights has left experts and activists in the grip of fear in initiating strategic litigation. Jurisprudence in Asian states on digital rights has ranged from being progressive to merely recognising the existence of rights or even to outright dismissal of long-established rights guarantees.

While numerous UN resolutions[11] and expert reports have opined that human rights offline are equally protected online,[12] jurisprudence from the region has not been consistent with adapting this. Courts have seldom accorded international human rights standards as the minimum guarantee or aim to further protections in online spaces. In some instances, passing reference has been made to international law without explicit discussions on applicable guarantees in the Universal Declaration of Human Rights (UDHR), International Covenant on Civil and Political Rights (ICCPR), International Covenant on Economic, Social and Cultural Rights (ICESCR) or other instruments. Through poor ICT laws and their arbitrary application, states have legitimised what is otherwise illegal or have legalised what would otherwise be illegitimate. This necessitates the study of jurisprudence on ICT laws and digital rights in the region with the hope of engaging in course correction.

**States studied**

South Asia was selected as the region for this study with a focus on Bangladesh, India, Nepal, Pakistan and Sri Lanka. The South Asian region, given the close similarities in the socio-cultural and economic context, political connectedness and similarities in legal systems formed a natural block for the study. The economic and political challenges faced in these countries are largely similar with varying degrees of distress. Bangladesh, India, Pakistan and Sri Lanka share a history of being colonised by the same imperial powers. With the liberation of each of these states, a common law system evolved with many key pieces of legislation from the colonial era continuing with adjustments over time. Nepal follows a hybrid legal system.[13] The five countries that were studied have written constitutions with elaborate articulation of fundamental rights.

With high rates of mobile internet penetration and over 590 million mobile subscribers[14] a large Section of the population is connected. However, a significant population is left behind. While mobile connectivity guarantees some basic access, the lack of significant broadband connectivity in the region remains a serious issue especially in rural areas and among economically weaker Sections.

Key digital rights challenges in the region range from low rates of meaningful access to the internet, persistent internet shutdowns, high levels of censorship, criminalisation of legitimate expression, pervasive hate speech, weaponisation of religious sentiments as a means to curtail speech, illegal surveillance and poor privacy protections. Marginalised groups such as women, LGBTIQ persons, religious minorities, oppressed caste groups and economically weaker Sections are highly vulnerable in online spaces finding very

[11] Human Rights Council. (2016). The promotion, protection and enjoyment of human rights on the Internet. A/HRC/32/L.2016. https://digitallibrary.un.org/record/845728?ln=en; Human Rights Council (2018). The promotion, protection and enjoyment of human rights on the Internet. A/HRC/38/L.10/Rev.1. https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/38/L.10/Rev.1; United Nations General Assembly. (2019). Promotion and protection of human rights and fundamental freedoms, including the rights to peaceful assembly and freedom of association.A/RES/73/173. https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/173

[12] Human Rights Committee. (2011). General comment No. 34, Article 19: Freedoms of opinion and expression. CCPR/C/GC/34. www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf; Human Rights Council. (2012). The promotion, protection and enjoyment of human rights on the Internet. A/HRC/20/L.13. https://daccess-ods.un.org/TMP/3578843.1763649.html; La Rue, F. (2011). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. A/HRC/17/27. https://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/17/27; Voule. C. (2019). Report of the Special Rapporteur on Freedom of Peaceful Assembly and of Association on Rights to freedom of peaceful assembly and of association in the digital age. A/HRC/41/41. para 10. https://www.ohchr.org/Documents/Issues/FAssociation/A_HRC_41_41_EN.docx

[13] Urscheler, H. (2012). Innovation in a hybrid system: The example of Nepal. *Potchefstroom Electronic Law Journal* 15(3) 98-119. https://core.ac.uk/download/pdf/26222722.pdf

[14] GSMA. (2019). Mobile Internet Connectivity 2019: South Asia Factsheet. *GSMA*. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/09/Mobile-Internet-Connectivity-SouthAsia-Fact-Sheet.pdf

little support from legal systems.[15] One of the key reasons for selecting this region and studying the jurisprudence across borders is the potential influence it has in informing other states in the region and perhaps even influencing the way the courts may decide on matters relating to digital rights. Broadly, the states studied are receptive to public interest or strategic litigation with relaxed stands on the strict locus standi rule thereby enabling civil society to engage with the courts.

## Methodology

This study on digital rights jurisprudence in South Asia primarily entailed desk research with a few interviews with experts in the different states. For the purposes of this study, digital rights[16] is understood as human rights as they are invoked in digitally networked spaces. Those spaces may be physically constructed, as in the creation of infrastructure, protocols and devices or they may be virtually constructed, as in the creation of online identities and communities and other forms of expression, as well as the agency exercised over that expression, for example, management of personally identifiable data, pseudonymity, anonymity and encryption. Such spaces include but are not necessarily limited to the internet and mobile networks and related devices and practices.

Existing research on the ICT legal and policy environment in Bangladesh, India, Nepal, Pakistan and Sri Lanka paved the way for focus on jurisprudence. The study involved extensive review of disposed or completed cases in these states. Cases selected were primarily from the Supreme Courts and High Courts. The study did not take into consideration decisions of administrative courts, magistrate court order or decisions of cybercrime tribunals given the absence of precedential value. The cases were primarily sourced from the official websites of courts and freely available judicial databases. We relied on websites such as Indian Kanoon, Pakistan Law Site and Manupatra. The case law database made available by Global Freedom of Expression - Columbia University was significant in locating cases and summaries.

The CYRILLA database[17] of digital rights laws, cases and analyses from across the globe formed the starting point for collation of cases from the countries of study. This database enables cross jurisdictional analysis and allows for users to find laws across different jurisdictions. The multilingual database is developed and maintained to map and analyse the evolution and impacts of legal frameworks on digital environments. It allows users to filter resources by region or issue area. The database links relevant resources to each other, allowing us to navigate between an article of legislation and the judicial decision that cited it.[18]

For cases that were not available on these platforms, the research team reached out to experts in the states and relied on the work of Ashwini Natesan, LIRNEAsia (Sri Lanka) and Rifat Khan (Bangladesh) for copies of relevant judgements. These additional judgements have been added to the CYRILLA database subsequently. The research titled *Unshackling Expression: A study on criminalisation of freedom of expression online in Nepal* developed by Body&Data was instrumental for our understanding of the ICT legal ecosystem and cases in Nepal as case law was not available in English.The cases collected from these sources went through an initial analysis to sift out cases that were not relevant to the study or those that did not discuss human rights as a part of the deliberations. The remaining cases were shared with experts from the states studied to ensure that they were important cases that informed the discourse on digital rights.

These cases were fed into a workbook[19] grouping them based on the state, authority and other information relating to the case. Search terms used for finding cases and a copy of the judgement were stored and analysed. A short summary was developed and the cases were categorised based on the themes discussed in the case. Based on the cases collected, three clear areas emerged for the study - access, privacy and freedom of expression. Perhaps, the networks we reached out to and the search terms used limited or influenced the categories of cases collected. This study is not meant to be looked at as a digest of cases relating to digital rights or the areas mentioned above. The cases finally selected are not an exhaustive list dealing with the subject.

[15] APC-IMPACT (2017). *State of the Internet in Asia: The case of India, Malaysia and Pakistan*. Bytes for All, Digital Empowerment Foundation, EMPOWER, Association for Progressive Communications. https://www.apc.org/en/pubs/state-internet-asia-case-india-malaysia-and-pakistan
[16] This working definition of digital rights was developed by SMEX while creating a methodology for collecting, categorising and analysing digital rights related legislation and a solid baseline of data on the emerging legal landscape for Arab digital rights, known as the Arab Digital Rights Datasets (ADRD).
[17] https://cyrilla.org/library/?q=(order:desc,sort:creationDate,treatAs:number)
[18] Tutorial for the database is available at https://youtu.be/3AQRVqeA5-Q
[19] https://docs.google.com/spreadsheets/d/1hbolMtuQWTukQ-cw38W8uL2_4KVfUDR9xI6GcBunhHc/edit?usp=sharing

They were picked on the consideration of whether the case would allow for analysis of key discussions on digital rights. They were primarily cases that were emblematic and had elaborate observations in the body of the judgement. Some cases selected are not necessarily the earliest or the first instance where a position of law is stated or settled, they have been selected based on multiple considerations. Most of these cases deal with important questions of law, it's validity or the legality of selective action. Judgements that showcased dissenting opinions or disagreements among the bench or across jurisdictions were also selected.

Once the list of cases was finalised and grouped, the research team studied each judgement and the context in which the cases were filed. Key components of the judgements namely facts of the case, arguments put forward, considerations of the court, findings, rationale of the court for coming to a conclusion, key principles of law including international law cited and precedents relied on were noted. An analysis was developed keeping these factors in mind.

Some of the key challenges faced in the course of the research primarily related to access to judicial pronouncements. While it was easier to find judgements from some jurisdictions, publicly available platforms did not document cases well in other jurisdictions. Instances where judgements were recorded in local language were not always translated in English. It was also challenging to determine the finality of a case as the status in relation to appeals preferred by parties was not easily accessible. It was difficult to agree on a final and manageable list of cases to work with as many cases seemed to deal with similar topics but had mild variations. Lastly, narrowing down the areas of focus for the study and restricting the geographical scope of the study entailed significant deliberation.

While this report looks at developments in five countries in South Asia with a specific focus on access, privacy and freedom of expression, several other issues warrant attention. Laws and jurisprudence relating to intermediary liability, misinformation, anti-trust, algorithmic discrimination, community networks, taxation, information sovereignty, physical infrastructure, spectrum allocation, sharing and licensing and cross-border data transfers are swiftly evolving. Future studies could focus on these issues and adapt the study to other regions or countries.

**Aim of the report**

This report is not meant to exhaustively list cases relating to digital rights in the states studied. The objective is to make available a resource that showcases and analyses the judicial thinking in Bangladesh, India, Nepal, Pakistan and Sri Lanka on broad questions relating to digital rights and more specifically issues relating to access, privacy and freedom of expression. We seek to develop documentation that can be used by policy experts, digital rights defenders and lawyers to identify and compare jurisprudence on the issues discussed. Ultimately, we hope that this document enables advocacy for improvements in digital rights guarantees based on progressive judicial pronouncements in other jurisdictions and that collaborations are made possible.

# ICT legal landscapes

## Countries and legal systems

Four of the South Asian states chosen for this report (Sri Lanka, Bangladesh, India and Pakistan) follow a common law system, while Nepal follows a hybrid legal system.[20] In all the five countries, the rights to freedom of speech, expression, assembly and association are guaranteed by the Constitution. These rights are not absolute in any of the states and the basis of which these rights can be restricted are laid down in the constitutions or other legal documents. Some of the prominent justifications that states provide to restrict freedom of speech are national security, friendly relations between states, public order, decency, blasphemy, morality, contempt of court and incitement to an offence. These justifications are commonly used by States to violate digital rights and crack down on even legitimate forms of expression, including political, artistic and sexual expression. The right to privacy is explicitly recognised in the Constitutions of Pakistan, Nepal and Bangladesh, while the Indian and Sri Lankan Constitutions do not contain an explicit right to privacy, though judicial interpretation has recognised the right to privacy as part of other fundamental rights. This Section introduces each of the five states which are part of this report, with a focus on both internet-specific and offline laws which affect digital rights.

## Bangladesh

The key laws regulating or impacting digital rights in Bangladesh are the Digital Security Act 2018 (which replaced the Information and Communication Technology Act 2006), the Bangladesh Telecommunications Act 2001, the Penal Code 1860 and the Anti-Terrorism Act 2013.[21] The Constitution of the People's Republic of Bangladesh guarantees all the "freedom of thought and conscience". Along with it, it also guarantees every citizen the right to freedom of speech and expression, assembly, association and information.[22] The right to freedom of speech and expression is subject to "any reasonable restrictions imposed by law in the interests of the security of the State, friendly relations with foreign states, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence."[23] However, digital laws in Bangladesh have fallen well short of these standards and consistently erode these guarantees. Political dissent online has oftentimes turned fatal and freedom of expression online, especially for bloggers, remains heavily compromised.

The Penal Code in Bangladesh targets various forms of expression in the name of sedition, causing disaffection towards the state, obscenity, insulting religion, defamation and affecting friendly relations with other states. Other laws which criminalise expression include provisions of the Anti-Terrorism Act 2013 relating to instigation of terrorism and a provision of the Foreign Donations (Voluntary Activities) Regulation Act 2016 which makes it an offence for NGOs to make "inimical" or "derogatory" remarks against the constitution or a constitutional body.

The Digital Security Act 2018 (the DSA), which is the central legislation used to regulate and curtail online freedoms, empowers the Digital Security Agency and in some cases, law enforcement, to remove or block any data in digital media for a wide variety of reasons that are broadly defined and leave much room for interpretation. Content is removed if it is violative of digital security, hampers the nation or nation's unity, financial activities, security, defence, is contrary to religious values, public discipline or incites racism and hatred. The DSA also establishes a number of offences which criminalise expression, including online defamation, hurting religious sentiments, causing hatred of destroying harmony or expression that is deemed to promote sentiments against the liberation war of Bangladesh, the Father of the Nation, or national flag or anthem. The DSA repealed and replaced some of the key provisions of the Information and Communication Technology Act 2006 (ICT Act), including Section 56, which had been criticised for suppressing free speech online. However, pending cases

[20] http://www.juriglobe.ca/eng/index.php?i=1
[21] Khandhadai, G. (2016). *Desecrating Expression: An Account of Freedom of Expression and Religion in Asia.* Bytes for All, Pakistan and FORUM-ASIA. https://www.forum-asia.org/uploads/ wp/2016/12/Final_FoER_Report.pdf. Please refer to this report for further details.
[22] The Constitution of the People's Republic of Bangladesh 1972. Articles 38, 39. http://bdlaws.minlaw.gov.bd/act-367.html
[23] The Constitution of the People's Republic of Bangladesh 1972. Article 39. http://bdlaws.minlaw.gov.bd/act-367.html

even under the repealed Sections of the ICT Act continue to be prosecuted. In addition to the powers granted under the DSA, the Bangladesh Telecommunications Act 2001 gives wide powers to the Bangladesh Telecommunication Regulatory Commission to intercept and monitor communications, as well as suspend data or voice calls on the grounds of national security and public order. The right to privacy of "correspondence and other means of communication" are guaranteed under Article 43 of the Constitution. The right to privacy is not absolute and is "subject to any reasonable restrictions imposed by law in the interests of the security of the State, public order, public morality or public health".[24]

While the DSA does provide for some means of data protection by making it a crime to intervene with identity information in Bangladesh, the law also exempts service providers from any liability for facilitating access to data-information, if they show that it happened without their knowledge or that they took "all possible" steps to prevent it from happening, without defining what these steps should be.

**India**

The key laws regulating or impacting digital rights in India are the Information Technology Act 2000, the Indian Telegraph 1885 (and the rules issued thereunder), the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016, the Indian Penal Code 1860 and the Code of Criminal Procedure 1973.[25] India's Constitution guarantees the right to freedom of expression to all its citizens, subject to reasonable restrictions such as the "interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence".[26] Though the right to privacy is not expressly guaranteed by the Constitution, it has been held to be a fundamental right as part of the right to life and personal liberty under Article 21 of the Constitution.[27]

However, India has a long history of criminalising speech and digital laws and other laws applied to the internet in India are routinely used to curtail the rights to freedom of expression, assembly, association, information and privacy. The colonial-era Indian Penal Code 1860 criminalises various kinds of expression through offences relating to obscenity, hurting religious sentiments, defamation and sedition, amongst others. The provisions of the Indian Penal Code have been applied to target online speech as well, with political & artistic expression online especially coming under severe attack over the years. However, despite the rampant criminalisation of expression, hate speech is not defined under Indian law and continues unabated, particularly in online spaces, often targeting religious, caste and sexual minorities.

Other offline laws are also extensively applied in a manner which restricts digital rights and censors or criminalises online expression, even when originally unintended by the law in question. Section 144 of the Code of Criminal Procedure 1973 which broadly gives Magistrates powers to issue orders in urgent cases of nuisance or public disorder, is repeatedly used along with other laws to impose network shutdowns with little to no accountability or oversight. The Indian Telegraph 1885, along with the recently issued Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules 2017 are also used to impose network shutdowns and intercept messages. In addition, laws relating to the indecent representation of women,[28] prohibition of sex selection,[29] child sexual offences,[30] contempt of court,[31] prevention of insults to national honour[32] and the prevention of atrocities against marginalised communities[33] are used to criminalise expression online, in many cases targeting speech by the very communities they were meant to protect.

Laws made specifically to regulate ICTs such as the Information Technology Act 2000 (IT Act) along with the Amendment Act of 2008 and rules framed under the IT Act create online offences such as

[24] The Constitution of the People's Republic of Bangladesh 1972. Article 43. http://bdlaws.minlaw.gov.bd/act-367.html
[25] Association for Progressive Communications (2017). Op. cit. Please refer to this report for further details. See also APC-IMPACT (2017). Op. cit.; Khandhadai, G. (2016)
[26] Constitution of India 1950, Article 19. http://legislative.gov.in/sites/default/files/COI-updated.pdf
[27] Justice K.S. Puttaswamy v. Union of India. 2017 (10) SCALE 1.
[28] Indecent Representation of Women (Prohibition) Act 1986. http://legislative.gov.in/sites/default/files/A1986-60_0.pdf
[29] Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act 1994. https://www.ncpcr.gov.in/view_file.php?fid=434
[30] Protection of Children from Sexual Offences Act 2012. https://www.indiacode.nic.in/bitstream/123456789/2079/1/201232.pdf
[31] Contempt of Courts Act 1971. https://www.indiacode.nic.in/bitstream/123456789/1514/1/197170.pdf
[32] Prevention of Insults to National Honour Act 1971. https://www.indiacode.nic.in/bitstream/123456789/1578/3/A1971-69.pdf
[33] Scheduled Castes and the Scheduled Tribes (Prevention of Atrocities) Act 1989, https://ncsk.nic.in/sites/default/files/PoA%20Act%20as%20amended-Nov2017.pdf

cheating, impersonation, interference with privacy, cyber-terrorism among other harms.

Unfortunately, it also includes provisions criminalising online speech, enabling internet shutdowns and blocking of websites, monitoring of data and prohibition of sexual expression. Interception of messages is also made possible violating privacy. Some of the provisions of the IT Act have come under severe judicial scrutiny, as will be discussed in later chapters. In relation to telecom infrastructure, the Telecom Regulatory Authority of India Act 1997 established the Telecom Regulatory Authority of India (TRAI) which has powers to regulate the telecommunications sector. Concerns regarding severe violations to privacy were brought to the fore in India once again with the passing of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016, which governs India's unique identity number project and requires citizens in India to enrol for the biometric system of identification and obtain anAadhaar number. Such privacy concerns are compounded by the lack of a law which protects personal data in India. Though the Personal Data Protection Bill 2019 is currently under deliberations, the current draft contains several problematic provisions relating to surveillance, voluntary social media verification and wide powers to government authorities.

**Nepal**

The key laws regulating or impacting digital rights in Nepal are the Electronic Transactions Act 2006, Online Media Operation Directive 2017, Individual Privacy Act 2019, the National Broadcasting Act 1993 and the National Penal (Code) Act 2017.[34] Article 17(a) of the Constitution of Nepal, 2015 guarantees the right to freedom of expression and opinion.[35] Article 19 of the Constitution guarantees right to communication.[36] This article ensures the information dissemination through any means of media is disseminated without any censorship from the authority and valuing press freedom. Reasonable restrictions to the freedom of expression and opinion are permitted on a number of vague and overbroad grounds, including prohibition of acts which undermine the nationality, sovereignty, independence and indivisibility of Nepal, jeopardise harmonious relations, incite racial discrimination, or untouchability, disrespects labour, or any act of defamation, contempt of court, an incitement of offence and act contrary to decent public behaviour or morality.

Several provisions of the National Penal (Code) Act 2017 criminalise expression including those related to acts prejudicial to harmonious relationships between different classes, religions or communities, obscenity, defamation and blasphemy. In addition to these restrictions in the offline laws, Section 47 of the Electronic Transactions Act 2006 contains a broad prohibition on the publication or display of any materials that are prohibited by the prevailing law, may be contrary to the public morality or decent behavior, may spread hate or jealousy or which may jeopardise the harmonious relations on any electronic media including the internet. The penalties applicable for violation of this provision are also significantly higher than those applicable for similar provisions governing offline behaviour in the Penal Code.

Nepal does not currently have a comprehensive ICT law, though the Information Technology Bill is currently pending before Parliament. This Bill has received widespread criticism from Nepali civil society due to several provisions which would severely curtail freedom of expression online.[37] Currently, the Online Media Operation Directive 2017 governs the registration, operation, renewal and monitoring of online media. This Directive contains ambiguous and vague provisions which threaten the freedom of expression online.[38] Article 11 of the Directive prohibits publication and broadcast of any materials on online media on a number of grounds, including those against "public protocol or morality" as well as materials "without

[34] Body and Data (2020). Unshackling Expression: A study on criminalisation of expression online in Nepal. *Association of Progressive Communications* https://www.apc.org/en/node/37060
[35] Constitution of Nepal, 2015. Article 17. http://www.lawcommission.gov.np/en/archives/category/documents/prevailing-law/constitution/constitution-of-nepal
[36] Constitution of Nepal, 2015. Article 19. http://www.lawcommission.gov.np/en/archives/category/documents/prevailing-law/constitution/constitution-of-nepal
[37] Amnesty International. (2020 16 January). Nepal: Information Technology Bill threatens freedom of expression. *Amnesty International*. https://www.amnesty.org/en/latest/news/2020/01/nepal-information-technology-bill-threatens-freedom-of-expression/
[38] http://freedomforum.org.np/concern-over-online-mass-communications-operation-directive-2017/

authorised source, that could create illusion and have an adverse impact on international relations".

Article 28 of the Constitution of Nepal guarantees the right to privacy "in relation to the person and their residence, property, documents, records, statistics and correspondence and their reputation". However, there is a broad exception allowed to this constitutional right in any "circumstances provided by law".[39]

The Privacy Act 2018 was passed by the Nepali government in order to operationalise the constitutional right to privacy. This law has numerous provisions regulating the collection, use, storage and transmission of personal information. However, Article 19 of the Act authorises the interception and monitoring of electronic communications by authorised officials without adequate safeguards or regulations on how this power can be used.

**Pakistan**

The key laws regulating or impacting digital rights in Pakistan are the Prevention of Electronic Crimes Act 2016 (and rules), Pakistan Telecommunication (Re-organisation) Act 1996, the Telegraph Act 1885, the Pakistan Penal Code 1860, the Anti-Terrorism Act 1997 and the Electronic Transactions Ordinance 2002.[40] The Constitution of the Islamic Republic of Pakistan guarantees the rights to freedom of expression, information, peaceful assembly and association, subject to reasonable restrictions imposed by law.[41] With respect to the right to freedom of expression, limitations permitted by the Constitution are "in the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, commission of or incitement to an offence".[42]

Despite these Constitutional guarantees, laws applied to the internet pose serious hurdles to the exercise of rights online and censorship is common, particularly on grounds of blasphemy. The Pakistan Penal Code 1860 is used to criminalise expression and dissent online by prosecuting the speaker for sedition, outraging religious feelings and blasphemy, obscenity or sexually explicit conduct, sexual deviance and criminal defamation. Most of the restrictions to free speech prescribed in Article 19 have been codified through a set of laws which are also used to crack down on online speech. The Anti-Terrorism Act 1997 includes Sections criminalising speech and behaviour intended to cause fear and hatred and also covers publication and dissemination of information.[43]

The Security of Pakistan Act 1952 is used against any expression directed at defence, external affairs or security of the state. The Contempt of Court Act 2012 in Pakistan is also used to criminalise expression and criticism of judicial processes. The Electronic Transactions Ordinance 2002 criminalises unauthorised access to information while the Defamation Ordinance 2002 deals with civil defamation, slander and libel. The Prevention of Electronic Crimes Act 2016 (PECA) is a major legislation that is used to regulate online spaces in Pakistan. Section 37 of the PECA grants the Pakistan Telecommunication Authority the power to block or remove content, require service providers to retain traffic data and enable real-time surveillance, amongst others. PECA also creates a number of offences.

While hate speech and child pornography are criminalised, so are glorification of an offence or terrorism, false information that harms the privacy or reputation of an individual and even sexual expression. Section 37 of the PECA, contains a list of restrictions allowing the Pakistan Telecommunication Authority (PTA) to block, remove and censor online content. It gives the PTA full discretionary powers to restrict access to "any" information if it considers it necessary to do so in the interest of integrity of Islam, morality, contempt of court, the integrity, security or defence of Pakistan, etc. without providing any reasons or explanation, which is a blatant violation of Article 19 of the constitution along with a number of international treaties.

[39] *Constitution of Nepal, 2017*. Article 28. http://www.lawcommission.gov.np/en/archives/category/documents/prevailing-law/constitution/constitution-of-nepal.
[40] *Association for Progressive Communications* (2017). Op. cit. Please refer to this report for further details. See also APC-IMPACT (2017). Op. cit.; Khandhadai, G. (2016) Op. cit.
[41] Constitution of the Islamic Republic of Pakistan 1973, Articles 19 19A 16 and 17. http://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2Fvbpw%3D-sg-jjjjjjjjjjj
[42] Constitution of the Islamic Republic of Pakistan 1973, Article 19. http://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2Fvbpw%3D-sg-jjjjjjjjjjj
[43] Anti-Terrorism Act 1997, Articles 8, 9 & 11(W). http://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2FqaJw%3D-sg-jjjjjjjjjjj

PECA in Section 10 defines "cyber terrorism" as committing or threatening to commit offences such as unauthorised access to information infrastructure or data transmission of critical data, or interference with such infrastructure or glorification of offences. This is an overbroad provision which is open to abuse and differs significantly from how other nations view cyber terrorism, carrying a prison term of up to fourteen years and penalty. Many free speech activists opposed these provisions when the law was being tabled and now the PECA seems to be targeting all those who express disagreement with either the state or other establishment.[44] The Citizens Protection (Against Online Harm) Rules 2020[45] originally notified under PECA and Pakistan Telecommunication Authority (Reorganisation) Act aimed to define the procedure for regulating online content. These rules required social media companies to localise, facilitate speedy blocking of content and provide user data to the government and threatened social media companies with the potential blocking of platforms. These rules were heavily criticised for the potential negative impact on expression and privacy and the potential for abuse against legitimate expression, [46] and were later suspended by the Prime Minister. A revised version of these Rules renamed as the Rules for Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguard) Rules 2020 have been notified and due to be published in official gazette at the time of the publication of this report.[47]

Apart from PECA, other laws directly related to the operations of the ICT sector are also used to control and censor speech and impact privacy and access. The Telegraph Act 1885 criminalises transmission of false information and obscenity online while the Pakistan Telecommunication (Re-organisation) Act 1996 criminalises transmission of information deemed as intelligence or false/ fabricated information, obscenity and mischief; and allows the federal government to suspend telecommunications services "when an emergency has been proclaimed by the President".[48]

In relation to privacy, the lack of a personal data protection law coupled with contradictory provisions in different laws, weakening the regulation of real time communications surveillance have serious implications on the right to privacy of citizens guaranteed by the Constitution. Article 14 of the Pakistani Constitution provides that the privacy of the home shall be inviolable, subject to the law.[49] The Pakistan Telecommunication (Re-organisation) Act 1996 allows the Federal Government to authorise the interception and tracing of calls and messages through any telecommunication system "in the interest of national security or in the apprehension of an offence",[50] while the Investigation for Fair Trial Act 2013 permits secret warrants to be issued for surveillance or interception.[51] While the Fair Trial Act requires warrants to be obtained from High Courts, PECA further weakens that by allowing the provision of similar permissions through lower courts. The provisions of the National Database and Registration Authority Ordinance 2000 have been criticised as insufficient in protecting the identification data of Pakistani citizens, who are required to be registered in this system.

**Sri Lanka**

The key laws regulating or impacting digital rights in Sri Lanka are the Computer Crime Act 2007, the Sri Lanka Telecommunications Act 1961, the Information and Communication Technology Act 2003, the Penal Code, the Prevention of Terrorism (Temporary Provisions) Act 1978 and the International Covenant on Civil and Political Rights Act 2007.[52] Sri Lanka's

[44] https://www.apc.org/sites/default/files/Bottlenecks-Incompetence-and-Abuse-of-Power-An-analysis-of-PECA-implementation_0.pdf
[45] Citizens Protection (Against Online Harm) Rules 2020. https://moitt.gov.pk/SiteImage/Misc/files/CP%20(Against%20Online%20Harm)%20Rules%2C%202020.pdf
[46] Media Matters for Democracy (2020, February). Citizens Protection (Against Online Harm) Rules 2020: Key Concerns, Objections and Recommendations. *Digital Rights Monitor - Pakistan*, http://www.digitalrightsmonitor.pk/wp-content/uploads/2020/02/citizens-protection-rules-00.pdf
[47] http://www.digitalrightsmonitor.pk/new-social-media-rules-notified-on-16th-october-yet-to-be-made-public/
[48] Pakistan Telecommunication (Re-organisation) Act 1996. Section 54(3). http://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apqWaw%3D%3D-sg-jjjjjjjjjjj
[49] Constitution of the Islamic Republic of Pakistan 1973. Article 14. http://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2Fvbpw%3D-sg-jjjjjjjjjjj
[50] Pakistan Telecommunication (Re-organisation) Act 1996. Section 54(1). http://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apqWaw%3D%3D-sg-jjjjjjjjjjj
[51] Investigation for Fair Trial Act 2013. Section 9. http://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2FqbZw%3D-sg-jjjjjjjjjjj
[52] For the information on the legal landscape in Sri Lanka contained within this section, reliance was placed on Khandhadai, G. (2016). Op. cit. Please refer to this report for further details.

Constitution guarantees the freedom of speech and expression, peaceful assembly, association and the right to access information.[53] The right to freedom of speech and expression is subject to "such restrictions as may be prescribed by law in the interests of racial and religious harmony or in relation to parliamentary privilege, contempt of court, defamation or incitement to an offence."[54] It is relevant to note that unlike other South Asian countries, the Sri Lankan Constitution does not expressly require that such restrictions be reasonable. Various provisions in the Sri Lankan Penal Code however criminalise expression through offences relating to insulting religions, wounding religious feelings, obscenity and causing disaffection against the State. The Prevention of Terrorism (Temporary Provisions) Act 1978 contains restrictions of freedom of expression and broadly criminalises expression likely to cause racial, religious or communal disharmony, ill-will or hostility and has been used to shut down dissent online.[55] Cyber Security Bill and the Data Protection Bill have been formulated, both of which are in the process of undergoing public consultations.

[53] Constitution of the Democratic Socialist Republic of Sri Lanka. Articles 14 and 14A. https://www.parliament.lk/files/pdf/constitution.pdf
[54] Constitution of the Democratic Socialist Republic of Sri Lanka. Article 15(2). https://www.parliament.lk/files/pdf/constitution.pdf
[55] Prevention of Terrorism Act 1978. Section 2(1)(h). http://www.commonlii.org/lk/legis/num_act/potpa4801979608/

# Access and network shutdowns

## Introduction and policy ecosystem

Access to the internet is a necessary precondition for the exercise and enjoyment of a whole host of human rights online and offline. Universal affordable internet access is a stated priority for all the states studied. Broadband and access related national policies in Bangladesh,[56] India,[57] Nepal,[58] Pakistan[59] and Sri Lanka[60] articulate a path for delivering services to larger Sections of the population.

Broadband access is made available through public sector and private sector commercial operators in the five countries. The primary means through which internet connectivity is ensured is over reliant on mobile internet connectivity which comes with several limitations.[61] Laws regulating access include those dealing with the establishment of regulatory bodies and the allocation of spectrum for operators. The functioning and modalities of access are broadly dealt with through policies, directives and license agreements of relevant ministries and regulatory bodies. In addition, broadband policies and various other policy documents outline the goals and processes for increasing access to the internet. The compliance of operators is overseen by regulatory bodies.[62]

In addition to national operators, local operators are emerging in the region. Local operators serve a much smaller and more distinct market, with deeper knowledge of their users, able to provide more affordable connectivity when it comes to serving a local market. Local operators can be further classified into two types: commercial and social-purpose. Although the business models of national operators and local commercial operators providing connectivity are fairly well understood, less is known about local social-purpose operators and their role in providing affordable access to communication in places where the commercial operators see no interest. These local social-purpose operators are commonly referred to as community networks, where the telecommunications infrastructure is built, managed and operated by local communities to meet their communications needs.[63] They offer an alternative to big commercial operators and are viewed as a means of democratising infrastructure and achieving sustainable development. The networks are often built using low-cost WiFi equipment and unlicensed spectrum bands to interconnect members of the community and improve their lives.[64]

In the five states studied, community networks exist and operate at different levels in India, Nepal and Pakistan while strong community radio networks operate in Bangladesh and Sri Lanka which have the potential of evolving into community networks.[65] However, in this report we were unable to locate concrete cases or jurisprudence that impact the ability of community networks to function, this warrants a dedicated study.

## Access and rights

Meaningful access to the internet impacts our ability to realise several rights including the right to freedom of expression, assembly and association, health, information, participation in governance, livelihood and education among

[56] Government of Bangladesh. (2009). National Broadband Policy 2009. *Bangladesh Telecommunication Regulation Commission*. http://www.btrc.gov.bd/sites/default/files/national_broadband_policy_2009_0.pdf
[57] Ministry of Communications and Information Technology, Government of India (2004). Broadband Policy 2004. *Department of Telecommunications*. https://dot.gov.in/broadband-policy-2004.
[58] Government of Nepal (2015). Broadband Policy 2015. Nepal. *Nepal Telecommunications Authority*. https://nta.gov.np/wp-content/uploads/2012/06/Broadband-Policy-2071.pdf
[59] Ministry of Information Technology, Government of Pakistan (2004). National Broadband Policy for Pakistan. *Universal Service Fund*. https://usf.org.pk/assets/rules-pdf/broadband-policy.pdf.
[60] Government of Sri Lanka (2016). National Broadband Policy of Sri Lanka 2016. *International Telecommunications Union*. https://www.itu.int/md/D14-SG01.RGQ-C-0288/en
[61] Manzar, O. (2020 12 September). A phone is not enough. https://www.civilsocietyonline.com/cover-story/a-phone-is-not-enough/
[62] Bangladesh: Bangladesh Telecommunication Regulatory Commission (BTRC), India: Telecom Regulatory Authority of India (TRAI), Nepal: Nepal Telecom Authority (NTA), Pakistan: Pakistan Telecommunication Authority (PTA) and Sri Lanka: Telecommunication Regulatory Commission of Sri Lanka (TRCSL).
[63] APC & IDRC. (2018). *Community Networks*. Global Information Society Watch 2018. https://www.apc.org/en/pubs/global-information-society-watch-2018-community-networks
[64] Gautam, A. (2020, 26 June). Closing the Digital Divide in Nepal. https://www.internetsociety.org/blog/2020/06/closing-the-digital-divide-in-nepal/
[65] Srivastava R., Srivastva S. & Singh, K. (2020). *Community Networks & the Internet of People*. Digital Empowerment Foundation. https://www.apc.org/sites/default/files/DEF_report_2019.pdf and APC & IDRC. (2018). Community Networks. Global Information Society Watch 2018

others.[66] The internet boosts economic, social and political development and contributes to the progress of humankind as a whole.[67] Access to the internet plays a pivotal role in our lives especially in times of distress and disaster. For instance, during the COVID pandemic,[68] various organs of the state have heavily relied on the internet to reach relief materials, provide essential services and critical medical information. Dispensation of justice and governance through virtual platforms became the norm. The pandemic has also surfaced several challenges and exacerbated violations, especially for those who do not have access to the internet.[69]

As a result of its pervasive nature and determining role, access to the internet is increasingly being viewed and recognised as a right. Experts have argued that human rights must evolve to meet present day realities and that laws governing human rights must be viewed as living instruments.[70] By drawing support from international guarantees on freedom of expression and other rights in the UDHR and ICCPR, experts have furthered the case for recognition of access to the internet as a right as it is the medium through which these rights become effectively exercisable. Increasing references to the internet and calls for ensuring universal access to the internet in treaty body recommendations, resolutions and the universal periodic review over recent years also show the importance of access in discussions on human rights in international mechanisms.[71] Specific reliance is placed on Article 15 of the International Covenant on Economic, Social and Cultural Rights (ICESCR) which recognises the right of everyone to enjoy the benefits of scientific progress and its applications and the right to benefit from the protection of the moral and material interests resulting from any scientific, literary or artistic production authored. ICTs are undeniably the result of scientific progress and the internet is thus an application of it, which makes the case for recognition as a right. However, arguments countering this have also been put forward which essentially view the internet as an enabler and not an end in itself, cautioning against inflation of rights, especially where positive and negative responsibilities of states are involved.

The earliest South Asian cases on access began by establishing that the right to freedom of speech and expression includes the right to impart and receive information via electronic media. Though not deliberating on access to the internet, the Supreme Court of India[72] in 1995 stated that:

> If the right to freedom of speech and expression includes the right to disseminate information to as wide a Section of the population as is possible, the access which enables the right to be so exercised is also an integral part of the said right. The wider range of circulation of information or its greater impact cannot restrict the content of the right nor can it justify its denial.[73]

A similar pronouncement was issued in 2000 by the Sri Lankan Supreme Court in ***Sunila Abeysekera v. Ariya Rubasinghe***,[74] where the court found that the right to free speech includes the right to use "whatever medium is deemed appropriate to impart ideas and to have them reach as wide an audience as possible". In ***Anuradha Bhasin v. Union of India***,[75] the Indian Supreme Court went further and declared that the rights to freedom of speech and expression and the right to work over the medium of the internet enjoy constitutional protection.The court held that the right to freedom of speech and expression under Article 19 of the Indian Constitution includes the right to choose the medium of expression, in this case, the internet.

[66] https://www.apc.org/sites/default/files/4699_A_HRC_44_NGO_APC_Covid_and_HR_Final_0.pdf, https://www.apc.org/en/news/ending-digital-exclusion-why-access-divide-persists-and-how-close-it and https://www.apc.org/sites/default/files/APC_Submission_to_the_Special_Procedures_COVID-19_Questionnaire.pdf
[67] La Rue, F. (2011). Op. cit.
[68] https://www.apc.org/en/pubs/closer-ever-keeping-our-movements-connected-and-inclusive-association-progressive
[69] Association for Progressive Communications (2020, June). Written statement submitted by Association for Progressive Communications. A/HRC/44/NGO/X. *Human Rights Council*. https://www.apc.org/sites/default/files/4699_A_HRC_44_NGO_APC_Covid_and_HR_Final_0.pdf
[70] De Hert, P. & Kloza, D. (2012). Internet (access) as a new fundamental right. Inflating the current rights framework? *European Journal of Law and Technology* 3(3). https://cris.vub.be/files/49868990/de_hert_kloza_2012_internet_access.pdf
[71] Szoszkiewicz, L. (2018). Internet Access as a New Human Right? State of the Art on the Threshold of 2020. *Przegląd Prawniczy Uniwersytetu im Adama Mickiewicza* 8 (50). https://www.researchgate.net/publication/328290234_Internet_Access_as_a_New_Human_Right_State_of_the_Art_on_the_Threshold_of_2020
[72] Secretary, Ministry of Information and Broadcasting, Government of India v. Cricket Association of Bengal. AIR 1995 SC 1236.
[73] Ibid.
[74] S.C. Application No. 994/99 (Supreme Court of Sri Lanka 1999).
[75] WP (C) 1031/2019 (Supreme Court of India, 2020).

The Kerala High Court in India has taken a definitive position in regard to recognising the right to access the internet. In ***Faheema Shirin v. State of Kerala***,[76] the court stated that:

> When the Human Rights Council of the United Nations have found that right to access to Internet is a fundamental freedom and a tool to ensure right to education, a rule or instruction which impairs the said right of the students cannot be permitted to stand in the eye of law.

This case involved a college student challenging hostel rules which banned use of mobile phones between 10 P.M. to 6 A.M. The petitioner claimed that depriving her ability to access the internet and her phone violated her right to freedom of speech and expression under Article 19(1)(a) of the Constitution of India. The court relied on important precedents set by the Supreme Court in discussing the internet and held that the right to access the internet is part of the right to education as well as the right to privacy under Article 21 of the Constitution. It ordered the reinstatement of the Petitioner who had been expelled from the hostel for resisting the ban on use of mobile phones. Following this judgement and the ***Anuradha Bhasin*** case, the Additional Sessions Court, Ernakulam recently ordered limited access to the internet and software legal journals to an undertrial prisoner by observing that:

> When it is declared by the constitutional courts that right to legal aid and right to use internet are fundamental rights, the petitioner has every justification in asking permission to use the same for accessing legal materials to properly defend his case, in the absence of any prohibition in the prison laws.[77]

**Network shutdowns**

An internet shutdown is an intentional disruption of internet-based communications, rendering them inaccessible or effectively unavailable, for a specific population, location, or mode of access, often to exert control over the flow of information.[78] An internet shutdown happens when someone — usually a government — intentionally disrupts the internet or mobile apps to control what people say or do. Shutdowns are also sometimes called "blackouts" or "kill switches." Bangladesh, India, Pakistan and Sri Lanka have imposed multiple network shutdowns on the pretexts ranging from public order, national security, curtailing misinformation to preventing malpractices during examinations.[79] According to Internetshutdowns.in[80] (a project of the Software Freedom Law Centre, India), since 2012 there have been 443 instances[81] of internet shutdowns in India. These internet shutdowns have largely been imposed under Section 144 of the Code of Criminal Procedure with no accountability or legal oversight.

National and international civil society has repeatedly maintained that the internet is essential to the exercise of freedom of expression, assembly and association, both online and offline.[82] Network shutdowns indiscriminately restrict the exercise of these rights and hinder the realisation of economic, social and cultural rights, including the right to health, education and livelihoods. They have significant technical, economic and human rights impact.[83] They also raise concerns for people's safety by reducing the ability of emergency services to communicate and locate people and undermining the ability of the authorities to disseminate important information to move people to safety. Shutdowns also severely impact the work of the media, preventing media workers from being able to carry out reporting and dissemination of

[76] 2019 (2) KHC 220.
[77] *Roopesh v State of Kerala* Crl.M.P. No.164/2020 in S.C No.43/2017 [Additional Session Courts, 2020]. https://www.livelaw.in/pdf_upload/pdf_upload-383886.pdf
[78] Taye, B. (2020). Targeted, *Cut Off and Left in the Dark: The #KeepItOn report on internet shutdowns in 2019*. AccessNow. https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf
[79] https://www.accessnow.org/keepiton/
[80] https://internetshutdowns.in/
[81] As of 18 October 2020
[82] Venkiteswaran, G. (2016). *Freedom of assembly and association online in India, Malaysia and Pakistan*. APC-IMPACT. https://www.apc.org/sites/default/files/FOAA_online_IndiaMalaysiaPakistan_1.pdf
[83] https://www.internetsociety.org/policybriefs/internet-shutdowns

of information during critical times.[84] Several UN resolutions and reports have condemned network shutdowns and have called on states to eradicate its imposition.[85] The UN Human Rights Council has unequivocally condemned[86] intentional measures to prevent or disrupt access to or dissemination of information online, in violation of international human rights lawand called on states to cease this practice. Multiple UN Special Rapporteurs have pronounced internet shutdowns as unjustifiable[87] and in violation of international law.[88]

Jurisprudence on the legality of network shutdowns have been examined in a few jurisdictions including Indonesia,[89] Congo, Zimbabwe,[90] Cameroon,[91] ECOWAS in relation to a shutdown in Togo,[92] Russian Federation,[93] India and Pakistan.[94] The cases brought before the courts challenging network shutdowns have been largely initiated by public spirited lawyers, human rights groups and law students.[95] In ***CMPak Limited v. Pakistan Telecommunication Authority***[96] in the Islamabad High Court, the appellant was CMPak Limited, a major Pakistan based telecommunications service provider operating through a license granted by the Pakistan Telecommunication Authority. In the cases stated above, the petitioners primarily contended that legal procedures prescribed in national legislation and rules for imposing extraordinary measures like internet shutdowns have not been followed. They also argued that imposition of network shutdowns had far reaching consequences on the exercise of fundamental rights and freedoms given that they are not the least intrusive measure. Lastly, they showcased the economic costs and impact of internet shutdowns on communities and businesses. States on the other hand have justified action taken by authorities as within the legal framework and argued that network shutdowns are necessitated to prevent violence, damage to public property and maintain public order among other considerations. In most of these cases the courts seem to be more receptive to contentions relating to procedural irregularities over questions of fundamental rights.[97]

The jurisprudence on the issue so far has varied from deeming network shutdowns as legal to holding that procedures were not followed and in some cases the courts have extensively elaborated on first principles and fundamental freedoms while failing to make available any tangible remedies or reparation for affected communities. Overall, none of the judgements have held network shutdowns to be illegal falling well below what UN experts have stated. The primary contention of states in relation to imposing internet shutdowns to curtail the spreading of information is belied by the ***Supreme Court of India in Secretary, Ministry of Information and Broadcasting, Government of India v. Cricket Association of Bengal***[98] when turning down the contention of the state in relation to exclusive telecast rights, where the court held that the wider range of circulation of information or its greater impact cannot restrict the content of the right nor can it justify its denial. While addressing the question of mere apprehension relating to law and orderforming the basis for imposition of internet

[84] Association for Progressive Communications. (2020 15 January). *A step closer to realising internet freedoms in India: Supreme Court rules indefinite internet shutdowns are unconstitutional.* Association for Progressive Communications. https://www.apc.org/en/pubs/step-closer-realising-internet-freedoms-india-supreme-court-rules-indefinite-internet-shutdowns
[85] Human Rights Council (2016). Op. cit.; Kaye, D. (2017). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/35/22. https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/35/22
[86] Ibid.
[87] Voule, C. N. (2019). Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association. *United Nations*. https://www.ohchr.org/Documents/Issues/FAssociation/A_HRC_41_41_EN.docx
[88] Kaye, D. (2017). Op. cit.
[89] *Aliansi Jurnalis Independen (AJI) and Pembela Kebebasan Berekspresi Asia Tenggara (SAFEnet) v The Ministry of Communication and Information (Kominfo) and The President of the Republic of Indonesia.* (2020).
[90] *ZLHR and MISA Zimbabwe v Minister of State for National Security and Others*. (2018).
[91] *Global Concern Cameroon v Ministry of Post and Telecommunication, Cameroon Telecommunicationand State of Cameroon*. (2018).
[92] *Amnesty International Togo, L'Institut Des Medias Pour La Democratie Et Les Droit De L'Homme,La Lantere, Action Des Crechretiens L'Abolition De La Torture, Association Des Victim De Tortut Au Togo, Ligue Des Cosnommateurs De Togo, L'Association Togolaise Pour L'education Aux Droits De L'Homme Et La Democratie, Houefa Akpeda Kouassi v The Togolese Republic.* (2020).
[93] *Murad Khazbiev v Federal Security Services.* (2019).
[94] Visit https://docs.google.com/spreadsheets/d/14s7JmGpAoVSTgItLOSNpTpskuUIFFx9MgwZMMn20nUc/edit#gid=0 for more information on the cases.
[95] Rathi, A., Basu, A., & Soni, A. Dialling in the Law: A Comparative assessment of jurisprudence on internet shutdowns. *Association of Progressive Communications*. https://www.apc.org/en/pubs/dialling-law-comparative-assessment-jurisprudence-internet-shutdowns
[96] FAO No. 42/2016 (Islamabad High Court, 2018).
[97] Rathi, A., Basu, A., & Soni, A. Dialling in the Law: A Comparative assessment of jurisprudence on internet shutdowns. *Association of Progressive Communications*. https://www.apc.org/en/pubs/dialling-law-comparative-assessment-jurisprudence-internet-shutdowns
[98] AIR 1995 SC 1236.

shutdowns, the Islamabad High Court in ***CMPak Limited v. Pakistan Telecommunication Authority***,[99] the court held them to be in violation of Section 54(3) of the Telecommunication Act 1996. In this case, the petitioner had challenged the right of the Pakistan Telecommunication Authority to suspend mobile cellular voice and data services on grounds of law and order. The court held that the Authority can impose such shutdowns only in cases where the President of Pakistan has issued a Proclamation of Emergency under the Constitution. The court also cautioned that the unlawful suspension of telecommunication services "may expose the Federal Government or the Authority to claims of compensation or damages by the licensees or the users of the mobile cellular services". However this decision of the Islamabad High Court was overruled by the Supreme Court of Pakistan in ***Ministry of Information Technology and Telecommunications & Pakistan Telecommunication Authority v. CMPak Limited.***[100] Though the Supreme Court agreed with the High Court's limited interpretation of Section 54(3), it held that the shutdowns at issue in this case were actually governed by Section 8(2)(c) of the Telecommunication Re-organisation Act which empowers PTA to take steps pertaining to matters of national security, diplomatic protocols and State functions. Holding that the power under Section 8(2)(c) could be exercised when the shutdowns were temporary, localised and event-specific, the court observed that the only question was whether PTA exercised its power "reasonably, fairly, justly and for the advancement of the purposes of the Act". Examining the shutdown directives issued by PTA as precautionary measures during public holidays or parades, the court held:

> These protective measures are taken on the request of law enforcement authorities in view of past experience of terrorist activities at similar events. If such events caused the issuance of the impugned directions then the same would be in the public interest, reasonable, fair, consistent with the object of the law and therefore valid.

Similar to the approach taken by Pakistani Supreme Court, courts in India have been far more deferential to the power available to the authorities for imposing internet shutdowns. The Gujarat High Court in ***Gaurav Sureshbhai Vyas v. State of Gujarat***[101] turned down the contention of the petitioner that Section 144 of the Code of Criminal Procedure (CrPC) with a broader sweep must not be used and that Section 69A of the Information Technology Act (IT Act) should instead be followed for imposition of internet shutdowns. However, the court held that there was an appropriate use of Section 144 CrPC as this provision and Section 69A IT Act operate in two separate domains. It stated that Section 69A may, in a given case, also be exercised for blocking certain websites, whereas under Section 144 of the CrPC, directions may be issued to certain persons who may be the source for extending the facility of internet access. The High Court of Gujarat held that the temporary ban on internet through mobile phone services was permissible through the invocation of Section 144 as the state government had sufficient justification to prevent public disturbance and maintain public order. The Court further noted that a ban on Internet access may not be considered a per se violation of the right to freedom of expression if such restriction is "minimal". According to the Court in this case which only involved suspension of mobile services, the ban was viewed as a minimal restriction as access to internet through broadband and Wi-Fi services continued.

In a significant judgement, ***Anuradha Bhasin v. Union of India,***[102] while addressing the months' long internet shutdown in Kashmir, the Supreme Court of India held that the indefinite imposition of internet shutdowns is unconstitutional. The court observed that internet shutdowns cannot be ordered to suppress dissent and Section 144 of the Code of Criminal Procedure (CrPC) cannot be mechanically imposed. The court held that periodic reviews of any suspension order must be carried out as per the provisions laid down in Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules 2017 and as such an order suspending internet indefinitely is a violation of these Rules. The court directed the Jammu & Kashmir administration to publish all Section 144 and internet shutdown-related orders proactively. A Review Committee was sought to be appointed to look into all internet shutdown

[99] FAO No. 42/2016 (Islamabad High Court, 2018).
[100] C.A 977 & 978/2018 (Supreme Court of Pakistan, 2020).
[101] WP (PIL) No. 191 of 2015 (Gujarat High Court, 2015).
[102] WP (C) 1031/2019 (Supreme Court of India, 2020).

orders. Given the significant inconvenience caused to people, the state was directed to consider allowing government websites, e-banking facilities, hospital services and other such essential services in regions where the internet services are not likely to be restored immediately. While civil society has largely welcomed this verdict,[103] there was palpable disappointment at the court falling short of providing actual remedy, holding states accountable or ordering restoration of services.[104]

In contrast, in ***Banashree Gogoi v. Union of India,***[105] the Guwahati High Court issued an interim order directing the government to restore mobile internet services of all Mobile Service Providers in the state of Assam. The court deliberated on the suspension of mobile and broadband internet due to protests, wherein the government of Assam eventually restored broadband services while continuing suspension of mobile internet. The Court held that no material was submitted by the state to demonstrate or satisfy that there were sufficient disruptions, incidents of violence or a deterioration of law and order to justify the ongoing restrictions. The failure of the state to show that the situation that prevailed on the date of issuance of the initial Notification for suspension subsist as on date; the apparent shift to a state of normalcy in the lives of the citizens and diminishing of the period of acute public emergency formed the basis of the court's decision. However, the government was allowed to take steps to curb and stop dissemination of explosive messages or videos on various social media platforms which may have a tendency to incite violence and disruptions affecting public safety on cogent and justifiable grounds and materials.

Similarly, in ***Dhirendra Singh Rajpurohit v. State of Rajasthan,***[106] while dealing with an instance where the Divisional Commissioner had imposed internet shutdowns to prevent cheating during an examination, the Jodhpur High Court picked up on the immediate pressing need to resume internet services, which was the ongoing competitive exams for the post of constable and also stated in the order that the internet should not be shut down in the future during competitive exams. Following the judgement in ***Anuradha Bhasin,*** the petitioners in ***Foundation of Media Professionals v. Union Territory of J &K***[107] challenged the continued suspension of 4G services in Jammu & Kashmir. In this case, the Supreme Court of India held that the fundamental rights of citizens need to be balanced with national security concerns, when the situation so demands. In considering the proportionality of the restriction, the court observed that a blanket order was passed for the entire Union Territory of Jammu and Kashmir regions, rather than for specified at risk areas. Despite recognising the failures of the Indian government to abide by the ruling in Anuradha Bhasin when implementing internet restrictions, the court did not find that the impugned order was unconstitutional. Rather, in consideration of the "compelling circumstances" regarding terrorist activity in the region, the court ordered the constitution of a Special Committee to oversee the extent and duration of the restriction. After this judgement, contempt proceedings have been initiated against the government of India since no information was available in public domain regarding the functioning of the Special Committee. In the course of the hearings for the contempt petition, the Indian government finally agreed to a "carefully calibrated easing" of restrictions on 4G services in Jammu & Kashmir, over a year after the restrictions were first imposed.[108]

Of particular importance in the Anuradha Bhasin case was the declaration that an internet shutdown, as restriction on the freedom of speech and expression, must fulfil the requirements under Article 19(2) of the Indian Constitution. These requirements are first that there must be a law providing for the action, second that the restriction must be reasonable and third, it must be in order to further the interest of sovereignty and integrity,security of state, public order, or

[103] Association for Progressive Communications. (2020, 15 January). A step closer to realising internet freedoms in India: Supreme Court rules indefinite internet shutdowns are unconstitutional. *Association of Progressive Communications*. https://www.apc.org/en/pubs/step-closer-realising-internet-freedoms-india-supreme-court-rules-indefinite-internet-shutdowns.
[104] Sircar, S. (2020 11 January). Can't Suspend Internet Indefinitely: SC on J&K's 158-Day Shutdown. The Quint. https://www.thequint.com/news/india/supreme-court-judgment-jammu-and-kashmir-internet-shutdown
[105] 2019 SCC Online Gau 5584.
[106] D. B. Civil Writ No. 10304/2018 (Rajasthan High Court, 2018)
[107] Writ Petition D. No. 10817/2020 (Supreme Court of India, 2020).
[108] Internet Freedom Foundation (2020 11 August). Govt. agrees to staggered restoration of 4G mobile internet in J&K before the Supreme Court. https://internetfreedom.in/staggered-4g-restoration-j-k/

any of the other grounds mentioned in the text of Article 19(2). The court in this case rejected the argument of the petitioner that restrictions can never equal complete prohibition and stated that the same is allowed in certain appropriate cases. As per the court, the requirements to impose a complete prohibition are first that there must not be an excessive burden on free speech and the government must justify why complete prohibition was the least restrictive measure and, second that the existence of a complete prohibition is a question of fact. Further, they held that the test for proportionality would necessarily involve the prioritisation of different interests at stake.[109]

[109] Rathi, A., Basu, A., & Soni, A. Dialling in the Law: A Comparative assessment of jurisprudence on internet shutdowns. *Association of Progressive Communications*. https://www.apc.org/en/pubs/dialling-law-comparative-assessment-jurisprudence-internet-shutdowns

# Privacy and surveillance

Comprehensive legislative frameworks establishing and protecting the right to privacy, particularly in digital spaces, are yet to be put in place in four of the South Asian countries which are covered within this report, with Nepal being the only country to pass a privacy law. In this context, it is perhaps fairly unsurprising that jurisprudence on issues related to digital privacy and surveillance across these countries is also rather limited. This chapter will analyse available jurisprudence which establishes or interprets the constitutional right to privacy in digital spaces, as well as case laws relating to communications surveillance, data protection and digital identity systems.

## International law on digital privacy and surveillance

The right to privacy is established in Article 12 of the UDHR, which states that:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Article 17 of the ICCPR also provides that "no one shall be subject to arbitrary or unlawful interference with his privacy, family or correspondence." General Comment No. 16 of the Human Rights Committee, while interpreting the scope of Article 17, has stated that:

> Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited….The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorised by law to receive, process and use itand is never used for purposes incompatible with the Covenant.[110]

Between 2013 and 2018, the United Nations General Assembly (UNGA) had adopted four resolutions and the Human Rights Council has adopted three resolutions on the "Right to Privacy in the Digital Age".[111] These resolutions condemned unlawful or arbitrary surveillance and interception of communications as "highly intrusive acts" that interfere with fundamental human rights. They call upon all States to respect and protect the right to privacy in digital communication and to review their procedures, practices and legislation related to communications surveillance, interception and collection of personal data. These resolutions also emphasise the need for States to ensure the full and effective implementation of their obligations under international human rights law.

## Establishing a constitutional right to digital privacy

The right to privacy is expressly guaranteed by the Constitutions of Pakistan, Nepal and Bangladesh. In Bangladesh, jurisprudence applying and interpreting this constitutional right is scarce,[112] and there are no reported cases from the High Court or Supreme Court which apply the right to privacy in the digital context that we could access.Though Pakistan's Constitution explicitly recognises the right to "privacy of home", Pakistani courts have failed to develop a robust doctrine which lays down an expansive right to privacy linked to the right to life and dignity.[113] However, in some cases, Pakistani courts have interpreted the constitutional right to privacy more broadly to include issues such as protection from communications surveillance and protection of personal data. In ***Benazir Bhutto v. President of Pakistan,***[114] Justice Saleem Akhtar in his concurring opinion (joined by Justice Fazl Ilahi Khan) held that the term privacy of home "symbolises the security and privacy of a nature which a person enjoys in his home". Noting that the "inviolability of privacy is intrinsically linked with the dignity of man", Justice Akhtar held that a person's privacy whether within or outside

[110] Human Rights Committee. (1988). General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence and Protection of Honour and Reputation. United Nationshttps://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f6624&Lang=en

[111] G.A. Res. 73/179 (Dec. 17, 2018); H.R.C. Res. 34/7 (Mar. 23, 2017).

[112] Silvee, S. & Hasan, S. (2018). The Right to Privacy in Bangladesh in the Context of Technological Advancement. *International and Comparative Law Journal 1(2)*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3298069

[113] Digital Rights Foundation (2017). A Data Protection Law in Pakistan: Policy Recommendations. *Digital Rights Foundation*. https://digitalrightsfoundation.pk/wp-content/uploads/2017/10/Policy-Brief-for-MOIT.pdf

[114] PLD 1998 SC 388.

the home or even in public spaces needs to be protected from illegal intrusion. In ***MD Tahir v. Director, State Bank,***[115] the Lahore High Court ruled on the validity of a State Bank circular which required all banks to provide personal information about customers (such as name, National Identity Card number, National Tax Number, address) who had received interest from the bank in excess of a certain amount to the Central Board of Revenue.

Referring to Article 14 of the Constitution, the Court opined that "[i]t can hardly be denied that taking of private information without any allegation of wrongdoing of ordinary people is an extraordinary invasion of this fundamental right of privacy". Noting that the public gave their personal details to banks on a "fiduciary understanding" that their details will be kept secret in the absence of specific wrongdoing, the Court held that deposits in banks constitute "manifestly the creation of a safe and secure environment" which the State cannot attempt to pry into. Hence, the State Bank circular failed the test of reasonableness and violated Article 14 of the Constitution. These decisions suggest that the constitutional right to privacy can be extended to cover digital privacy as well.[116] In Nepal, the constitutional right to privacy was extended to apply in the digital space in the landmark case of ***Baburam Aryal v. Government of Nepal.***[117] This case established that the right to privacy is a human right. The surveillance of private activities by the government or a third party is a violation of privacy in the digital era. The court found that the right to privacy is related to the right to be left alone and any breach of privacy by the government or the third party is condemned by this right.

Unlike Pakistan, Nepal and Bangladesh, the Constitutions of India and Sri Lanka do not explicitly recognise privacy as a constitutional right. In India, the question of whether privacy is a fundamental right was authoritatively addressed by a nine-judge-bench of the Indian Supreme Court in the case of ***Justice K.S. Puttaswamy v. Union of India***[118] (hereinafter referred to as ***Puttaswamy I***). In the landmark judgement which is expected to have far-reaching consequences, the Supreme Court held that "the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution". The legal confusion that existed with respect to the right to privacy in India, caused by a number of ambiguous judgements, was finally laid to rest, with the Court in ***Puttaswamy I*** overruling past decisions of the Supreme Court which had held that the right to privacy was not protected by the Constitution.[119]

As such, any law that affects privacy will now be subject to a constitutional scrutiny. The judgement sets out three fundamental aspects of an individual's right to privacy, namely, intrusion with an individual's physical body, informational privacy and privacy of choice. The Court expansively defined the right to privacy, holding that privacy was intrinsic to freedom, liberty, dignity and recognising privacy as a necessary basis of other fundamental rights such as the freedom of speech, association, movement, liberty, conscience and the right to live life with dignity. The judgement also notes that privacy has both positive and negative content, which restrains the State from committing an intrusion upon the life and personal liberty of a citizen, while alsoimposing a positive obligation on the State to take all necessary measures to protect the privacy of the individual. Clarifying that the right to privacy is not absolute, the Court has held that any restrictions on privacy must meet the test of "fair, just and reasonable" and must fulfil the test of proportionality. Any restriction to privacy must therefore meet the following three criteria i.e. (i) existence of a law (ii) must serve a legitimate State aim and (iii) the extent of interference must be proportionate.

All the Judges in ***Puttaswamy I*** highlighted the importance of informational privacy (i.e. the protection of personal information) in the electronic age, where data is easily accessed, aggregated, transferred and mined. Crucially, Justice Chandrachud's plurality opinion (on behalf of 4 judges including himself[120]) recognised that "[t]he dangers to privacy in an age of information

[115] 2004 CLD 1680 Lahore.
[116] *Digital Rights Foundation* (2017). Op. cit.
[117] *Baburam Aryal vs GoN*. NKP (2017), N.S.C 9740
[118] 2017 (10) SCALE 1.
[119] *MP Sharma & Others v. District Magistrate, Delhi & Others* 1954 SCR 107; Kharak Singh v. State of Uttar Pradesh & Others (1964) 1 SCR 334.
[120] The remaining five judges each wrote separate opinions

can originate not only from the state but from non-state actors as well." The Court highlighted the need for a data protection legislation and highlighted the privacy concerns relating to digital surveillance. The expansive definition of the right to privacy laid down in ***Puttaswamy I***, which recognises the importance of privacy in its varied dimensions, laid the foundation for many more decisions applying the fundamental right to privacy to issues such as data protection, surveillance, transparency and the right to information, free speech and bodily autonomy.[121] However, worryingly, the Court also seemed to envision a broad range of reasons for which the right to privacy could be restricted, including for the purposes of national security, "public interest" and the like.[122] In contrast to the approach of the Indian Supreme Court, Sri Lankan Courts have yet to establish the right to privacy as a constitutional right. In fact in 2008, the Sri Lankan Supreme Court, in ***Advisory Opinion, SC Reference No. 1 of 2008*** recognised that the right to privacy was protected under various provisions of common and statutory law, though not under the Constitution and concluded that Sri Lanka's legal framework adequately protects the right to privacy established under Article 17 of the International Covenant on Civil and Political Rights.[123] However, such piecemeal protection of privacy rights cannot substitute the recognition privacy as a fundamental right, given that the current legal framework in Sri Lanka does not adequately protect privacy in all its varied dimensions (especially since the data protection laws are yet to come into effect) and does not allow an individual to hold the government accountable for invasion of their privacy rights.[124]

**Surveillance**

Some of the landmark cases on privacy rights in South Asia were handed down in the context of communications surveillance and telephone tapping. In Nepal, the case of ***Baburam Aryal v. Government of Nepal***[125] established that the surveillance of private activities by the government or a third party was a violation of privacy in the digital era. In this case, a writ petition was filed in the Nepali Supreme Court claiming a violation of individual privacy after a news report on an ongoing criminal investigation indicated the extent of government surveillance of phone calls and text messages. The court held that surveillance could be permitted only during times of emergency or in the name of national security, after following certain procedures. As a result, the court ruled that it was illegal to provide details of an "individual's private phone call details and SMS" for "unpermitted objectives".[126] Importantly, the court also stated that telecommunication service providers, while providing the service must protect the privacy of individuals and also the information related to them. Without a proper legal order or in the absence of an authenticated formal application in writing, no unauthorised access to such information should be allowed.[127]Thus, an order of the district court is required before personal information is accessed for criminal investigations.

In ***People's Union for Civil Liberties v. Union of India***[128] ***(PUCL),*** the Indian Supreme Court in 1996 held that the right to privacy included telephone conversations held in the privacy of one's home or office and that tapping of such telephone conversations would violate the right to privacy "unless it is permitted under the procedure established by law". While upholding the validity of Section 5(2) of the Indian Telegraph Act which allowed interception of communications in certain circumstances, the Court narrowly interpreted the terms "public emergency" and "public safety", which were the grounds under which an interception order could be issued under Section 5(2). In addition, the Court laid down a series of guidelines to regulate the government's power of surveillance, which included a number of procedural safeguards aimed at protecting the right to privacy including a requirement that the order be issued by the Home Secretary (though this power can be delegated in urgent cases), time limits on the validity of the surveillance order,

[121] Bhatia, G. (2017). The Supreme Court's Right to Privacy Judgment: I - Foundations. https://indconlawphil.wordpress.com/2017/08/27/the-supreme-courts-right-to-privacy-judgment-i-foundations/amp/
[122] Arun, C. (2017, 25 August). Data Privacy: Great Idea, but there's room for the State to step in. *Indian Express*. https://www.newindianexpress.com/opinions/2017/aug/25/data-privacy-great-idea-but-theres-room-for-the-state-to-step-in-1647907.html
[123] Supreme Court Advisory Opinion, SC Reference No. 1 of 2008.
[124] Edrisinha. R. & Welikala, A. (2016). *Civil and Political Rights in the Sri Lankan Constitution and Law: Making the New Constitution in compliance with the ICCPR*, Centre for Policy Alternatives. http://constitutionalreforms.org/wp-content/uploads/2016/06/Working-Paper-8.pdf
[125] *Baburam Aryal vs GoN*, NKP (2017), N.S.C 9740
[126] Aryal, B (2018). Privacy in Digital Age: Judicial Approach in South Asia. CPR South. http://dx.doi.org/10.2139/ssrn.3275123
[127] Pradhan, D. & Kansakar, A., (2020, March) Nepal - Data Protection Overview. https://www.dataguidance.com/notes/nepal-data-protection-overview#:~:text=The%20Supreme%20Court%20held%20that,concerned%20person%20has%20been%20obtained.
[128] AIR 1997 SC 568.

maintenance of records and the establishment of a review committee. However, the Court declined to provide for prior judicial scrutiny as a safeguard in all cases of tapping.

Shortly after the decision in the PUCL case, the Pakistani Supreme Court in 1998 in ***Benazir Bhutto v. President of Pakistan***[129] (***Benazir*** case) dealt with the issue of tapping the telephones of Judges, political leaders and military officials by the ruling government. The Court held that tapping of telephones and eavesdropping on citizens is a violation of the right to privacy guaranteed under Article 14 of the Constitution and if tapping were to be allowed with legal justification, "it can be done only when grave risk to the security of the country is involved". The illegal tapping of telephones was in fact one of the grounds under which the Court upheld the dissolution of Benazir Bhutto's government by the President. In the separate opinion of Justices Akhtar and Ilahi Khan, it was ordered that since the Telegraph Act itself failed to lay down the procedure for regulating the tapping of telephones, any communications surveillance carried out by the government in the future must be done with the "prior permission of the Supreme Court or by a Commission constituted by the Supreme Court which shall examine each case on its merits".

In both the ***PUCL*** and ***Benazir*** cases, it was also held that telephone tapping violated the right to freedom of speech and expression since the lack of privacy on the telephone would impact the ability of the speaker to freely express her thoughts and opinions. However, unlike in ***PUCL***, the majority opinion in the ***Benazir*** case failed to lay down specific guidelines and procedural safeguards under which the government would be allowed to intercept communications. It appears that the direction in Justice Akhtar's opinion requiring prior permission of the Supreme Court for tapping telephones was never implemented and in fact a connected suo moto inquiry which had been initiated by the Pakistani Supreme Court in 1996 to look into the tapping of telephones is still pending before the Supreme Court.[130]

In India, though the ***PUCL*** guidelines were implemented by amendment of the rules issued under the Telegraph Act and have influenced the Indian government's exercise of its surveillance powers, the lack of judicial scrutiny has resulted in the guidelines being flouted with impunity in practice.[131] Building on the observations in the ***Benazir case***, Justice Shah of the Pakistani Supreme Court expanded on the constitutional protection against government surveillance in his dissenting opinion in ***Justice Qazi Faez Isa v. The President of Pakistan & others.***[132] Noting that the only statute in Pakistan which permitted surveillance was the Investigation for Fair Trial Act (IFTA), which permits surveillance only on obtaining a court warrant during the pendency of a criminal investigation, Justice Shah observed:

> Any covert surveillance or interception of the citizens of Pakistan other than under IFTA is starkly offensive to their fundamental rights of privacy and personal liberty. There is no law in the country that authorises any law enforcementor intelligence agency to pry into the privacy of home to dig out private family information through targeted surveillance and to use it against them to achieve various ends.

The Indian Supreme Court in Puttaswamy I while outlining the contours of the right to privacy recognised the heightened risk to privacy caused by newly available modes of digital surveillance including through profiling, use of "big data" and the like. The proportionality and legitimacy test for judging the validity of restrictions on privacy as laid down in ***Puttaswamy I***, was subsequently applied by the Bombay High Court in ***Vinit Kumar v. Central Bureau of Investigation.***[133] In this case, an order to intercept the phone calls of a businessman in the course of investigating him for corruption, was challenged. The High Court noted that the orders for the interception of Kumar's communications were ostensibly issued on the grounds of "public safety". The Court held that there was nothing in the CBI's argument that justified "any ingredients of risk to the people at large or interest of public safety, for having taken resort to the telephonic

[129] PLD 1998 SC 388.
[130] Malik, H. (2015, 22 May). Over 5000 being tapped by IB, SC Told. The Express Tribune. https://tribune.com.pk/story/890674/over-5000-phones-being-taped-by-ib-sc-told
[131] Ramachandran C. (2014). PUCL v. Union of India Revisited: Why India's Surveillance Law must be Redesigned for the Digital Age. *NUJS Law Review* 7 105.
[132] Constitution Petition No.17 & 19 of 2019 [Pakistan Supreme Court, 2020].
[133] W.P. 2367/2019 (Bombay High Court, 2019).

tapping by invading the right to privacy". The Court held that the three interception orders did not have the "sanction of law", were not issued for a legitimate aim and so did not satisfy the test of proportionality and legitimacy as set out in ***Puttaswamy I.*** It ordered destruction of the intercepted messages and held that the CBI could not use the evidence obtained by intercepting communications without following proper procedure.

**Privacy and national identity programmes**

Digital identity systems backed by biometric data are well-established in India and Pakistan and are in the process of development in Bangladesh, Nepal and Sri Lanka.[134]

The National Database and Registration Authority (NADRA) was established in Pakistan as far back in 2000 and is one of the world's most extensive citizen registration regimes.[135] There have been numerous reported data breaches and civil society organisations have raised concerns as to the impact on citizens' privacy and potential for mass surveillance. Pakistani courts have yet to opine on the constitutional validity of NADRA's biometric identity scheme in relation to the right to privacy. However, in ***Justice Qazi Faez Isa v. The President of Pakistan & others,***[136] which was a case linked to a presidential reference filed against a Supreme Court Judge on the issue of non-declaration of spousal assets, the investigation team and Asset Recovery Unit (ARU) had obtained personal records of the Judge and his family from NADRA. In his dissenting opinion, Justice Shah found that the disclosure of the personal records of the Judge by a NADRA employee to the ARU violated not only the confidentiality provision in Section 28 of the NADRA Ordinance, 2000, but also the constitutional rights to personal liberty and privacy. Justice Shah recommended that appropriate legal action be taken against the NADRA official who violated this confidentiality requirement.

Given the burgeoning development of digital national identity systems across South Asia, the decisions of the Indian Supreme Court regarding India's national identity scheme could have a profound impact on jurisprudence across the region. India's unique identity number project, known as Aadhaar, relies heavily on digital infrastructure and contains biometric data of over a billion people, such as photographs, fingerprints and iris scans, which are stored in a centralised database. It is governed by the provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016. In 2018, in the case of ***Justice K.S. Puttaswamy v. Union of India***[137] (hereinafter referred to as ***Puttaswamy II***), the Supreme Court of India upheld the constitutionality of the Aadhar programme, finding that any violations of the right to privacy were covered within the reasonable restrictions to this constitutional right as permitted by the Indian Constitution. The Supreme Court, while upholding the constitutionality of Aadhaar, found that there were sufficient safeguards in place to protect the data of Aadhaar card holders. The Court also opined that it believes enrolment in the programme to be fool proof and that biometric data cannot be replicated, despite many instances disproving this conclusion. However, in its judgement, the court has imposed numerous restrictions on and conditions under which the Aadhaar scheme must be implemented, in order to meet the test of proportionality for protecting the constitutional right to privacy of Indian citizens.

*First*, the judgement has limited the access of corporate entities, including banks, to the details of individuals stored in the Unique Identification Authority of India (UIDAI) database. The portion of Section 57 of the Aadhar Act 2016 that enabled such corporate access has been declared to be unconstitutional and as a result, corporate bodies can no longer demand authentication via Aadhaar. The mandatory linking of Aadhaar to bank accounts and SIM cards was thus rendered invalid. *Second*, the court has held that authentication

[134] Prasad, S. & Aravindakshan, S. (2020). Playing catch up – privacy regimes in South Asia. *The International Journal of Human Rights*. https://www.tandfonline.com/doi/full/10.1080/13642987.2020.1773442
[135] Privacy International & Digital Rights Foundation (2019). State of Privacy - Pakistan. https://privacyinternational.org/state-privacy/1008/state-privacy-pakistan
[136] Constitution Petition No.17 & 19 of 2019 [Pakistan Supreme Court, 2020].
[137] (2019) 1 SCC 1.

records cannot be kept beyond a period of six months, as opposed to the five-year period permitted under the Aadhaar Act and has also held that maintaining a database relating to transactions is impermissible.

*Third*, Section 33(1) of the Aadhaar Act which authorised a district judge to permit disclosure of an Aadhaar number, has been read down, clarifying that an individual whose information is sought to be released shall be afforded an opportunity of hearing and appeal against a decision permitting disclosure. Similarly, another part of the Section permitting disclosure on the basis of national security has been struck down and the state has been asked to reframe the Section within the framework prescribed by the Court.

*Fourth*, children were provided the right to exit the Aadhar programme on attaining the age of majority.

In a strongly worded dissenting opinion, Justice Chandrachud takes a rights-based approach to technology and holds the entire Aadhaar Act and the programme to be unconstitutional. The dissenting opinion recognises the weakness of biometric data, in terms of the loss of control over it by individuals and the security architecture behind the programme.[138] Justice Chandrachud's dissenting opinion was quoted with approval and relied on the Jamaican Supreme Court in 2019 in ***Robinson, Julian v. The Attorney General.***[139] Noting the real threat of a surveillance state caused by such digital identity programmes, the Jamaican Supreme Court found that Jamaica's national identity system was unconstitutional.

**Data protection**

The data protection regime is underdeveloped in all these countries and with Nepal being the only country to pass a law protecting personal information and data. Data protection bills pending in India, Pakistan and Sri Lanka. Though Bangladesh's Digital Security Act has some provisions relating to data protection, these are extremely limited in their scope. The Privacy Act of Nepal has certain provisions relating to data protection,[140] though experts have noted the limited definition of personal data and the fact that most of the data protection obligations are limited to public bodies as major shortcomings in the law.[141] Jurisprudence relating to data protection is also quite scarce. The Indian Supreme Court in ***Puttaswamy I***, the Court called on the Indian government to put in place a robust data protection regime. In this regard, the Court highlighted the importance of ensuring that personal information is not used without the consent of the data provider and that the data is only used for the purpose and to the extent which it was disclosed.

[138] Association for Progressive Communications. (2018, October). APC calls for strong data protection safeguards following the Supreme Court of India's verdict on Aadhar, India's biometric identity programme. https://www.apc.org/en/pubs/apc-calls-strong-data-protection-safeguards-following-supreme-court-indias-verdict-aadhar

[139] 2018 HCV 01788.

[140] Articles 12 and 25, Privacy Act 2018. http://www.lawcommission.gov.np/en/archives/20722

[141] Greenleaf, G. (2019). Advances in South Asian data privacy laws: Sri Lanka, Pakistan and Nepal. *Privacy Laws & Business International Report* 22-25. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3549055; Rayamajhi S. (2018 16 July). Right to Privacy Nepal. Rayz News. https://www.rayznews.com/right-to-privacy-bill-of-nepal/

# Freedom of expression

## Overview of challenges in relation to freedom of expression

Freedom of expression and opinion, the foundation stone of every free and democratic society, faces new and exacerbated challenges in online spaces. Throughout South Asia and the world, people have taken to social media and online platforms to express themselves in ways that were not possible through traditional offline mediums. In response to this and to the reach of the internet, states have sought to regulate and control online speech and expression. Offline regulations, typically in penal legislation, are applied to online spaces, to bolster internet-specific legislation

These legislations regulate various facets of freedom of expression including political, religious, artistic and sexual expression. The primary means through which freedom of expression is impeded is through blocking or filtering, takedowns and criminalisation. APC's 2017 research titled *Unshackling Expression: A study on laws criminalising expression online in Asia*[142] sheds light on how digital laws and penal legislations are used to target online expression.

The study found that offline regulations, typically in penal legislation, are applied to online spaces, to bolster internet-specific legislation. Legitimate expression on the internet is increasingly being redefined as cybercrime. The range of expression online currently being criminalised includes content related to religion, sexual expression, gender identity, political opinion, dissent and factual statements – prosecuted as blasphemy, obscenity, sexual deviance, sedition and criminal defamation. States rely on legal provisions relating to public order, national security, decency and religion-based exemptions to crack down on legitimate forms of expression and dissent.

Offline laws are also used to target online activities in addition to online specific laws, multiple legal provisions are used to target "single offence" and harsher punishments are prescribed for the online realm as compared to offline.

While the states studied as part of this report share similarities in how freedom of expression is regulated, there are many divergent trends too. Each state uses a unique combination of legal provisions to target online speech and the definitions of different provisions, while similar, differ across the states. The constitutions of these five states guarantee the right to freedom of opinion and expression to their citizens. In none of these states is this right absolute and the states lay down justifications for the curtailment of the right in their constitutions or other legal documents. Some of the prominent justifications that states provide to restrict freedom of speech are national security, friendly relations between states, public order, decency, blasphemy, morality, contempt of court, incitement to an offence. These justifications are commonly used by States to crack down on even legitimate forms of expression, including political, artistic and sexual expression.

In terms of digital rights jurisprudence, a significant portion related to freedom of expression and criminalisation. Oftentimes, national and international law providing guarantees for freedom of expression are central to the contentions before the court.

## International norms on the freedom of expression

The right to freedom of opinion and expression is a crucial right in the UDHR and the ICCPR. Article 19 of the ICCPR as well as the UDHR guarantees the right to hold opinions without interference and guarantees everyone the right to freedom of expression and the right to receive and impart information, regardless of frontiers. Any limitations placed on this right must meet the standards required and justified by provisions in Article 19(3) of the ICCPR.

[142] https://www.giswatch.org/2017-special-report-unshackling-expression-study-law-criminalising-expression-online-asia

Article 19 of the ICCPR reads:

> (1) Everyone shall have the right to hold opinions without interference;
>
> (2) Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice…

As the text of the right makes clear, the right to freedom of opinion, speech and expression is available regardless of borders or frontiers. More importantly, it is available through any media of one's choice. The Human Rights Council has affirmed that offline human rights must be equally protected and guaranteed online. In its 20th session (29 June 2012), the Human Rights Council adopted a resolution which unanimously declared:

> [T]he same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.[143]

Any limitations placed on the right to freedom of expression must meet the standards required and justified by provisions in Article 19(3) of the ICCPR which allows curtailment of the right for respect of the rights or reputations of others, protection of national security or of public order (order public) or of public health or morals. The Human Rights Committee holds that there shall be no exceptions to the right to hold opinions, whether they are of a "political, scientific, historic, moral or religious nature." In particular, the Committee makes clear that it is unacceptable to criminalise the holding of an opinion, noting that the "harassment, intimidation or stigmatisation of a person, including arrest, detention, trial or imprisonment for reasons of the opinions they may hold, constitutes a violation of article 19, paragraph 1".[144]

In addition to Article 19, Article 20 of the ICCPR also impacts speech. Article 20 prohibits any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence. Speech that falls within the ambit of Article 20 (as hate speech) cannot merely be offensive, but must have an intent to cause harm and be likely to cause harm. That is, for speech to fall within the definition of hate speech, it must have the quality of inciting imminent violence.[145]

In key judgements relating to freedom of expression online in Bangladesh, India, Nepal, Pakistan and Sri Lanka, international law has been referenced and tested against national developments. For instance, in Sri Lanka, the Supreme Court advisory opinion analysed the extent of compliance of provisions of the Constitution and other laws with the rights guaranteed under the ICCPR.[146]

In many of the cases however, international law obligations have not been referred to by courts even when relied on by parties to the case. Often, the cases dealing with free speech online even disregards overall national jurisprudence and principles evolved by national courts on freedom of expression over decades. The decisions impacting freedom of expression online usually involve either the criminalisation or censorship of expression (under various grounds such as national security, public order, religious/communal harmony, obscenity, defamation or contempt of court) or preventing access to content online through measures such blocking, filtering and takedowns.

[143] Human Rights Council. (2012). Op. cit.
[144] Human Rights Committee. (2011). Op. cit.
[145] Khandhadai, G. (2016). Op. cit.
[146] SC Reference No. 1 of 2008 (Sri Lanka Supreme Court, 2008).

## Blocking/filtering

Blocking refers to measures taken to prevent certain content from reaching an end user, including through preventing users from accessing specific websites, IP addresses or taking down websites from the web server where they are hosted.[147] On the other hand, filtering is "commonly associated with the use of technology that blocks pages by reference to certain characteristics, such as traffic patterns, protocols or keywords".[148] Blocking and filtering are the primary means through which states prevent access to content which they believe is inappropriate or unlawful, such as for example, child pornography or content which amounts to incitement to violence, harms national security, infringes intellectual property rights and the like. States' use of blocking and filtering is frequently in violation of their obligation to guarantee freedom of expression, as often content is blocked arbitrarily or excessively. Further, these measures are ineffective as they can often be easily circumvented and carry risks of both over-blocking and under-blocking.[149] In the context of the widespread and arbitrary blocking of content, including legitimate expression the Special Rapporteur on Freedom of Expression has opined that:

> States should provide full details regarding the necessity and justification for blocking a particular website and determination of what content should be blocked should be undertaken by a competent judicial authority or a body which is independent of any political, commercial, or other unwarranted influences to ensure that blocking is not used as a means of censorship… Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3 [of Article 19, ICCPR].[150]

There are a number of cases from South Asian states which deal with the arbitrary blocking and filtering of content online. Jurisprudence regarding the powers of government authorities to order blocking of websites, apps and social media is rather limited in Bangladesh, Nepal and Sri Lanka. Media reports indicate that the Sri Lankan Supreme Court had dismissed a petition in 2012 which challenged the blocking of certain websites.[151] The Sri Lankan government stated that these websites had been blocked for failing to register in accordance with a government requirement[152] that all websites carrying news and current affairs must be registered with the government to ensure that they did not carry defamatory material.[153] However, the Supreme Court refused to accord a full hearing for the case and thus did not decide on the implications of this government order on the freedom of speech and expression.[154] In Bangladesh, media reports refer to a High Court order from 2018 which directed the blocking of all pornographic websites for a period of six months.[155] A copy of the order could not be traced online, however.

In India and Pakistan, the text of Section 37 of the Prevention of Electronic Crimes Act 2016 (PECA) in Pakistan and Section 69A of the Information Technology Act 2000 (as amended in 2008) in India hold some common ground justifying the need for blocking or removing online content.[156] Both provisions allow blocking of content on a number of grounds including integrity or security of state, public order or incitement of an offence. Pakistani law provides additional grounds which permit blocking including for the glory of Islam or in the interest of decency or morality.

In a number of cases, orders to block websites were passed not by government authorities, but rather by Pakistani courts in response to public interest petitions filed requesting blocking of websites on various grounds. For instance, in ***Jamal Akram v. Federation of Pakistan,***[157] the petitioner sought direction for authorities to ban porn websites which were "against the interest of the Muslim community of the Islamic Republic of Pakistan". Justice Chaudhry of the Lahore High Court issued an expansive order and formulated guidelines for the government for blocking of websites containing "objectionable" material such as pornography. These guidelines included that the IMCEW set up the government should keep a "vigilant eye on the websites and in the eventuality of any objectionable material concerning the

[147] La Rue, F. (2011). Op. cit.
[148] Article 19. (2016, December). Freedom of Expression Unfiltered: How blocking and filtering affect free speech. https://www.article19.org/data/files/medialibrary/38586/Blocking_and_filtering_final.pdf.
[149] https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/.
[150] La Rue, F. (2011). Op. cit., p. 13.
[151] Dietz, B. (2012, May), Sri Lanka Supreme Court slams door on websites, Committee to Protect Journalists. https://cpj.org/2012/05/sri-lanka-supreme-court-slams-door-on-websites/.
[152] PTI (2016, 2 March). Sri Lanka makes registration mandatory for news websites. *India Today*. https://www.indiatoday.in/pti-feed/story/lanka-makes-registration-mandatory-for-news-websites-566504-2016-03-02
[153] Sri Lanka Campaign for Peace & Justice (2012, 29 May). Banned websites go to Supreme Court. https://www.srilankacampaign.org/banned-websites-go-to-supreme-court/.
[154] Dietz, B. (2012). Op. cit.
[155] Dhaka Tribune (2018, November). High Court wants all porn sites blocked for six months. *Dhaka Tribune*. https://www.dhakatribune.com/bangladesh/court/2018/11/19/hc-wants-all-porn-sites-blocked-for-6-months.
[156] APC-IMPACT (2017). Op. cit., p. 26.
[157] 2011 PLD 377.

religious faith of any group would take prompt action before it reaches to the public at large", that "the Crisis Cell working in the Services Division ICT Directorate and Enforcement Division shall be used as a tool to unearth such material and to block the relevant websites/URL forthwith and in case of failure stern action be taken against the delinquents"; and "that the government shall also see the viability of permanent blocking of the websites involved in unethical, unIslamic and illegal activities in the event that such material is against presented on internet".

The following year, a similar order was passed in ***Islamic Lawyers Movement v. Federation of Pakistan,***[158] in response to a petition which sought a permanent ban on Facebook as the petitioner was aggrieved about posting of cartoon drawings of the Prophet on Facebook. The Lahore High Court formulated guidelines for the government to ensure that social media websites are not used to spread religious disharmony. Justice Chaudhry passed directions which were almost verbatim to those passed by him a year earlier in the ***Jamal Akram*** case, except this time in relation to spreading religious disharmony.

While Pakistani courts in the above-mentioned cases were encouraging expansive blocking of websites on very broad grounds rather than opposing online censorship, subsequent cases afforded some relief for the protection of free speech online. In ***Bytes for All v. Federation of Pakistan,***[159] a petition was filed challenging the ban on YouTube, which had been blocked in Pakistan since 2012. Through interim orders issued in 2013 and 2014, the Lahore High Court ordered the government to hold consultations with experts to decide on the issue. Based on the recommendations of these experts, the court concluded that the most feasible option for consideration was allowing full access to YouTube with interstitial warnings on pages with objectionable or blasphemous content. However, no final decision was taken in this case, due to the existence of a Supreme Court order from 2012 which directed the Pakistan Telecommunications Authority (PTA) to block blasphemous material on YouTube. A local version of YouTube has since been allowed by the government in Pakistan, which allows the government to demand removal of any content which it deems to be in violation of any provisions of Pakistani law.

Prior to the passage of PECA, the Pakistani government in 2006 had set up the Inter-Ministerial Committee for Evaluation of Websites (IMCEW) which was mandated to issue directives for blocking access to online content and websites. A petition challenging the constitution of the IMCEW and its power to pass blocking orders was filed before the Islamabad High Court in ***Bolo Bhi v. Federation of Pakistan.***[160] Through interim orders, the High Court in its 2014 order required IMCEW to cease to provide "any direction for blocking a website without approval of this Court" and directed the IMCEW to provide details of all websites blocked in the last three years. This interim order was modified in January 2015, allowing PTA to block websites "strictly in accordance with law" and during the pendency of the petition, requiring the PTA to report to the Court explaining the reasons for regulating any particular site. In March 2015, the IMCEW was disbanded and denotified. Between March 2015 and August 2016 when PECA was passed by Parliament, all the content blocking was ad hoc and done by PTA on instructions from different government bodies, without having any legal regulatory power.

In its final decision in 2018, the Islamabad High Court analysed the power of PTA under Section 37 of PECA to block websites and held that the power to block websites is required to be exercised independently by the PTA without being influenced by any direction or information laid before it by the federal government. It held that while exercising its discretionary power, the PTA must not act "arbitrarily and capriciously." The directions by court in this case helped limit interference by the federal government in website blocking orders and clarified the limits of PTA's power to block websites.

[158] 2012 CLC 1300.
[159] WP No. 958/2013 (Lahore High Court, 2013, 2014).
[160] WP No. 4994/2014 (Islamabad High Court, 2014, 2015, 2018).

The limits and contours of PTA's powers to block websites was further delineated by the Islamabad High Court in ***Awami Workers Party v. Pakistan Telecommunication Authority.***[161] In this case, the Awami Workers Party challenged PTA's decision to block their website on national security grounds prior to the general elections. PTA had argued that it had the power to block websites without giving notice or hearing to the person affected by the order. The court held that PTA's interpretation of Section 37 was in "flagrant violation of the fundamental rights guaranteed under the Constitution as well as the settled law enunciated by the superior courts. It is noted that the principles of natural justice are required to be read in every statute". It found that the blocking of the website of the petitioner was in violation of the principles of natural justice and Art 10-A of the Constitution. However, no remedies were granted as the court found that the grievance ofpetitioner was redressed because its website was unblocked by PTA during the pendency of the petition. The court also directed the PTA to prescribe and notify rules under PECA.

The need to follow procedural requirements and safeguards prior to blocking websites was once again stressed upon by the Islamabad High Court in ***Proxima Beta Pte v. Federation of Pakistan.***[162] In this case, the suspension of Player Unknown's Battle Grounds Mobile (PUBG game) by PTA was challenged by the company. The petitioner argued that the temporary suspension of PUBG was beyond the scope of Section 37 of PECA. The Court set aside the temporary suspension of PUBG as the PTA had not issued a formal order banning the game as required under Section 37 (it had only issued a press release) and because the principles of natural justice not followed (a hearing was given to the company only after a decision to temporarily suspend the game was taken by PTA). Immediately after the court order was passed however, the PTA passed a detailed order for blocking PUBG on the grounds that the game was negatively impacting the mental and physical health of the players and thus needed to be blocked as a preventive measure to maintain "public order".[163] This decision was then reversed and the game unblocked within a week after discussions between PTA and the company.[164]

Similar to Pakistan, Indian courts have also passed a few orders directing and regulating the blocking of websites and apps. In an ongoing litigation before the Supreme Court of India, ***Kamlesh Vaswani v. Union of India,***[165] a petition has been filed challenging the constitutional validity of numerous provisions of the IT Act on the ground that they are allegedly insufficient to tackle the issue of pornography. The petition also called for a ban on all online pornography and asks for a direction to the government to treat watching pornography as a criminal offense. Though the case is still ongoing, in the course of the hearing, the court had referred the matter to the Cyber Regulation Advisory Committee, while refusing to pass an interim order for blocking of all pornographic websites. Despite the lack of a court order, during the pendency of the proceedings, the Department of Telecommunications (DoT) had ordered ISPs to block a number of websites for hosting pornographic content. On 31 July 2015, the DoT issued another notification ordering the blocking of 857 porn websites.[166] After public outcry, the DoT clarified its order to note that only websites hosting child pornography need to be mandatorily blocked.[167]

This ban on porn websites was revived by the Uttarakhand High Court in ***Suo moto PIL after gangrape incident,***[168] wherein in the High Court took suo moto cognizance of the gang rape of a schoolgirl, noting that the perpetrators in the case were reportedly influenced by watching pornography online. In its September 2018 interim order, the court ordered all ISPs to "punctually obey" the 2015 DoT notification and "block the publication or transmission of obscene material in any electronic form". The Indian government complied with this order and took steps to block the 857 identified pornographic websites. As a result, porn websites remain blocked in India despite the refusal of the Indian Supreme Court to pass an interim order on this and despite the fact that the ***Kamlesh Vaswani*** case is still pending before the court. The Uttarakhand High Court's

[161] WP No. 634/2019 (Islamabad High Court, 2019).
[162] WP No 1788/2020 (Islamabad High Court, 2020).
[163] Pakistan Telecommunication Authority (2020, July). Decision on Playerunknown's Battlegrounds (PUBG) Online Game under Section 37 of the Prevention of Electronic Crimes Act 2016. No: PTA/IP&WA/Web Analysis/Complaints/Nil/146/2019/.
[164] https://twitter.com/PTAofficialpk/status/1288831986551762946/photo/1.
[165] W.P. (Civil) No. 177/2013.
[166] https://sflc.in/sites/default/files/wp-content/uploads/2015/08/2015-07-31_DoT-block-order-decency.pdf
[167] https://www.newsgram.com/porn-sites-ban/
[168] WP PIL No. 158/2018 (Uttarakhand High Court, 2018).

interim order for such blocking was passed without substantive consideration of the constitutional objections to such ban which have been raised by parties in the ***Kamlesh Vaswani*** case, including the potential violations of the rights to free speech and privacy caused by such a blanket ban.[169]

In ***Sabu Mathew George v. Union of India,***[170] a petition was filed asking for blocking of advertisements related to prenatal sex determination which is illegal in India. The Supreme Court directed the respondents to develop a "technique so that the moment any advertisement or search is introduced into thesystem, that will not be projected or seen by adopting the method of auto-block." It listed around 40 search terms which need to be auto-blocked. The court directed that a nodal agency should be set up which will provide search engines the details of any websites to be blocked if they were acting in contravention of the Preconception and Prenatal Diagnostic Techniques (Prohibition of Sex Selection) Act. Experts have expressed serious concerns about this method of blocking. The dangerous doctrine of auto-block adopted by the Supreme Court in this case leads to over-censorship has an impact on free speech. Because this is a generic ban (where the terms themselves are banned) which is not content-specific, there is a risk of legitimate expression being blocked.[171]

In ***S. Muthukumar v. TRAI***,[172] a writ petition was filed before the Madras High Court asking for a ban on the download and use of Tik Tok which allegedly contained explicit content and was harmful to children. The court, as an interim measure, without hearing the respondents, directed the authorities to ban the download of Tik Tok and prohibited media from telecasting the videos made using the Tik Tok app. The interim order in this case was a form of prior censorship which violates the right to freedom of expression.[173] Tik Tok's parent company appealed to the Supreme Court against this ban. The Supreme Court directed the Madras High Court to decide on the matter immediately, otherwise the interim order would be automatically suspended. After the Supreme Court order was issued, the Madras High Court heard the parties and vacated its earlier interim order banning Tik Tok. However, in response to Tik Tok's argument that the interim order had violated the right to freedom of speech under Article 19 of the Indian Constitution, the court opined that "the creator of a platform for users for commercial purpose may not take shelter under Article 19(1)(a)" without deliberating on the issue. The power of the Indian government to order blocking of websites (as opposed to court-ordered blocks) is governed by the provisions of Section 69A of the IT Act and the Information Technology (Procedures and Safeguards for Blocking Access of Information by Public) Rules issued thereunder. The constitutional validity of Section 69A and the rules were challenged in ***Shreya Singhal v. Union of India.***[174]

The petitioners argued that these provisions were not valid due to the absence of a guaranteed hearing of the author of the content before a decision is made; the limited procedural safeguards when compare to those provided in the case of offline bans (under Section 95 and 96 of the Criminal Code of Procedure); and the requirement for strict confidentiality with respect to all blocking requests.. However, the court upheld the constitutionality of Section 69A and the rules and rejected the petitioners' arguments on the grounds that the provision was narrowly framed and included a number of procedural safeguards, even if they were different from safeguards for offline content.[175]

With the legal backing of Section 69A, in the context of ongoing border tensions with China, the Indian government issued three orders between June to September 2020, blocking over 200 Chinese-linked apps, including Tik Tok on the grounds that they were "prejudicial to sovereignty and integrity of India, Defence of India, Security of State and Public Order".[176] While an Indian court is yet to rule on the validity of this ban, its widespread nature risks setting a precedent which will undermine digital rights in India.

[169] Hariharan G. (2014). *Our Unchained Sexual Selves: A case for the liberty to enjoy pornography privately*. http://docs.manupatra.in/newsline/articles/Upload/AD8AC438-666E-427C-A910-CAFBDBF50C7A.pdf
[170] (2018) 3 SCC 229
[171] Internet Freedom Foundation (2017, 20 February). Statement of concern on the Sabu Mathew George Case: Don't "auto-block" online expression. https://internetfreedom.in/statement-of-concern-on-the-sabu-mathew-george-case-dont-auto-block-online-expression/
[172] WP(MD) No. 7855/2019 (Madras High Court, 2019).
[173] Software Freedom Law Center (2019, 4 August). Madras High Court bans downloading Tik Tok. https://sflc.in/madras-high-court-bans-downloading-tiktok
[174] AIR 2015 SC 1523.
[175] Association for Progressive Communications (2017). Op. cit., p. 68
[176] The Wire (2020, 2 September). In Third blocking order, Indian bans 118 New Chinese-linked Apps. *The Wire*. https://thewire.in/tech/pubg-banned-chinese-apps-blocking-order-tension-pangong-tso

## Political, artistic and sexual expression

Free expression online is restricted through various means, including by criminalisation of certain forms of expression. The cases referred to in this Section deal with restrictions on political, artistic and sexual expression. By political expression, we refer to any form of speech or expression related to political issues, including those which express dissent against the state or are critical of any state policies or actions. Artistic expression on the other hand, refers to information, ideas or opinionswhich are communicated or imparted through an artistic work such as an image, drawing, video, story or the like. Sexual expression as used here refers to sexually explicit content, messages or interactions online amongst adults which are shared with the consent of all parties involved.[177] The focus on political, artistic and sexual expression is due to the fact these forms of expression are most likely to be restricted or suppressed by the state, on grounds such as nationality security, public order, decency or morality. In some cases, expression in an artistic format which seeks to "shock, offend or disturb" is seen as less acceptable than other forms of expression such as speeches or academic writing. In relation to sexual expression, even consensual expression is often conflated with obscenity and is therefore viewed as unacceptable, as opposed to being a legitimate and valid form of expression.

Between 2009 and 2015, a provision of Indian law which became particularly notorious for its chilling effect on online speech was Section 66-A of the IT (Amendment) Act 2008, which criminalised expression that was "grossly offensive", had a "menacing character" or were sent "for the purpose of causing annoyance or inconvenience," among other overly broad grounds.[178] This provision was overused by the Indian government to stifle political dissent online. Section 66-A was struck down as unconstitutional by the Supreme Court of India in 2015 in the landmark case of ***Shreya Singhal v. Union of India.***[179] The court found that it was permissible under Article 14 of the Indian Constitution (the equality clause) to create a specific offence regulating speech on the internet. However, it held that such an offence must meet the same tests for reasonable restrictions to free speech as must be met by laws governing offline speech.

The court struck down Section 66-A in its entirety as unconstitutional for the following reasons: (i) the law failed to establish a clear proximate relation to the protection of public order; (ii) the provision leaves many terms open-ended and undefined, therefore making the statute void for vagueness; (iii) because the provision fails to define terms, such as inconvenience or annoyance, "a very large amount of protected and innocent speech" could be curtailed; (iv) the government failed to show that the law intends to prevent communications that incite the commission of an offense because "the mere causing of annoyance, inconvenience, danger etc., or being grossly offensive or having a menacing character are not offences under the Penal Code at all". As such, the court found that Section 66-A violated the right to freedom of speech and expression under Article 19(1)(a) of the Indian Constitution and could not be covered within the reasonable restriction on free speech prescribed under Article 19(2).

The landmark decision in the Shreya Singhal case upholding free speech online has the potential to set a progressive precedent for other South Asian states as well, many of whom continue to have broad provisions criminalising speech online, similar to the erstwhile Section 66-A. However, within India, many of the principles laid down by the court in Shreya Singhal have not been followed in later cases. Even worse, Section 66-A has continued to be invoked by the police even after it was struck down,[180] forcing the Supreme Court of India to pass further directions for the enforcement of the Shreya Singhal judgement, including closure of existing 66-A cases and directions that fresh cases ought not be registered.[181] The abuse of provisions criminalising online speech is demonstrated in a case from Bangladesh. In ***State v. Md Rafiqul Islam,*** [182] the High Court of Bangladesh took suo moto cognizance of a news report regarding the conviction of a 19-year-old boy under the ICT Act by a mobile court for allegedly sending an offensive message

[177] Ibid.
[179] AIR 2015 SC 1523.
[180] Gupta, S. (2019, 30 June). Section 66A: When a celebrated judgment cannot be implemented by the police. Bar and Bench. https://www.barandbench.com/columns/section-66a-when-a-celebrated-judgment-cannot-be-implemented-by-the-police
[181] *People's Union for Civil Liberties v. Union of India* M.A.No. 3220/2018 in W.P. (Crl.) No. 199 of 2013.
[182] 69 DLR (2017) 18

on Facebook to a lawmaker which contained "abusive" and "humiliating" words. Mobile courts (now declared unconstitutional) in Bangladesh are special courts moving one place to another held by the executive for summary trial of particular offences with a view to maintaining law and order of the country and have been criticised for their lack of independence and for infringing on citizens' rights.[183] In this case, the accused was arrested bythe police, convicted by a mobile court two days later and reportedly sentenced to two years' imprisonment under the ICT Act. Newspaper reports cited the magistrate who tried the case as saying that the conviction was under the ICT Act though the Magistrate could not cite the provision under which the conviction took place. There were no official records of the proceedings before the mobile court. The Bangladesh High Court held that the conviction had no legal effect and ordered a re-inquiry to determine whether any criminal offence was made out. Though this judgement does not contain an analysis of substantive provisions impacting free speech under the ICT Act it is a good example of the abuse of process which takes place in many South Asian countries by law enforcement officials while using vague provisions and implementing laws which criminalise online speech. In many of these cases, even if the decision of an appeals court results in acquittal, "the process is the punishment"[184] as draconian laws are used to arrest, imprison and ultimately stifle free political and artistic expression.

One such case from India of criminal complaints being used to stifle political expression was in ***Anna Vetticad and Jack Dorsey v. State of Rajasthan.***[185] In this case, the Rajasthan High Court was asked to quash the First Information Report (FIR) filed against a journalist and the CEO for Twitter for posting a photo to Twitter featuring the slogan: "Smash Brahminical Patriarchy". The FIR was filed under provisions of the Indian Penal Code relating to outraging religious feelings, defamation and incitement on the basis that the tweet hurt the feelings of the Brahmin community. The Rajasthan High Court held that "by no stretch of imagination" could the phrase "Smash Brahminical Patriarchy" be considered as "hurting the religious sentiments of any citizen of India nor the same can be interpreted as creating a religion-based rift in any Section of society". Finding that the ingredients of the offence were prima facie not made out, the court quashed the FIRs.

In contrast to these cases upholding free speech, the Sri Lankan Supreme Court in ***Sunila Abeysekera v. Ariya Rubasinghe***[186] upheld the validity of multiple emergency regulations issued by the Sri Lankan President during the pendency of the civil war. These regulations prohibited the publication, including by electronic means, of matters "pertaining to official conduct, morale, the performance of the Head or any member of the Armed Forces, or the Police Force or of any other person authorised by the Commander in Chief of the Armed Forces, for the purpose of rendering assistance in the preservation of national security". The petitioners argued that the regulations were unconstitutional as they violated the right to freedom of speech and expression. The Court found that the regulations, though broadly framed, were not vague. The broad framing was justified to take into account changing circumstances. It held that "the regulations in question were not so vague as to exclude any predictability, if need be with appropriate advice". Given that the aim of the regulations was to protect national security, the court stated that a fair balance had been struck between competing interests and that the pressing social need to protect national security outweighed the right to free speech in this case, concluding that "[in] such a situation, national security must take precedence over the right of free speech". In this decision, the court accorded excessive deference to the government, allowing it to stifle political dissent on grounds of national security.

Another case in which free speech was allowed to be restricted in the name of national security and social harmony was in ***Robert Ian Penner v. Department of Immigration***[187] from the Supreme Court of Nepal. A Canadian citizen Robert Ian Penner, residing in Nepal on a work visa, was deported back to Canada by the immigration department. The department revoked his visa and asked him to leave the country within two days on the grounds that his tweets disturbed

[183] Hossain M. (2020), Separation of Judiciary in Bangladesh-Constitutional Mandates and Masdar Hossain Case's Directions: A Post Separation Evaluation. *International Journal for Court Administration* 11(2), 4. https://doi.org/10.36745/ijca.310.
[184] Liang, L. (2012, 25 January). The Process is the bloody punishment. Outlook. https://www.outlookindia.com/website/story/the-process-is-the-bloody-punishment/279699
[185] S.B. Criminal Misc. (Pet) No. 2818/2019 (Rajasthan High Court, 2020).
[186] S.C. Application No. 994/99 (Supreme Court of Sri Lanka 1999).
[187] NKP (2018), N. S.C 10091.

the peace, security and social harmony of the country. Penner's Tweets had criticised the new Nepali constitution, supported the rights of the Madhesi ethnic group and commented on other political matters in Nepal.[188] Penner's petition before the Nepali Supreme Court challenged the deportation order on the grounds that it violated the right to freedom of speech. However, the court established that the fundamental rights on freedom of expression and opinion are exclusive only to its citizens and not to aliens. Penner's deportation caused significant debate and exposed the intolerance of state machineries to political criticism and the differential treatment meted out to non-citizens in relation to legitimate political expression.

Protection of artistic expression came up before an Indian court in the case of ***Ashutosh Dubey v. Netflix Inc,***[189] where an injunction was sought on the webseries Hasmukh on Netflix on the grounds that the show defamed lawyers. Noting that the web series was a satirical comment, a work of art which exaggerated different issues to expose the shortcomings of the profession, the Delhi High Court opined that:

> The very essence of democracy lies in the fact that its creative artists are given the liberty to project the picture of the profession in any manner, including by using satire, to exaggerate the ills to an extent that it becomes a ridicule.

In relation to sexual expression, both online and offline laws prohibiting "obscenity" and "indecency" are used across South Asia to control and censor sexuality and sexual expression.[190] Studies have shown that these provisions are used to criminalise expression which constitutes legitimate political speech as well.[191] For instance, the case of ***Mohammad v. State***[192] dealt with the issue of a man being charged under Section 67 of the Indian IT Act which criminalises publication of obscene content in electronic form. The accused was charged for sending an email to the then Chief Minister of Gujarat which threatened to "finish" the Chief Minister and associated political parties. The Gujarat High Court found that there was nothing obscene or lascivious about the email and ordered the deletion of the charges under Section 67 of the IT Act. Similarly, in ***Linga Bhaskar v. The State***[193], the accused persons were charged under Section 67 of the IT Act merely for sending crying emojis in response to a video by one of their co-workers which showed some customers complaining about the service received from the company for which they all worked. The Madras High Court held that an emoji could not be considered as an overt act on others, but was rather a comment even though it "may be intended to ridicule or to show one's disapproval in a given context." Since there was no sexual content involved in the messages, the Court ordered quashing of the charges under Section 67 of IT Act. Though the charges were struck down by the High Court in both these cases, they demonstrate the misuse of obscenity provisions by police and prosecutors to prosecute other forms of expression as well even if no sexual content is involved.

In addition to criminalisation of sexual expression, as highlighted in the Blocking section above, courts across all five states studied have issued orders at various points of time for blocking of websites hosting pornography.[194] Laws criminalising all sexual expression or court decisions blocking access to and prohibiting even private consumption of pornography further contribute to the portrayal of sexuality as inherently corrupting, while disregarding the importance of consent in any sexual act or in the creation, circulation and publication of images of such acts. In this way, they help to keep existing power relations and their associated conceptions of morality intact.[195]

[188] BBC News. (2016, 3 May). Canadian Man asked to leave Nepal after criticising government on Twitter. *BBC News*. https://www.bbc.com/news/world-asia-36197089
[189] I.A. 3754/2020 in CS(OS) 120/2020 (Delhi High Court, 2020).
[190] EROTICS (2017). South Asia exploratory research: Sex, rights and the internet. Association for Progressive Communications. https://www.apc.org/sites/default/files/Erotics_1_FIND.pdf
[191] Datta, B. (2017). Guavas and Genitals: An exploratory study on section 67 of the Information Technology Act India. Point of View.
[192] SCR.A/1832/2009 [Gujarat High Court, 2010].
[193] CRL.O.P.(MD)No.3110 of 2017 [Madras High Court, 2018].
[194] Freedom Forum. (2016). Freedom of Expression on the Internet in Nepal. Kathmandu: Freedom Forum; Sydney Morning Herald (2009, 25 July). Sri Lanka Court blocks 100 porn websites. https://www.smh.com.au/technology/sri-lanka-court-blocks-porn-websites-20090725-dwov.html.
[195] Association for Progressive Communications (2017). Op. cit. p. 65.

**Blasphemy and hate speech**

The rights to freedom of expression and religion are often portrayed as being in opposition with each other. This notion is particularly strong in South Asia, where multiple religions and cultures coexist. Religion and discussions about religion in South Asia are a central part of social, cultural and political life. A significant portion of online expression that has come into debate or been subjected to state action in South Asia touches on religion on religious sensitivities. A 2015 report, *Desecrating Expression: An Account of Freedom of Expression and Religion in Asia*[196] discussed the intersection between these rights, highlighting violations and laws that impinge on freedom of expression in the name of protecting the sanctity of religion.

The rights to freedom of expression and freedom of religion are internationally recognised and guaranteed rights that are crucial for any democratic society. The right to religion is intrinsically linked to freedom of opinion and expression, freedom of association and assembly, as well as other human rights and fundamental freedoms. These rights, individually and collectively, guarantee and contribute to the building of peaceful, inclusive, pluralistic, tolerant, progressive and democratic societies.

In addition to Article 19 of the ICCPR which guarantees freedom of expression, Article 18 of the ICCPR guarantees freedom of thought, conscience and religion. Article 20 of the ICCPR declares that any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law. The Constitutions of the States studied as part of this report also provide explicit guarantee for freedom of religion.

Although Bangladesh was declared a secular State in 1972, subsequent amendments to the Constitution of Bangladesh, such as Article 2A, declare Islam as the State religion and provides equal status and rights to other religions.[197]

Article 12 and Article 41 of the Constitution provide for secularism and freedom of religion. Sections 295, 295A and 298 of the Penal Code of Bangladesh impose punitive measures for making derogatory comments against one's religious belief. Section 57 of the Information and Communication Technology Act included hurting religious belief as basis for criminal action. This Section has since been repealed and replaced by the Digital Security Act however, pending proceedings under the provision are allowed to continue. Section 28 of the Digital Security Act states that publication or broadcast of "any information that hurts religious values or sentiments" is a criminal offence. Provisions of the Anti-Terrorism Act subsequent to amendments in 2013 are also a threat to freedom of expression in the context of religion, as persons can be targeted for expressing views that are seen as anti-state.

In India, the Preamble of the Constitution of India explicitly recognises the secular nature of the State while Articles 25, 26 and 28 guarantee and limit freedom of religion and conscience. Sections 153-A 153-B and 505 of the Indian Penal Code (IPC), deal with hate speech, Section 295A penalises those who insult religion or religious freedoms and Section 298 deals with uttering words that may wound religious feelings. Besides these a vast body of provisions are used to address hate speech in India.[198] Section 66 A of the Information Technology Act had criminalised speech that spreads hatred; however, this provision has been declared unconstitutional by the Supreme Court of India.[199] The Law Commission in India is currently preparing a law on hate speech.[200]

In Pakistan, Article 2 of the Constitution of Pakistan recognises Islam as the official state religion. Article 20 guarantees freedom of religion for all, including sects. The 1974 amendment to the Constitution resulted in Articles 106 and 260, which excluded Ahmadis (also known as Qadianis), terming them non-Muslims. The Pakistan Penal Code sets out various offences against religion. Sections 153-A and 505 deal with hate speech, Section 295(A) penalises acts done to outrage religious feelings. Sections 295(B) and 295(C) have severe provisions for blasphemy, defilement of the Quran or insulting Prophet Muhammad, including life imprisonment and death penalty. Section 298 specifically deals with

[196] Khandhadai G.(2016). Op. cit.
[197] Arzt, D. (1990). The application of international human rights law in Islamic states. Human Rights Quarterly 202-230.
[198] Center for Communication Governance. (2018). Hate Speech laws in India. *National Law University, Delhi.* https://ccgnludelhi.wordpress.com/2018/05/04/launching-our-mapping-report-on-hate-speech-laws-in-india/
[199] *Shreya Singhal v. Union of India* AIR 2015 SC 1523.
[200] Singh, V. (2018 19 March). Centre plans law on online hate speech. The Hindu. https://www.thehindu.com/news/national/centre-moves-for-law-on-online-abuse/article23295440.ece

words uttered that wound religious feelings. Section 298(A) penalises any insults to any wife or family member of Prophet Muhammad. Sections 298(B) and 298(C) target Ahmadis and other groups penalising them for posing as Muslims or for preaching or propagating their faith. The Telegraph and Publication Act along with many regulations are used to target books and other writings. The Protection of Pakistan ordinance was enacted to tackle terrorism and the National Action Plan on security has provisions which can be used to detain and prohibit expression touching on religious issues. Section 37 of the PECA, contains a list of restrictions allowing the PTA to block, remove and censor online content, giving the PTA full discretionary powers to restrict access to "any" information if it considers it necessary to do so on a number of grounds, including morality and in the interest of integrity of Islam.

Article 26 of the Constitution of Nepal guarantees freedom of religion while prohibiting the exercise of the right in a manner which is contrary to public health, decency and morality, public order, or acts aimed to convert a person of one religion to another, or to disturb the religion of other people. The Constitution also gives the power to restrict freedom of expression in the name of reasonable restrictions on any act which undermines amongst other things the harmonious relations between various castes, tribes, religions or communities or any act of hatred or incitement to caste-based untouchability as well as gender discrimination. Section 65 of the National Penal (Code) Act 2017 prohibits acts that are prejudicial to the harmonious relationship between different communities, including on the grounds of religion.[201] Section 15 of the National Broadcasting Act prohibits the broadcast of various matters, including materials misinterpreting disregarding, insulting and devaluing any tribe, language, religion and culture.

Article 9 of the Constitution of Sri Lanka requires the state to give Buddhism the foremost place. Articles 10 and 14(1)(E) guarantee freedom of religion. The Penal Code of Sri Lanka provides for offences relating to religion in Sections 290, 290(A), 291, 291(A), 291(B) and 292. Section 291(A) addresses any expression that wounds religious feelings. Section 81 of the Criminal Procedure Code, which deals with maintaining peace, has also been used to target expression on the basis of religion. Section 3(1) of the International Covenant on Civil and Political Rights (ICCPR) Act 2007 prohibits propaganda for war or advocacy for hatred. The Prevention of Terrorism Act which seeks to protect minority religious and ethnic groups has been used to crackdown on expression on the pretext of protection, particularly Section 2(1)(H) (which relates to causing religious disharmony and hostility) and Section 14 (approval for publications). These are used in tandem with Public Security Ordinance and other such national security laws and regulations. The Press Council Law in Section 15 targets the publication of materials, including those that insult a religion or its founder, deities and so on. This and other regulations are applied along with the Profane Publications Act.

While blasphemy relates to offences broadly referred to as "defamation" or "insulting" religion, hate speech deals with a wholly different form of speech. There is no internationally agreed definition of hate speech, however, recent documents have framed common understanding of the term. The basis for curtailing hate speech emanates from restrictions prescribed for speech under Article 19 (3) of the ICCPR and Article 20 which requires that any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.

The UN Strategy and Plan of Action on Hate Speech[202] defines hate speech as any kind of communication in speech, writing or behaviour, that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are, in other words, based on their religion, ethnicity, nationality, race, colour, descent, gender or other identity factor. For the purposes of this Section, we will only be examining hate speech on the basis of religion.

[201] National Criminal (Code) Act 2017. http://www.moljpa.gov.np/en/wp-content/uploads/2018/12/Penal-Code-English-Revised-1.pdf
[202] https://www.un.org/en/genocideprevention/documents/UN%20Strategy%20and%20Plan%20of%20Action%20on%20Hate%20Speech%2018%20June%20SYNOPSIS.pdf

Former UN Special Rapporteurs Ms. Asma Jahangir and Mr. Doudou Diene explain that the right to freedom of religion or belief protects primarily the individual and, to some extent, the collective rights of the community concerned but it does not protect religions or beliefs per se. While the exercise of freedom of expression could in concrete cases potentially affect the right to freedom of religion of certain identified individuals, it is conceptually inaccurate to present this phenomenon in abstract as a conflict between the right to freedom of religion or belief and the right to freedom of opinion or expression.[203]As noted in numerous other reports by the UN Special Rapporteur on freedom of religion, international human rights law protects individuals, not religion or belief itself. The right to freedom of religion or belief, as enshrined in the relevant international standards, does not include the right to have a religion or a belief that is free from criticism or ridicule. These experts have repeatedly called on states to decriminalise blasphemy laws as they are contrary to international law and have also expressed concerns on application of blasphemy regulations to online content and on the other hand failure to curb incitement to violence, discrimination and hate on the basis of religion through online mediums. [204]

Despite this, jurisprudence in South Asia has largely sought to protect and retain blasphemy provisions and has extended it to online spaces, while doing little to curb hate speech and incitement to violence. Courts in Pakistan for instance, have of their own volition sought blocking of content that insults religion as seen in the earlier Section. In ***Salman Shahid v. Federation of Pakistan,***[205] the Islamabad High Court passed directions to the Government to take "immediate and strict action" to restrict blasphemous content online, including through blocking of websites. Similarly, in ***Muhamad Ayoub v. Federation of Pakistan,***[206] the Lahore High Court in a petition relating to allegedly inflammatory and blasphemous content on Facebook pages, directed blocking these pages on social media. The court further directed that if the authorities were not successful in blocking access to the blasphemous content, the government should consider amending PECA to allow the Pakistan Telecommunications Authority to block entire websites that fail to remove blasphemous content (such as blocking access to Facebook entirely). The court also recommended the introduction of a specific blasphemy offence in PECA in line with Sections 295 to 295-C of the Pakistan Penal Code. While passing these orders, the court observed that "distortion of any religion on the pretext of right of speech/expression or information now amounts to another form of terrorism".

However, the same High Court in ***Bytes For All v. Federation of Pakistan,***[207] placed the onus on individuals by observing that:

> We as a nation need to regulate ourselves rather than take up a defenceless battle against the digital age and the global information available on the world wide web. In the end, the responsibility and the choice is of the individual to watch or not to watch controversial websites as the same cannot be effectively blocked according to the level of technology present in our country today.

This case related to a petition challenging the blocking of YouTube for hosting allegedly blasphemous content. The Lahore High Court concluded, based on consultations with Ministries and experts, that the most feasible option for consideration was allowing full access to YouTube with interstitial warnings on pages with objectionable content. A local version of YouTube has since been allowed by the government in Pakistan, which allows the government to demand removal of any content which it deems to be in violation of any provisions of Pakistani law.

In ***Islamic Lawyers Movement v. Federation of Pakistan,***[208] the Lahore High Court called for greater state action. This case relates to cartoons and drawing of the Prophet, which the petitioner claimed injured the religious feelings of Muslims, thus seeking a permanent ban on Facebook. The High Court formulated guidelines for the government to ensure that social media websites are not used to spread religious disharmony.

[203] Jahangir, A. (2005). Report of the Special Rapporteur on Freedom of Religion and Belief to the 61st session of the Commission on Human Rights. E/CN.4/2005/61.
[204] Shaheed, A. (2019). Report of the Special Rapporteur on Freedom of Religion and Belief to the 40th session of the Human Rights Council.A/HRC/40/58. https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/40/58 port of the Special Rapporteur on Freedom of Religion and Belief to the 61st session of the Commission on Human Rights. E/CN.4/2005/61
[205] W.P. No. 739/2017 (Islamabad HC, 2017).
[206] 2018 P Cr LJ 1133
[207] WP No. 958/2013 (Lahore High Court, 2013, 2014).
[208] 2012 CLC 1300 215 Human Rights Committee (2011). Op. cit.

It recommended that the Inter-ministerial Committee for the Evaluation of Websites (IMCEW), which operated prior to the enactment of PECA, should not even wait for complaints from the public, but should take action on their own as if the objectionable material reached the public, then the purpose of IMCEW and the Crisis Cell of the IT Department would "fall to the ground". The court in this case is encouraging both prior censorship and continuous monitoring of online content by the government in order to restrict blasphemous content online, completely ignoring international human rights standards relating to free speech.The courts in Pakistan have also widened the jurisdiction for courts in dealing with criminal sanctions against individuals for allegedly blasphemous content on social media.

In ***Muhammad Abdul Rauf Siddiqui v. SHO,***[209] the Sindh High Court in a case where the accused made an allegedly blasphemous statement about the Prophet at a press conference which was broadcast widely on electronic media and posted on the internet, held that courts have jurisdiction to take cognisance of the offence where the consequences of the offence was felt even if the place where the press conference was held did not fall under its jurisdiction. This is particularly worrisome given the vast reach of social media, essentially making it possible for multiple cases to be filed across the expanse of a country.

In relation to hate speech online, there are a few instances of action by courts by upholding convictions and calling for state action. In ***Asim Nawaz v. The State***,[210] the Lahore High Court upheld the conviction of the accused under Section 11-W of the Anti-Terrorism Act for posts on Facebook that were held to instigate sectarian hatred. The court held that in view of the material available on the record that they were of the view that the prosecution has successfully proved this case beyond shadow of doubt by producing relevant and admissible evidence. The High Court however does not discuss whether the posts themselves amount to hate speech.

In ***High Court Bar Association v. Government of Balochistan,2***[211] the Balochistan High Court took suo moto notice of a case concerning the murder of twenty-six persons belonging to a particular sect by a banned organisation and in relation to print and electronic media broadcasting and printing propaganda of banned organisations and extremists. The High Court ordered authorities to take action to prosecute print and electronic media under Section 11-W of the Anti-Terrorism Act if they propagated/ disseminated the views of banned organisations or extremist and hate literature. While nothing specific about electronic media was explicitly stated, the directions are equally applicable. In this case, some media representatives had submitted before the court that they received threats from terrorist organisations which forced them to publish the propaganda in fear of an attack. However, the court opined that:

> We however do not consider the same to be a justification for violating the law and the Constitution of Pakistan and if anyone does so he will have to face the consequences provided in the law. It is also not expected that the media, which is stated to be the fourth pillar of the State, would undermine or weaken the integrity and the cohesion of the State and the people residing within it.

Similarly, in ***Tehseen S. Poonawalla v. Union of India***,[212] before the Supreme Court of India, the petitioner, a social activist, had asked for action against the cow protection groups indulging in violence, including lynchings, which had resulted in international outrage. The petitioner also asked the court to issue directions to remove violent content from social media uploaded and hosted by the said groups. The Supreme Court issued guidelines to prevent lynching and mob violence. The court directed the government to take steps to prohibit instances of dissemination of offensive material through different social media platforms or any other means for inciting such tendencies by initiating criminal action against perpetrators. The government was required to set up a task force to procure intelligence about people who are likely to commit such crimes or who spread hate speech and fake news. The government was directed to register FIRs under Section 153-A IPC (promoting enmity between groups based on religion etc.) or other relevant provisions against people who disseminate irresponsible and explosive messages and videos having content which is likely to incite mob violence and lynching of any kind.

[209] 2013 P CrLJ 70.
[210] 2019 P CrLJ 920.
[211] PLD 2013 Balochistan 75.
[212] (2018) 9 SCC 501.

**Defamation**

Defamation is categorised as both a civil wrong and a criminal offence in four out of the five states studied, i.e. in Bangladesh, India, Nepal and Pakistan. Sri Lanka is the only one of these countries which repealed its criminal defamation law as far back as in 2003.[213] Criminal defamation lawshave been frequently utilised to suppress free speech (including online speech) across South Asia in a manner which is inconsistent with international human rights standards.[214] In this regard, the Human Rights Committee has called for states to "consider the decriminalisation of defamation" and noted that "the application of the criminal law should only be countenanced in the most serious of cases and imprisonment is never an appropriate penalty."[215]

In both India and Pakistan, the offence of criminal defamation is covered under Sections 499 and 500 of the respective Penal Codes and is defined as spoken or written words or visible representations, concerning any person intended to harm his/her reputation. Exceptions to this include an "imputation of truth" required for a "public good", or the conduct of any person touching any public question, or expressing opinions on a public performance. The Indian Supreme Court recently upheld the validity of the criminal defamation law in India, holding that it was a reasonable restriction on the constitutional right to freedom of speech and expression.[216]

The application of defamation laws to online spaces has come up before South Asian courts in a number of cases. In India, in the case of ***Tata Sons Limited v. Greenpeace International,***[217] Tata Sons Ltd. sued Greenpeace and sought a permanent injunction and damages for defamation on the grounds of unauthorised use of trademark and loss of reputation for the company. The suit was in relation to a game launched by Greenpeace, based on Pacman, titled "Turtles v. Tata", where the turtles are portrayed as escaping the Tata logo to protest the impact of Tata's industrial activities on Olive Ridley turtles.[218] In this case, Tata had argued that an injunction was necessary (and that damages would be insufficient) because the "publication" took place on the internet, which had a greater impact than other mediums. The Delhi High Court however rejected the possibility of setting a different standard for internet publications while deciding on whether to grant an injunction restraining publication, stating:

> That an internet publication has wider viewership, or a degree of permanence and greater accessibility, than other fixed (as opposed to intangible) mediums of expression does not alter the essential part, i.e. that it is a forum or medium.

The Court relied on common law jurisprudence for temporary injunctions in defamation cases to hold that such an injunction before the trial takes place was an unreasonable restriction on freedom of speech. A similar view was taken in a later decision of the Delhi High Court in ***Ashutosh Dubey v. Netflix Inc,***[219] where a permanent injunction was sought against the webseries Hasmukh on Netflix on the grounds that the show defamed lawyers. The Delhi High Court refused to grant an ad interim injunction on the grounds that such an injunction would interfere with the right to freedom of speech and expression guaranteed under Art. 19(1)(a) of the Indian Constitution. In contrast, in ***Swami Ramdev v. Facebook***,[220] a yoga guru Swami Ramdev was able to obtain injunctions from the Delhi High Court for the takedown of an allegedly defamatory video and related content summarised the contents of a book which had been found to be defamatory in an earlier case. In that case, the book "Godman to Tycoon – The Untold Story of Baba Ramdev" was found to be defamatory since it contained insinuations of alleged criminal behaviour by Ramdev and alleged financial irregularities in his businesses which damaged his reputation based on "unverified" allegations.[221]

[213] Jha, J. Defamation laws in South Asia: Abolish criminal defamation. *Lokaantar*.214 Association for Progressive Communications (2017). Op. cit.
[214] Association for Progressive Communications. (2017). Op. cit.
[215] Human Rights Committee (2011). Op. cit.
[216] *Subramaniam Swamy v. Union of India* (2016) 7 SCC 221.
[217] CS(OS) 1407/2010 (Delhi High Court, 2011).
[218] Abraham, R. (2011 13 April). *Tata and the Turtles. Greenpeace India*. https://www.greenpeace.org/india/en/story/2937/tata-and-the-turtles/
[219] I.A. 3754/2020 in CS(OS) 120/2020 (Delhi High Court, 2020).
[220] CS (OS) 27/ 2019 (Delhi High Court, 2019).
[221] CM (M) 556/2018 (Delhi High Court, 2018).222 PLD 2011 Karachi 484.

Another issue of concern for courts in relation to online defamation is the question of what constitutes publication for the purposes of the defamation offence. This issue arose before the Sindh High Court in Pakistan, in ***A. Khalid Ansari v. Mir Shakil Ur Rahman,***[222] where the plaintiff sued for defamation based on an email which he had received from an editor-in-chief of a media group. This email merely forwarded another email from a journalist which contained the allegedly libellous material. Since the email was sent only to the plaintiff and not published to a third party, the court held that the mere forwarding of an allegedly defamatory email to only the person who was defamed does not meet the publication requirement of the defamation offence. The Delhi High Court in India, in ***Khawar Butt v. Asif Nazir Mir***[223] was faced with the question of whether republication on the internet constituted a fresh offence. In this case, the defendant had shared on Facebook a pamphlet which contained allegedly libellous material. On the question of whether the suit was barred by limitation, the Delhi High Court adopted the single publication rule (the limitation period begins at the time of the first publication of the allegedly defamatory material, even if content remains online or copies continue to be sold later). It rejected the plaintiff's contention that the publication on Facebook gave rise to a continuous cause of action which amounted to a fresh publication every time the allegedly defamatory content remained on the website. The Court found that if presence of alleged defamatory material on a website would suffice to give a continuous cause of action, then the purpose of the law of limitation would be defeated.

**Contempt of court**

Contempt of court is explicitly recognised in all five states as a permissible restriction on the constitutional right of freedom of expression. Criminal contempt provisions have been broadly applied to prosecute and punish statements which are critical of court decisions. Two landmark cases from India and Bangladesh are discussed in this context, which demonstrate how criminal contempt laws are being used to stifle free speech and dissent online.

In ***Abul Kalam Azad v. David Bergman***,[224] a foreign journalist working in Bangladesh had published three articles on his blog on issues surrounding the Bangladesh Liberation War of 1971. These articles included criticism of the International Crimes Tribunal for holding a trial where the defendants were absent, as well as criticism regarding its failure to inquire into the exact number of people who had died during the war. In a contempt proceeding against the journalist, the Tribunal opined that while it welcomed post-verdict criticism, criticism on a matter under judicial consideration which intended to "derogate the institutional image and authority of the Tribunal" could not be allowed. The Tribunal held that Bergman's criticism of its in absentia trial (which was published post-verdict) was a deliberate attempt to "lower down and demean the tribunal's authority and ability that finally tends to shake the public confidence upon the judicial machinery of the Tribunal and its governing Statute." It ruled that the freedom of speech does not protect a criticism, even a post judgement criticism, that "create[s] debate and mystification in the mind of the public as to fairness, dignity, image, judicial process and independence of the Tribunal." For foregoing reasons, the Tribunal found Bergman in contempt and imposed imprisonment "till rising of the court" and imposed a fine.

The Supreme Court of India took a similar approach in the case of In ***Re Prashant Bhushan & Another***,[225] where it took suo moto notice of two tweets by advocate Prashant Bhushan and initiated contempt proceedings. The first tweet related to the Chief Justice of India (CJI) riding an expensive motorcycle belonging to a political leader during lockdown and commented that the CJI "keeps the SC in Lockdown mode denying citizens their fundamental right to access Justice". The second tweet noted the role of the Supreme Court and particularly the last four Chief Justices of Indias in the destruction of democracy in India. With regard to the first Tweet, the Supreme Court held that any statement related to the CJI in his individual capacity would not amount to contempt. However, the second portion of the tweet which noted that the Supreme Court was kept in lockdown mode denying access to citizens'

[222] PLD 2011 Karachi 484
[223] CS(OS) 290/2010 (Delhi High Court, 2013).
[224] 5 CLR (2017) 7.
[225] *Suo moto* Criminal Contempt Petition No 1 of 2020 (Supreme Court of India, 2020).226 Human Rights Committee (2011). Op. cit

fundamental right to access justice was held to be "patently false" and "had the tendency to shake the confidence of the public at large in the institution of the judiciary and the institution of the CJI". With regard to the second Tweet, the Court while determining whether it was made in good faith took into account the manner of publication("the publication by Tweet reaches millions of people") and opined that the Tweet was malicious in nature and had the tendency to scandalise the court. It found that the content cannot be said to be a fair criticism of the functioning of the judiciary, made bona fide in the public interest. The Court held that the Tweets amounted to criminal contempt and imposed a nominal fine of Rupees 1 as punishment.

In its General Comment No. 34, the Human Rights Committee has stated that for contempt proceedings to comply with the ICCPR, "such proceedings and the penalty imposed must be shown to be warranted in the exercise of a court's power to maintain orderly proceedings".[226] Both the cases referred to above are examples of courts using their contempt jurisdiction to clamp down on legitimate criticism against judicial performance or judicial decisions by journalists, lawyers and human rights defenders. Such decisions create a chilling effect on free speech and are not in compliance with international human rights law.

**Intermediary liability**

An internet intermediary is an entity which provides services that enable people to use the internet. There are many different kinds of internet intermediaries which fall into two broad categories: "conduits" and "hosts". "Conduits" are technical providers of internet access or transmission services. Conduits do not interfere with the content they are transmitting other than for automatic, intermediate or transient storage needed for transmission. "Hosts" are providers of content services – for instance, online platforms and storage services.[227]
Intermediaries, especially social networks, search engines and aggregators as well as messaging services have a significant impact on how people and communities exercise or face violations of digital rights through ICTs. The UN and more specifically the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has repeatedly called on these platforms to root their community standards in international human rights law especially when dealing with content moderation.[228] The Global Network Initiative describes "intermediary liability" as the allocation of legal responsibility to content providers of all kinds for regulated categories of content.[229] "Internet intermediary liability" means the legal responsibility ("liability") of intermediaries for illegal or harmful activities performed by users through their services. "Liability" means that intermediaries have an obligation to prevent the occurrence of unlawful or harmful activity by users of their services. Failure to do so may result in legal orders compelling the intermediary to act or expose the intermediary to civil or criminal legal action.[230]

Regulation of social media is coming, as the UN Special Rapporteur famously said.[231] This is particularly true in South Asia. In the States studied, offline regulations have been extended to deal with intermediary liability and ICT specific laws also cover the issue. Several guidelines are in the pipeline to regulate the functioning of intermediaries. However, civil society has raised concerns regarding the lack of transparency in public-private cooperation between intermediaries such as Google, Facebook, Twitter, etc. and the latter's compliance with state's requests for disclosure and takedowns.[232]

In Bangladesh, provisions of the Digital Security Act (DSA) including Section 8 are used for ordering blocking and takedowns. Under Section 38 of the DSA, intermediaries will not be held liable if it's proven that the concerned violation was committed without their knowledge or that they had taken all measures to prevent the occurrence of the

[226] Human Rights Committee (2011). Op. cit.
[227] Association for Progressive Communications (2014, May). Frequently asked questions on Intermediary Liability. *APC*. https://www.apc.org/en/pubs/apc%E2%80%99s-frequently-asked-questions-internet-intermed; Comninos, A. (2012). *The liability of internet intermediaries in Nigeria, Kenya, South Africa and Uganda: An Uncertain Terrain*. Johannesburg: APC, p. 5. https://www.apc.org/en/node/15649/
[228] Kaye, D. (2018, 6 April). Report of the on the promotion and protection of the right to freedom of opinion and expression to the 38th session of the Human Rights Council. A/HRC/38/35. https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/38/35. Rizvi, S. (2018 11 July). Content regulation: State responses to report on freedom of opinion and expression. *Association for Progressive Communications*. https://www.apc.org/en/news/content-regulation-state-responses-report-freedom-opinion-and-expression
[229] https://globalnetworkinitiative.org/policy-issues/intermediary-liability-content-regulation/
[230] Comninos, A. (2012). *The liability of internet intermediaries in Nigeria, Kenya, South Africa and Uganda: An Uncertain Terrain*. Johannesburg: APC, p. 5. https://www.apc.org/en/node/15649/
[231] Kaye, D. (2019, June 6). The clash over regulating online speech. *Slate*. https://slate.com/technology/2019/06/social-media-companies-online-speech-america-europe-world.html
[232] APC-IMPACT (2017). Op. cit.233 The Centre for Internet and Society (2016). *Internet Intermediaries in South Asia*. Centre for Internet and Society. http://responsible-tech.org/wp-content/uploads/2016/06/CIS-Draft-2.pdf

offence. In addition, Section 79 of the ICT Act also provides that intermediaries shall not be liable under the ICT Act for any third-party information or data made available by the intermediary the offence or contravention was committed without their knowledge or they exercised due diligence to prevent the commission of such offence. However, greater clarity is needed on the framework for intermediary liability[233] and scope of these safe harbour provisions as well as the measures which intermediaries need to take to avoid liability.[234] These concerns are also shared by industry bodies and the private sector.[235]

In India, multiple regulations impact intermediary liability.[236] Intellectual property related regulations such as the Copyright Act of 1957, as amended by the Copyright (Amendment) Act 2012 provides for take down of material which infringes valid copyrights. Section 79 of the Information Technology Act 2000, as amended by the Information Technology (Amendment) Act 2008 specifies "safe harbour" protection available to online intermediaries. Under Section 79, intermediaries are only absolved from liability if they function as platforms and not speakers and if they do not "initiate, select the receiver or modify" information being transmitted.[237] According to Section 67C of the IT Act intermediaries are required by law to "preserve and retain certain specified information for specific durations in a manner prescribed by the Central Government".

In addition, the Information Technology (Intermediaries Guidelines) Rules 2011 (to be read with Section 79 of the IT Act) and the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules 2009 (to be read with Section 69A of the IT Act) also regulate intermediaries. The Intermediaries Guidelines require intermediaries to observe "due diligence". Among other obligations, the Guidelines specifies that an intermediary must take down infringing material upon receiving "actual knowledge". The draft Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018 is currently under consideration.

Nepal is currently considering the Information Technology Bill. Section 91 of the bill states that it is mandatory for social network sites to register at the Department of Information and Technology to operate in Nepal and intermediaries will be banned for not doing so. Section 92 of the bill gives the Department of Information and Technology direct power to remove any content through a social network, which is commonly referred to as a notice-and-takedown system. "Social network" in the bill includes all information and communication technology-based platforms where people and organisations interact or share content. This would include everything from Facebook, Twitter, Instagram to messaging services like Viber. Even the more secure platforms like WhatsApp and Wire would fall under the purview of the laws enacted through this bill.[238]

In Pakistan, Section 38 of PECA limits civil or criminal liability for service providers for content posted by users, unless it is proven that the service provider had "specific actual knowledge and wilful intent to proactively and positively participate" in crimes committed under PECA. However, experts have expressed concerns about the use of vague terms such as "wilful" for determining the liability of intermediaries under this provision.[239] The government has recently proposed the draft Removal and Blocking of Unlawful Content (Procedure, Oversight and Safeguards) Rules 2020 to specifically address content on social media and the responsibility of intermediaries to comply with orders.[240] At the time of the publication of this report, the text of the Removal and Blocking of Unlawful Content (Procedure, Oversight and Safeguards) Rules 2020 was not available online. This draft replaced and rebranded the Citizens Protection (Against Online Harm) Rules 2020. The Online Rules which was issued under PECA

[233] The Centre for Internet and Society (2016). Internet Intermediaries in South Asia. Centre for Internet and Society. http://responsible-tech.org/wp-content/uploads/2016/06/CIS-Draft-2.pdf
[234] Barik, S. (2019, 23 July). Bangladesh's Digital Security Bill can have a chilling effect on free speech: Asia internet coalition. *Medianama*. https://www.medianama.com/2019/07/223-bangladeshs-digital-security-bill-can-have-a-chilling-effect-on-free-speech-asia-internet-coalition/
[235] Asia Internet Coalition. (2019 18 June). Industry Submission on Bangladesh Digital Security Act 2018. *Asia Internet Coalition*. https://aicasia.org/wp-content/uploads/2019/07/Industry-Submission-on-Bangladesh-Digital-Security-Act.pdf
[236] Sflc.in. (2020, January). *The Future of Intermediary Liability in India*. Sflc.in. available at https://sflc.in/sites/default/files/2020-01/SFLC.in%20-%20Intermediary_Liability_Report_%282020%29_1.pdf
[237] Center for Communication Governance (2018). Op. cit.
[238] Social Media: Report on New IT Bill of Nepal Criminalising FoE in Social Media. https://www.slideshare.net/ShreedeepRayamajhi/report-on-new-it-bill-cirminalization-of-foe-in-social-media-by-shreedeep-rayamajhi
[239] Freedom House (2017). *Pakistan - Freedom on the Net* 2017. https://freedomhouse.org/sites/default/files/FOTN%202017_Pakistan.pdf
[240] Ahmadani, A. (2020, 2 October). Govt outlines new rules to remove or block unlawful social media content. *Pakistan Today*. https://www.pakistantoday.com.pk/2020/10/02/govt-outlines-new-rules-to-remove-or-block-unlawful-social-media-content/

contained provisions which allowed government authorities to demand that social media companies "remove, suspend, or disable" access to content within 24-hours (or six-hours in an "emergency"), as well as required them to "deploy proactive mechanisms" to prevent live streaming of online content.[241]

Sri Lanka does not currently have any law regulating digital media or governing intermediary liability. New laws which will regulate social media as well as address cyber security issues are planned by the Sri Lankan government.[242] It is anticipated that this new law will have provisions regulating intermediary liability and providing for a notice and takedown procedure for harmful content online.[243]

A significant portion of jurisprudence on intermediary liability comes to the fore in cases that deal with takedowns, most of which are from courts in India.[244] Judgements have broadly dealt with the process and power for takedowns, instances of harmful content being taken down or blocked, platforms being blocked for hosting content that violates national regulation, directions in relation to defamatory content and intellectual property concerns.

The most significant clarification comes from the Supreme Court of India in ***Shreya Singhal v. Union of India,***[245] where the court held that online content could be taken down from intermediary platforms like Facebook or Twitter only by a court's order or at the behest of the government. In this case, constitutional validity of Section 79 of the IT Act was challenged. The court held that Section 79 was valid subject to the Section being read down to mean that an intermediary upon receiving actual knowledge from a court order or on being notified by the appropriate government or its agency that unlawful acts are going to be committed, then fails to expeditiously remove or disable access to such material. As such, after this case, intermediaries in India are no longer liable to remove content on requests from private entities. The Supreme Court also clarified that the "actual knowledge" requirement under the law was in relation to information received through a "court order or on being notified by an appropriate government or its agency". Failure to comply with such orders and notices implies that intermediaries will not be granted "safe harbour" protection available under the IT Act.

However, despite this progressive decision protecting speech in the ***Shreya Singhal*** case, later cases from both the Indian Supreme Court and High Courts have ignored these directions in relation to intermediary liability. For example, in the case of ***S. Muthukumar v. TRAI***[246], a ban was imposed on Tik Tok by the Madras High Court (as discussed in the Blocking and Filtering Section above), through an interim order without considering the safe harbour provisions available to Tik Tok as an intermediary under the IT Act. While overturning the ban in its final decision, the Madras High Court noted that it was concerned about multiple reported incidents where women and children using cyber space were victimised. Referring to the fact that Tik Tok had removed about six million videos which had "doubtful content" after its interim order, the Court was convinced that the respondent had a pro-active take-down mechanism to deal with content abuse and complaints. The court considered the reply affidavits filed by Tik Tok and its parent company as an undertaking to ensure that any negative and inappropriate content would be filtered. In the event of any violation of the undertaking, the Respondents would be held liable in contempt of court.

In ***Sabu Mathew George v. Union of India***,[247] in addition to the orders on auto-blocking (which has been addressed in the section on Blocking and Filtering above), the court also stated that intermediaries are obliged to keep unlawful content from appearing on their networks. Both these cases contradict the ***Shreya Singhal*** ruling as intermediaries in these cases are being asked to exercise their personal judgement and proactively filter for illegal content on their platforms. However, requiring such proactive filtering of content is highly ineffective, as recognised by the Lahore High Court in ***Bytes for All v.***

[241] Digital Rights Monitor (2020, 28 October). PTA denies knowledge of the updated Rules; confusion on implementation status continues. *Digital Rights Monitor*. http://www.digitalrightsmonitor.pk/pta-denies-knowledge-of-the-updated-rules-confusion-on-implementation-status-continues/

[242] Mudalige, D. (2019 1 June). Laws to regulate social media soon. *Daily News*. http://www.dailynews.lk/2019/06/01/local/187191/laws-regulate-social-media-soon

[243] Economy Next. (2020, January 27). Sri Lanka drafting laws to control social media: *Defence Ministry*. *Economy Next*. https://economynext.com/sri-lanka-drafting-laws-to-control-social-media-defence-ministry-42446/

[244] https://sflc.in/policy-tracker/court-cases for an overview of cases in India.

[245] AIR 2015 SC 1523

[246] WP(MD) No. 7855 of 2019 (Madras High Court, 2019).

[247] (2018) 3 SCC 229.234 Barik, S. (2019, 23 July).

***Federation of Pakistan,***[248] where the blocking of YouTube by the Pakistani government was challenged. The court ordered the government to hold consultations with experts to decide on the issue. Based on the recommendations of these experts, the court concluded that the most feasible option for consideration was allowing full access to YouTube with interstitial warnings on pages with objectionable or blasphemous content. A local version of YouTube has since been allowed by the government in Pakistan, which allows the government to demand removal of any content which it deems to be in violation of any provisions of Pakistani law.

Courts have relied on amicus and expert support to develop solutions in relation to harmful content. In the ***Muthukumar*** case, the court appointed an amicus. In ***Re Prajwala,***[249] an ongoing litigation, the Supreme Court of India through interim orders constituted a Committee to assist and advice the court on the feasibility of preventing sexual abuse and violence videos from online spaces and circulation. The court ordered an inquiry by the central investigation agency into the specific cases highlighted by the petitioner. The Committee constituted by the Court provided several recommendations which included which included blocking of websites and specific search terms. The court directed all parties which included the State and intermediaries such as Google, Facebook, Microsoft, Yahoo! and WhatsApp to implement the recommendations. The Courts in India have also shown considerable concern in relation to the mental wellbeing of children and cautioned against online games that encourage suicide. The Madras High Court in ***The Registrar (Judicial) v. Secretary to the Government***[250] took suo moto cognizance, following suicides prompted by the Blue Whale challenge,[251] also known as the suicide game, which was viral in online spaces. Building on earlier instances of courts ordering blocking (including the auto-blocking orders in the ***Sabu Mathew George*** case), directions were issued to the State to ensure that all service providers comply with national legal provisions governing ICTs, particularly the IT Act and that this includes compliance by Indian subsidiaries of foreign entities. The court specifically ordered all links to Blue Whale to be taken down and for intermediaries to exercise due diligence to ensure such take down on all links circulating on social media. The court expressed displeasure in noting that despite having the capabilities to control content for commercial consideration, intermediaries have failed to protect public interest and safety. Similarly, in ***Sneha Kalita v. Union of India***[252] the Supreme Court of India while dealing with a petition seeking blocking and banning of Blue Whale content, took note of the government's directives to intermediaries and passed directions to spread awareness about the harmful nature of the game.

The courts have held intermediaries liable for failure to takedown illegal content such as defamatory posts. In ***Swami Ramdev v. Facebook***[253] the Delhi High Court issued an injunction against online intermediaries and directed them to globally take down allegedly defamatory links against the plaintiff. The court opined that it had jurisdiction and powers under the IT Act to order global takedowns. The court interpreted "computer resource" in the IT Act to include a "computer network", which goes beyond a geographically limited network. The court held that the intermediaries were obliged to take down and block all such illegal content and videos which had been uploaded from I.P. addresses within India, on a global basis. Further, for illegal content which was uploaded outside the Indian territory, the Court directed geo-blocking access and disabling viewership of such content from within India. The Delhi High Court relied on numerous international judgements where courts have passed global injunctions/blocking orders, restricting/ blocking access to offending / defamatory content to justify its decision.[254] This order carries farreaching consequences for access to information and freedom of expression given the varying understanding and limits for what is defamatory content across jurisdictions. Given the

[248] Writ Petition 958/2013 (Lahore High Court, 2013, 2014).
[249] (2018) 15 SCC 551.
[250] *Suo moto* WP No. 16668/2017 (Madras High Court, 2017).
[251] Adeane, A. (2019 13 January). Blue Whale: What is the truth behind an online 'suicide challenge'? *BBC News*. https://www.bbc.com/news/blogs-trending-46505722
[252] (2018) 12 SCC 674.
[253] CS (OS) 27/ 2019.
[254] https://sflc.in/policy-tracker/court-cases

broad and vaguely worded provisions in ICT laws in many countries, this may very well result in over-censorship and a takedown frenzy, as the countries with the most restrictive regulations in their ICT laws could order takedown of content available in other jurisdictions as well.[255]

In other instances, courts have come to the rescue of intermediaries and defended them against State action in line with safe harbour provisions. For instance, the case of ***Sharat Babu Digumarti v. NCT of Delhi***[256] involved the listing for sale of an MMS video depicting a sexual act between two minors on bazee.com. The video was taken down two days later. The manager and managing director of the website were charged under Section 67 of the IT Act which criminalised the publication or transmission of obscene material in electronic form, as well as Section 292 of the Indian Penal Code (a similar obscenity provision in general criminal law). The charges under Section 67 of the IT Act were dropped (on the grounds that personal liability of the company official could not be established) but the High Court allowed proceedings under Section 292 to continue. The Supreme Court of India quashed the charges under Section 292 and held that Section 292 IPC cannot be used to prosecute an intermediary for obscene content published online which is regulated solely by the IT Act. In making its decision, the court accorded importance to the fact that the IT Act was a special law, which granted additional protection to intermediaries.

In a more recent case, ***Re Prashant Bhushan & Another***,[257] suo moto contempt proceedings were initiated against an advocate for Tweets relating to the Indian judiciary. In that case, Twitter has also been made a respondent to the petition as an alleged contemnor. However, the court accepted the explanation of Twitter that it was only an intermediary without control as to what the users post on the platform. It noted that Twitter had shown its bona fides by suspending both tweets immediately after the Court had taken cognizance of the matter and discharged the notice issued to Twitter. However, this position of the court could also encourage excessive censorship by intermediaries such as Twitter, which proactively removed the Tweets under question in this case even before any court order was passed for fear of reprisals.

The Indian courts in numerous cases[258] have deliberated on copyright and trademark infringements and intermediary liability, including by ruling on issues such as dynamic injunctions, blocking orders and the like.[259] Since this report is restricted to aspects of access, privacy and freedom of expression, we have not examined these decisions and provided an analysis. However, Article 15 of the ICESCR recognises the right of everyone to enjoy the benefits of scientific progress and its applications and the right to benefit from the protection of the moral and material interests resulting from any scientific, literary or artistic production authored. Intellectual property thus falls within the purview of human rights discourse and discussions surrounding digital rights. Therefore, intermediary liability in relation to intellectual property from a rights-based approach, which goes beyond enforcement,[260] across the sub-region warrants examination.

[255] Software Freedom Law Center. (2019 15 November). An Analysis of Swami Ramdev v. Facebook – The Existential Risk of Global Take Down Orders, *SFLC*. https://sflc.in/detailed-analysis-swami-ramdev-v-facebook-judgment
[256] AIR 2017 SC 150.
[257] *Suo moto* Criminal Contempt Petition No 1 of 2020 (Supreme Court of India, 2020).
[258] UTV Software Communication Ltd. & Ors. v. 1337X.to & Ors CS (COMM) 724/ 2017 (Delhi High Court, 2019).; Christian Louboutin SAS v. Nakul Bajaj and Ors. Civil Suit No. 344/2018 (Delhi High Court, 2018); Kent RO Ltd & Anr. v. Amit Kotak & Ors. 2017 (69) PTC 551; Myspace Inc. v. Super Cassettes Industries Ltd. 236 (2017) DLT 478.
[259] https://sflc.in/policy-tracker/court-cases
[260] *https://www.apc.org/en/pubs/briefs/apc-expresses-concern-over-oecd-communique-princip*