

SADF Podcast S3E8 Edited Transcript

SADF Podcast

Regulating Big Tech in South Asia: Freedom, Control and Democratic Resilience

Host: Tapas Kanti Baul, South Asia Democratic Forum (SADF)

Guest: Professor Subhajit Basu, Professor of Law and Technology, University of Leeds

This transcript has been lightly edited for clarity, grammar and readability while preserving the substance and character of the original conversation. Views expressed by the speakers are their own.

Tapas Kanti Baul

Welcome to the South Asia Democratic Forum Podcast. I'm your host, Tapas Kanti Baul.

In this episode, we turn to a rapidly growing battleground: the struggle between Big Tech companies and governments across South Asia.

Platforms such as Meta, Google and X increasingly shape public discourse, influence elections and control vast amounts of user data. Governments across the region are scrambling to regulate their power—often with mixed motives and uneven success.

From India's proposed broadcasting regulations to Bangladesh's Digital Security Act, Cyber Security Act and Cyber Security Ordinance, South Asia is witnessing a tug-of-war between digital freedom and state control.

This raises urgent questions about privacy, accountability and democratic resilience.

To help us unpack these complex dynamics, we are joined by **Professor Subhajit Basu**, Professor of Law and Technology at the University of Leeds.

Professor Basu is a globally respected scholar in cyber law, digital governance and AI ethics, with a particular focus on the Global South. He has served as Chair of the British and Irish Law, Education and Technology Association and is a Fellow of the Royal Society of Arts.

His work has contributed to policy debates across Europe, Africa and Asia, and his publications, including work on privacy, healthcare data and global perspectives on e-commerce and taxation law, are widely cited in academic and policy circles.

Professor Basu, welcome to the podcast. It is a pleasure to have you with us.

Professor Subhajit Basu

Thank you very much, Tapas, for your kind introduction. It is a pleasure to be with you.

Tapas Kanti Baul

In recent years, we have seen social media play a significant role in youth uprisings in Bangladesh and Nepal.

Across South Asia, younger generations—especially Gen Z—are deeply engaged with social media, while these platforms are largely controlled by major technology companies.

So let me begin with this question: **what makes Big Tech regulation a uniquely urgent issue for South Asian countries today?**

Professor Subhajit Basu

Thank you, Tapas. It is a very pertinent question.

The examples you mentioned clearly demonstrate why regulating Big Tech in South Asia has become so urgent.

We first have to recognise that these companies are not simply operating social media platforms.

They are increasingly running parts of our economy and parts of our daily lives.

In the Global South, this is fundamentally about **power**.

Platforms such as Meta, Google and TikTok influence speech. We have seen that during the Nepal uprising, and we have also seen their impact in India and Bangladesh.

They can influence political dialogue, and there is a widely discussed view that they may even influence elections. That remains difficult to prove conclusively, but it is equally difficult to dismiss.

They also influence protest culture.

We have seen this not only in the Global South and South Asia, but also in the Global North.

If we look specifically at South Asia—India, Bangladesh, Pakistan, Sri Lanka and the wider region—we are talking about a population approaching two billion people, many of whom have access to social media.

Whoever controls these platforms therefore has enormous influence over what people see, what they say, what they believe and how collective action is organised.

This is not a theoretical concern.

We have already seen how social media can intensify communal tensions.

We have discussed misinformation during elections and its potential consequences.

We have seen harassment organised through social media, calls to violence and cross-border propaganda.

Recent uprisings in Bangladesh provide one example, and we have seen similar dynamics elsewhere in the region.

So we cannot simply leave this level of influence in the hands of technically unaccountable foreign companies.

There is also another dimension that I write about frequently: **data sovereignty**.

The information society is fundamentally about data.

People often say that “data is the new oil.” That phrase may sound clichéd, but the underlying point is real.

This is about access to data, use of data and what we might call data mining.

The data involved can include location data, relationship data, financial behaviour and, increasingly, biometric information.

Much of that data is stored or controlled by companies whose headquarters are outside the region.

From the perspective of a government, this can feel like a loss of control and a loss of jurisdiction.

You therefore have companies effectively governing significant aspects of the lives of hundreds of millions of people, while real-time behavioural data is controlled elsewhere—often in places such as California.

That creates a legitimate question about whether data should be governed locally and under domestic law.

You could call that a form of legitimate self-determination.

But this is where the issue becomes complicated, because the same argument can also lead towards **surveillance**.

So regulators in the Global South and in South Asia do need to act.

We also have to consider online abuse, religious tensions and increasingly sophisticated forms of manipulation.

Deepfakes can be used to influence majorities, victimise minorities and target women through sexualised imagery.

Religious hate speech is another major concern.

One of my biggest fears in South Asia is that religious hate speech can move from online platforms into street violence within hours.

Coordinated disinformation networks can amplify that effect.

So if you do not regulate Big Tech and social media, you risk leaving citizens exposed to companies whose primary incentive is profit.

But there is an equally important problem on the other side.

If regulation becomes too aggressive, governments risk scaring away investment and innovation.

That balance is particularly difficult to achieve in South Asia, because the stakes for economic growth are very high.

And there is another uncomfortable truth: regulation is also about **control**.

The same legal tools that can protect citizens from abuse can also be used to silence journalists, suppress opposition voices and target activists.

So when a South Asian government says, “We want to regulate Big Tech,” the question must always be:

Regulate to protect whom, and against what?

That question is crucial.

Civil society groups are often excluded from policymaking processes in the Global South.

They may have very little influence over the design of laws, and in some cases they themselves are targeted under cybercrime or national security legislation.

There is also a tendency for funding from the Global North to focus on priorities defined by external actors, rather than necessarily on the most urgent interests of ordinary citizens.

Meanwhile, platforms themselves rarely consult meaningfully with the people most exposed to risk—women, activists, journalists, LGBTQ users, ethnic minorities and religious minorities.

So to return to your question: yes, Big Tech regulation is an urgent and central policy issue for South Asia.

But regulation has to balance **freedom of speech and expression, personal safety, national sovereignty and the economic future of the region**.

That is the challenge.

Tapas Kanti Baul

My next question was going to be about regulatory gaps.

But after hearing your answer, I want to ask something more fundamental first.

Where do **we—the people, the users—stand** in this struggle between governments and Big Tech?

Governments are often interested in control.

Big Tech companies are interested in profit.

So where are we?

Professor Subhajit Basu

We are in the most vulnerable position.

On one side, Big Tech operates according to business models driven by profitability.

On the other side, governments seek to regulate, but they do not always regulate primarily in the public interest.

In many cases, governments regulate in ways that serve their own political interests or preferred policy agendas.

So ordinary users are caught between those two forces.

And the situation becomes even worse if you belong to a minority or marginalised group.

Those communities often have the least protection because they have less political influence and less commercial value.

They may not represent a sufficiently large consumer group for Big Tech to prioritise their interests from a business perspective.

At the same time, governments may not see political advantage in protecting them.

Their rights may not translate easily into electoral or “vote-bank” politics.

So these are often the people most exposed and least protected.

Tapas Kanti Baul

The way you describe it, the user almost becomes a ping-pong ball.

On one side is the government, and on the other side is Big Tech, and both are effectively playing with us.

So let us return to the regulatory question.

What are the key regulatory gaps in South Asian countries, and how can users be better protected within this system?

Professor Subhajit Basu

Let me answer that through two examples.

There are already regulations emerging across the region.

Bangladesh’s interim government, for example, has been considering a new data-protection framework in the form of an ordinance.

There are also online-safety laws and other forms of digital regulation.

India has its own information-technology legislation, which dates back to 2000, although the wider legal framework has evolved considerably since then.

But in my view, two major areas deserve particular attention.

The first is **data protection**.

The second is **online safety**.

And in both cases, there are useful lessons to be learned from Europe—but with important warnings.

Let us begin with the European Union's **General Data Protection Regulation, or GDPR**.

The GDPR forces companies operating in Europe, or targeting European consumers, to justify why they collect data, how they will use it, how long they will keep it and with whom it may be shared.

It also gives individuals important rights over their data, including rights of access and deletion.

Crucially, it creates independent data-protection regulators and gives them enforcement powers, including the ability to impose serious fines.

That question of **independence** is particularly important.

India, for example, has enacted data-protection legislation, but questions arise about the independence of the regulatory authority.

South Asian governments are increasingly interested in data localisation and data sovereignty.

But we have to ask why.

Is the objective genuinely to provide citizens with stronger privacy guarantees?

Or is the objective to give governments greater control?

A GDPR-style approach does allow states to access data in legitimate circumstances.

But that access is not automatic.

A government cannot simply say, “We need this because of national security,” and treat that as sufficient justification.

“National security” is an important concept, but it is also very broad and can be used to justify almost anything if it is interpreted too widely.

There should therefore be tests of **legality, necessity and proportionality**, as well as independent oversight.

The core idea is that the state itself is **not above the privacy regime**.

That is an extremely important principle.

There is, however, a warning.

The GDPR exists within a relatively mature rule-of-law environment.

European countries have long traditions of independent regulators and institutional checks.

Can we always assume the same level of independence and public trust in South Asia?

That is where the difficulty lies.

South Asian countries can certainly borrow the language of rights and accountability from European law.

But if the regulator is not genuinely independent, then the gap remains.

You may have legislation that looks like a gold-standard European law on paper.

But in practice, it may become little more than **surveillance vocabulary wrapped in the language of rights**.

The same problem arises with online-safety laws.

Tapas Kanti Baul

There is a Bengali proverb that essentially suggests the same problem: if the state retains the character of a sly fox, whatever protections it promises, there will always be some back door through which it can interfere with personal data and use it for its own purposes.

Professor Subhajit Basu

Absolutely. I agree.

So in many cases, the real regulatory gap is a gap of **intentions and institutions**.

If citizens expect that governments will abuse these powers, then it becomes extremely difficult to trust governments to protect them against Big Tech.

And Big Tech companies can take advantage of that mistrust.

Citizens then find themselves in a situation where their rights are at risk, but there is no single actor they can reliably hold accountable.

Tapas Kanti Baul

That brings us to another major issue: **algorithmic bias**.

How do algorithmic biases and disinformation campaigns affect minority communities?

And if governments respond through regulation, is there also a risk of **digital authoritarianism** being introduced under the guise of regulation?

How can Big Tech companies themselves be held responsible when trust is abused?

Professor Subhajit Basu

Algorithmic bias is extremely important.

We first have to acknowledge that societies themselves contain biases.

Bias is already part of our social structures.

The problem becomes much more serious when those biases enter algorithms.

Then the impact can become devastating.

We saw during previous US elections how algorithmic systems can create **echo chambers**.

When an algorithm shows people only information that confirms what they already believe—rightly or wrongly—it begins to shape their decision-making.

And we are moving towards an increasingly AI-driven society.

Artificial intelligence will influence much of what we see, what we hear and perhaps even what we think.

It can also influence who gets amplified and who gets silenced.

So Big Tech algorithms do not merely reflect social bias.

They can **reinforce and intensify it**.

That is the danger.

On your second question—digital authoritarianism in fragile democracies—I completely agree that this is not a theoretical concern.

Strong technology regulation can quietly become a tool of oppression.

We have to remember something important.

Social-media platforms, despite all their problems, have also given a voice and a public platform to people who previously had very little access to public debate.

That is why regulation is a double-edged sword.

If the legal framework is vague and overly broad, those vague powers can become tools of censorship.

Suppose a government can order platforms to remove anything that allegedly threatens “national security,” “public order” or, perhaps most troublingly, “morality.”

How do you define morality?

Whose morality are we talking about?

These are often vague terms.

They may not be clearly defined in legislation and may not be meaningfully reviewed by independent courts.

So imagine that I criticise a government.

The government then says, “This is destabilising content.”

It tells Meta, Facebook or Google to remove it.

The platform complies.

At that point, you have **copyright on demand**, but wrapped in legal language.

The government can always say, “The law requires this.”

And the platform can become an extension of an authoritarian state—effectively an enforcement arm.

Why would the company comply?

Because it is in its commercial interest.

A major technology company does not want to be banned or sanctioned in a valuable market.

It does not want to lose business.

So the easiest option may be to comply with government takedown orders rather than ask whether the speech is constitutionally protected.

In the worst-case scenario, this can even become automated.

Algorithms themselves can be designed to enforce censorship.

We have examples of this in highly controlled digital environments, where particular political terms are filtered automatically.

At that point, the state does not even need to block every piece of content directly.

The **code itself performs the censorship**.

Online-safety frameworks can be weaponised in a similar way.

Everyone can agree that gender-based abuse is wrong, that deepfake blackmail is wrong and that certain forms of online harm should be prevented.

But the speed of the internet itself can also become a weapon.

By the time authorities or individuals respond, a piece of harmful content may already have reached hundreds of thousands of people.

In a region as populous as South Asia, even reaching a tiny percentage of the population can mean an enormous audience.

So delay can have devastating consequences.

Now imagine a journalist reporting on corruption.

The government may call that “harmful content.”

An opposition figure calls for a protest.

The government may describe it as “incitement to violence.”

This is how Big Tech platforms can become highly effective tools of oppression in fragile democracies.

But there is another side.

If those companies suddenly say, “We do not accept regulation by sovereign states; we operate according to our own rules,” then they can themselves become quasi-sovereign actors.

That is also deeply problematic.

Tapas Kanti Baul

Exactly.

Recently we have heard arguments from major platform owners suggesting that their companies operate according to their own rules and should not necessarily be bound by the laws of individual states.

That is an extraordinary concentration of power.

Can you imagine a private US company effectively saying: “We will not obey the laws of sovereign countries”?

You then have companies with enormous power but very little responsibility, accountability or transparency.

So let me ask the final question.

What role can civil society and academia play in shaping this debate, and what future do you see for digital governance in South Asia?

Professor Subhajit Basu

I always say that when you regulate the public sphere—whether in the physical world or the digital world—you have to regulate it **in conversation with the public**.

You cannot regulate the public sphere with no public in the room.

That is one of the hallmarks of authoritarian government and of digital authoritarianism.

In many European countries, lawmaking processes include extensive public consultation.

There may be green papers, white papers, formal consultations and opportunities for civil society, NGOs, academics and ordinary citizens to respond.

Very recently, for example, I took part in a public consultation concerning the UK's Online Safety Act.

Ofcom is developing rules that companies will have to comply with, including rules for protecting vulnerable individuals.

That process creates ongoing dialogue.

It helps prevent law from becoming something alien, detached and imposed from the top down.

That kind of process is often missing elsewhere.

Social-media companies themselves like to present certain activities as public participation.

Around elections, for example, they may encourage people to vote and warn them about misinformation.

On the surface, that looks positive.

But if the same platform uses algorithms to suppress opposition voices, then the reality is very different.

Who can challenge that?

Civil society and academics can raise concerns, write about them and expose problems.

But they may themselves face censorship.

So Big Tech has a responsibility to ensure that dissenting voices are not unfairly throttled or suppressed.

We also need much greater scrutiny of **takedown powers**.

Are those powers narrowly defined in law?

Can takedown decisions be reviewed?

Is civil society involved in understanding how those powers operate?

Regulation is essential.

Regulation is not inherently bad.

But **regulation without safeguards can be disastrous in a democracy**.

Another important question is the regulator itself.

If there is an independent regulator, does that regulator have the necessary technological and technical competence?

How was it established?

Is it genuinely at arm's length from government?

Or is it effectively controlled by a ministry?

Independence has to be real.

We also need explicit protections for lawful political speech, journalism and human rights.

If the answer to those questions is yes—if the regulator is independent, technically competent and legally constrained—then you may have a good regulatory framework.

If the answer is no, then you may slowly be building censorship into the paperwork.

Civil society cannot be excluded by design.

It provides the checks and balances necessary to protect digital rights.

Independent academics also need to be heard.

That is essential whenever regulation of Big Tech is being designed.

Tapas Kanti Baul

Thank you very much.

It seems that regulating these technology giants is rather like **walking on very thin ice**.

Professor Subhajit Basu

One hundred per cent.

Tapas Kanti Baul

We have seen in both Bangladesh and Nepal that when governments restrict internet access or block social-media platforms, people can respond by taking to the streets—and in some cases the political consequences can be enormous.

This podcast will obviously not give us a complete answer.

I am not even sure that a thousand hours of discussion would be enough to capture the full depth of the problem.

Ultimately, there are three actors in this discussion: **governments, users and technology giants**.

All three have to behave reasonably.

As a law student, I will fall back on the legal idea of the “reasonable person,” even if defining reasonableness itself is difficult.

Thank you once again for discussing such a timely subject.

Professor Subhajit Basu

Thank you.

If I may add one final point, we often speak about **regulating technology**.

But this is not only about regulating technology.

It is also about **regulating behaviour**.

You are absolutely right that unless our behaviour changes—unless we act responsibly—things will not improve.

So the issue is not simply regulating the technology.

It is also about the behaviour of users and about the content people create.

Technology itself can be a very good thing.

Innovation is good.

What determines whether technology becomes beneficial or harmful is **how we use it**.

Tapas Kanti Baul

On that, at least, we agree completely.

To our viewers and listeners, we will certainly return to this issue in future podcasts, and I hope Professor Basu will join us again for those discussions.

This has been a very interesting conversation, and we invite everyone to follow our upcoming episodes.

Professor Basu, thank you very much for being with us.

Professor Subhajit Basu

Thank you very much.