NATIONAL CYBERSECURITY POLICY 2023

Three Risks to Human Rights in Nepal

The **National Cybersecurity Policy 2023** (Policy) aims to protect Nepal from cyber-attacks and keep the internet safe. It outlines actions the government is expected to take to achieve this goal. Although many aspects of the Policy are positive and will strengthen cybersecurity[1], certain actions it describes could weaken human rights.

Digital Rights Nepal (DRN) and the International Center for Not-for-Profit Law (ICNL) prepared this brief to inform ministry officials, legislators, and civil society of three key human rights concerns raised by the Policy:

The National Internet Gateway:

The Policy calls for the government to establish a National Internet Gateway (NIG) (Article 11.25) through which all internet traffic into and out of Nepal will be routed. This could provide a powerful tool for the government to control online information and to monitor individuals' personal communications.

Severe restrictions on online speech and content:

The Policy could enable the government to censor and prohibit nearly any type of speech it doesn't like. It explicitly calls for the prohibition of broad, vague, and undefined categories of speech. Governments should only be able to restrict speech in very narrow and limited circumstances.

Regular monitoring of online speech and activities:

The Policy calls for "regular monitoring" of online space by the government. This is not necessarily inappropriate, but strong safeguards must be established to ensure that the freedom of expression and right to privacy are not restricted.

Cybersecurity and human rights are not mutually exclusive. Strong human rights protections are fundamental to a strong cybersecurity framework. The government, including ministry officials and legislators, should work with civil society to draft laws and regulations that protect human rights and follow cybersecurity best practices by addressing the concerns noted below.

---

[1] For example, Article 11.18 mandates the use of encryption in data exchange between information communication systems and services, aligning with international best practices. This ensures privacy and security without compromising law enforcement efforts. Second, Article 11.5 underscores the requirement for legal and policy measures to adhere to international standards concerning fundamental rights, emphasizing the significance of upholding Nepal's international legal obligations and democratic values. Moreover, Articles 11.51 to 11.55 establish the necessity for public awareness campaigns on cybersecurity, with a specific focus on vulnerable groups such as senior citizens, women, children, and people with special needs.

WHY IS THIS IMPORTANT?

A free and open internet is not merely a technological innovation; it is the bedrock of contemporary democracy and a crucial channel for exercising fundamental human rights, including the freedom of expression and right to privacy. In our globally connected society, the internet is the primary means for communication, information sharing, and civic participation. It enables individuals to express their views, exchange diverse ideas, and partake in public dialogue on pertinent issues.

Upholding these principles is essential for the protection of human rights in the digital space. Reinforcing them through meticulously crafted cybersecurity legislation is vital to guarantee that individuals can freely and securely exercise their rights online.

The National Cybersecurity Policy 2023 itself requires laws and regulations to follow international standards related to fundamental rights. Article 11.5 of the Policy underscores the commitment to uphold international standards in the formulation of laws and regulations concerning cybersecurity.[2]

The Policy presents a unique opportunity to not only safeguard cybersecurity but also to actively promote and enhance the values of freedom and security in the digital realm. By ensuring that individuals can freely and securely exercise their rights online, the Policy has the potential to foster a more inclusive and participatory digital environment. Rather than curtailing freedoms, the Policy can serve as a catalyst for empowering individuals to engage meaningfully in digital spaces, thereby strengthening democratic principles and advancing human rights in Nepal's evolving digital landscape.

[2] Article 11.5: "Legal and policy measures shall be established as per national, regional and international standards in regards to protection of fundamental rights including Right to Information and right to privacy."

THREE KEY CONCERNS RAISED BY THE NATIONAL CYBERSECURITY POLICY:

1 The National Internet Gateway

What is a National Internet Gateway?

A National Internet Gateway (NIG) is a central checkpoint for all internet traffic entering and leaving a country. Normally, countries have multiple points where their internet connections meet the rest of the world. But with a NIG, all that traffic goes through one single point controlled by the government. It's kind of like having one main gate instead of lots of smaller gates.

Now, why is this important? Having one central point for all internet traffic makes it much easier for the government to keep an eye on what's happening online. They can monitor, filter, or even block websites or information. It's a bit like having a big security camera watching everything that goes in and out of the country's internet.

But here's the catch: while it might allegedly help with cybersecurity[3], it also raises concerns about privacy and freedom of expression. If all internet traffic goes through this one gate, the government could potentially see and control a lot more of what people are doing online. This is a significant threat to people's rights to privacy and free speech.

What are the risks to Human Rights?

Risk of Censorship/Threat to Freedom of Expression: Implementation of the NIG presents a profound risk of censorship and threatens the fundamental right to freedom of expression. By consolidating all internet traffic through a single centralized point, the government gains unprecedented control over the flow of information, enabling them to regulate and censor online content according to their own agenda. This centralized control allows authorities to block access to websites, platforms, or content deemed critical or undesirable, stifling dissenting opinions and limiting public discourse. Such censorship undermines the vibrant exchange of ideas and diversity of viewpoints essential for a healthy democracy, eroding the foundations of free speech and undermining citizens' ability to freely express themselves online without fear of reprisal.

Surveillance/Threat to Privacy: The NIG poses a significant threat to privacy rights through the enablement of mass surveillance on an unprecedented scale. By funneling all internet traffic through a single point, the government gains access to vast amounts of personal data, including browsing history, communications, and online activities. This pervasive surveillance infringes upon individuals' right to privacy, as it allows authorities to monitor and track citizens' online behavior without their consent or knowledge. The collection and storage of sensitive personal data raise concerns about its potential misuse or exploitation, further exacerbating the erosion of privacy rights in the digital age. Such extensive surveillance undermines trust in online communication and erodes individuals' sense of privacy, leading to self-censorship and chilling effects on freedom of expression. Without adequate safeguards in place to protect privacy rights, the unchecked expansion of state surveillance threatens to undermine the autonomy and dignity of individuals in the digital realm.

[3] A NIG is also a prime target for hacking and espionage; because all internet goes through one checkpoint, if a bad actor gains access to the NIG, it will be able to see and surveil all of Nepal's internet traffic.

Key Recommendations

- Avoid the implementation of a National Internet Gateway because it poses an unjustifiable threat to the freedom of expression and right to privacy.
- Ensure that any cybersecurity measures implemented prioritize the protection of human rights and adhere to international standards.

2 Restrictions on online speech and content

What does the policy call for?

The policy calls for restrictions on online speech and content through the following articles:

- Article 11.64: This article aims to control the dissemination of "false information" on the internet and social media by enacting laws to prohibit such dissemination.
- Article 11.67: This article seeks to prohibit various categories of digital content, including content that could "spread animosity," constitute "cyber bullying," or "hurt social harmony."

What are the risks to Human Rights?

Threat to Freedom of Expression: These restrictions pose a risk of censorship and threaten the freedom of expression guaranteed under international law and the Constitution. Prohibiting the dissemination of "false information" and other vaguely defined content could stifle independent media, chill public debate, undermine government accountability, and impede the availability of information necessary for informed decision-making, thereby undermining democracy.

Key Recommendations

- Ensure that laws and regulations do not include vague and broad restrictions on online speech and content, such as those outlined in Articles 11.64 and 11.67.
- Instead of new, blanket prohibitions, consider using existing laws to prosecute individuals for specific offenses, such as defamation or incitement to violence; develop narrowly tailored laws targeting coordinated disinformation campaigns.
- Implement non-legal programs to educate the public on identifying and addressing disinformation, promoting digital literacy, and fostering responsible online behavior.

3 Regular monitoring of online speech and activities

What does the policy call for?

The policy (Article 10.8) calls for "regular monitoring" of online space for cybersecurity. Specifically, it aims to build a safe online space through this monitoring.

What are the risks to Human Rights?

Threat to Privacy Rights and Surveillance: This provision could enable the widespread, systematic, and constant surveillance of online speech and activities. While the intention behind the provision is to enhance cybersecurity and ensure safety online, it raises concerns about intrusive monitoring that could violate individuals' rights to privacy and freedom of expression. This provision would empower the government to monitor online activities extensively, thus undermining individuals' ability to communicate privately and securely. Without proper safeguards and oversight, such monitoring could be abused and used to suppress dissenting voices or target specific groups.

Key Recommendations

- Ensure that any monitoring activities are conducted under the most exceptional circumstances and are subject to strict oversight by an independent judicial authority.
- Implement safeguards to prevent the abuse of monitoring powers and to protect individuals' privacy rights.
- Establish clear guidelines and limitations on the scope and duration of monitoring activities to prevent indiscriminate surveillance.
- Promote transparency and accountability in the monitoring process, including regular reporting on the nature and extent of monitoring activities to the public and relevant oversight bodies.
- Engage with civil society organizations and human rights experts to develop comprehensive frameworks for cybersecurity measures that balance security concerns with respect for human rights.

CONCLUSION: THE PATH FORWARD

Strong human rights protections are an essential component of a strong cybersecurity framework. The National Cybersecurity Policy 2023 is a good blueprint for cybersecurity in Nepal. However, future laws and regulations must address the concerns noted in this brief to ensure that people in Nepal enjoy a safe and free internet. DRN and ICNL stand ready to assist interested stakeholders with further information on these issues as necessary.

ABOUT US

Digital Rights Nepal (DRN) is a non-profit organization established in 2020, dedicated to safeguarding digital rights and fostering a secure online environment in Nepal. With a diverse team of advocates and experts, DRN conducts research, advocates for policy reforms, and engages in capacity-building initiatives to promote online freedom of expression, privacy protection, access to information, and cybersecurity. Led by passionate changemakers in human rights and digital advocacy, DRN plays a pivotal role in shaping the digital landscape of Nepal, both locally and on the international stage. For more information on DRN activities and resources, please visit www.digitalrightsnepal.org.

The **International Center for Not-for-Profit Law (ICNL)** is an international organization that provides technical assistance, research, and education to support the development of appropriate laws and regulatory systems for civil society organizations in countries around the world. ICNL has provided assistance to civil society, governments, and policy experts in over 100 countries. ICNL has worked closely with international and regional institutions; private foundations; and scores of in-country colleagues to promote and protect the freedoms of expression, association, assembly and right to privacy, online and offline. For more information on our work, please visit www.icnl.org.