Saudi Arabia's digital rights hypocrisy

Overview

1. **Introduction**
2. **Human rights' intersection with digital rights**
3. **The Kingdom of Saudi Arabia: human rights record**

- **Digital rights abuse**
    a. **Digital rights violations: case studies**
    b. **Internet censorship and mass surveillance: Neom case study**
    c. **Propaganda and threatening**

4. **West involvement:**

- **Investment in NEOM**
- **ICT deals and sales in MENA, facilitating abuse**
- **Case studies:**
    a. **BAE Systems**
    b. **Pegasus Spyware**
    c. **Google Cloud**

5. **Conclusion**

Introduction:

The intersection of human rights and digital rights has become increasingly critical as digital technologies permeate every aspect of modern life. The United Nations (UN) has been proactive in addressing digital rights and cyber law through a range of resolutions, reports, and frameworks aimed at shaping international norms and encouraging member states to align their policies with these principles. Despite these efforts, Saudi Arabia presents a stark contrast to the UN's vision of digital rights. The Kingdom has not ratified many of the critical international human rights treaties; this reluctance becomes particularly contentious in the context of Saudi Arabia hosting the Internet Governance Forum (IGF) at the end of this year. The IGF, a UN initiative, is designed to facilitate multistakeholder discussions on public policy issues related to the internet. Hosting such an event in Saudi Arabia, a country known for its severe restrictions on political freedoms, freedom of expression, and internet censorship, raises significant concerns about the commitment to the principles the IGF aims to uphold.

This paper delves into Saudi Arabia's human rights record, focusing on its extensive digital rights abuses. It further explores specific cases of digital rights violations, illustrating the Kingdom's pervasive surveillance and censorship infrastructure. Moreover, it critiques the involvement of Western nations and corporations, whose economic and strategic interests often overshadow human rights considerations, thereby enabling the continuation of these abuses.

The aim is to provide a comprehensive understanding of the implications of Saudi Arabia hosting the IGF, highlighting the inconsistencies and challenges in promoting digital rights in a repressive environment.

1. Human rights' intersection with digital rights

The United Nations (UN) has addressed digital rights and cyber law through various resolutions, reports, and frameworks. However, it does not have directly enforceable laws. Instead, the UN's work in this area helps shape international norms and encourages member states to adopt policies and laws consistent with these principles. The key UN initiatives and documents related to digital rights and cyber law are listed below:

- Universal Declaration of Human Rights (UDHR)

  The UDHR, adopted in 1948, is a foundational document that underpins the UN's approach to human rights, including digital rights. Key articles relevant to digital rights include:

  Article 19: Guarantees freedom of opinion and expression, which extends to digital communications.

  Article 12: Protects individuals from arbitrary interference with their privacy.

- International Covenant on Civil and Political Rights (ICCPR)

  Adopted in 1966, the ICCPR builds on the UDHR and is legally binding on its signatories. Key articles include:

  Article 17: Protects privacy.

  Article 19: Ensures freedom of expression, including digital mediums.

- Human Rights Council Resolutions

  The UN Human Rights Council has passed several resolutions emphasising the importance of human rights in the digital context:

  Resolution 20/8 (2012): Affirms that the same rights people have offline must also be protected online, particularly freedom of expression.

  Resolution 26/13 (2014): Focuses on the promotion, protection, and enjoyment of human rights on the Internet.

  Resolution 32/13 (2016): Condemns measures to intentionally prevent or disrupt access to information online and affirms the need for privacy protections in the digital age.

- Special Rapporteur Reports

  The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression regularly publishes reports on issues related to digital rights. Key reports include:

  2011 Report on Freedom of Expression and the Internet: Emphasises the importance of ensuring that Internet access is maintained and protected.

  2018 Report on Artificial Intelligence Technologies and Their Impact on Freedom of Expression: Analyses the implications of AI on digital rights.

- United Nations General Assembly (UNGA) Resolutions

  The UNGA has adopted several resolutions relevant to cybersecurity and digital rights:

  Resolution 68/167 (2013): Addresses the right to privacy in the digital age.

  Resolution 73/27 (2018): Emphasises the role of ICT in international security and the need for cooperation to combat cybercrime.

- International Telecommunication Union (ITU)

  The ITU, a specialied UN agency, plays a significant role in setting international standards and policies related to information and communication technologies (ICTs), including cybersecurity.

- United Nations Office on Drugs and Crime (UNODC)

  The UNODC addresses issues related to cybercrime through various initiatives, including:

  The Global Programme on Cybercrime: Assists member states in combating cybercrime and improving their legal frameworks.

- The Sustainable Development Goals (SDGs)

  While not specific to digital rights, the SDGs include targets related to access to information and communications technology, such as:

  Goal 9 (Industry, Innovation, and Infrastructure): Includes targets for increasing access to ICT and the Internet.

Having listed these important stances of the United Nations and its members vis a vis of digital rights in our increasingly digitalised world, it is crucial to underline Saudi Arabia's lack of ratification and engagement with most of these laws/proposals. Indeed, the country has not ratified most of them, these reservations indicate its reluctance to fully commit to internationally recognised human rights standards.

This is where lies Saudi Arabia's hypocrisy in hosting the Internet Governance Forum (IGF) at the end of this year. The United Nations' division was created as a multistakeholder platform facilitating the discussion of public policy issues pertaining to the internet, the programme will be shaped along four main themes:

- Harnessing innovation and balancing risks in the digital space
- Enhancing the digital contribution to peace, development, and sustainability
- Advancing human rights and inclusion in the digital age
- Improving digital governance for the Internet We Want

Thus, the kingdom will be hosting an event supposedly advancing human rights in the digital age, a country which has not ratified basic human rights treaties, and has abstained from voting for the Universal Declaration of Human Rights (UDHR) resolution, the most fundamental text protecting basic human rights. Let alone the record of human rights abuse that Saudi Arabia has, scoring 8 out of 100 in the 2023 Freedom House report, classifying the country as "not free".

3. The Kingdom of Saudi Arabia: human rights record

The situation in Saudi Arabia is notorious for its lack of political freedoms; the Kingdom is an **absolute monarchy,** where the King holds extensive powers that are not subject to meaningful checks and balances. Political parties are banned, and there is no elected legislature. Citizens have no opportunity to change their government through democratic means, and any form of political dissent is harshly repressed. Activists, political dissidents, and even bloggers face imprisonment, torture, and in many cases, the death penalty for expressing views that are critical of the government.

The legal system is based on Islamic law- Sharia- which severely restricts **women's freedoms**. While there have been some recent reforms, such as allowing women to drive and easing certain guardianship laws, Saudi Arabia continues to impose significant restrictions on women's rights. Women still face systemic discrimination in many areas, including employment, education, and legal matters. The male guardianship system, though slightly relaxed, still requires women to obtain permission from a male relative to make major decisions. Activists who campaign for women's rights are often arrested and subjected to abuse, but also imprisonment.

Alongside this, **freedom of assembly and association** are virtually non-existent in Saudi Arabia. Public protests are banned, and gatherings of a political nature are prohibited. Trade unions and independent human rights organisations are not allowed to operate freely. Organisers and participants of peaceful protests often face arrest and prosecution under broad anti-terrorism and public order laws. Therefore any kind of virtual association against the Kingdom is also severely censored: the Saudi government maintains **strict control over the media and the internet**. The country's laws criminalise criticism of the monarchy, the religious establishment, and other government bodies. Online platforms are heavily monitored, and content deemed objectionable is censored: websites, blogs, and social media accounts that advocate for political reform or criticise the government are often blocked. Those who manage to voice dissent online can face severe legal repercussions, including lengthy prison sentences, and severe abuse.

- Digital rights abuse

Digital rights in Saudi Arabia are completely abused, as fundamental human rights are as well in this country.

As explained above, the country maintains extremely strict control over the media and internet, more specific cases of digital rights abuse and violations are presented below, to emphasise the hypocrisy of the United Nations' decision to award the hosting of the IGF to Saudi Arabia.

a. Digital rights violations

Saudi Arabia's digital rights violations encompass censorship, surveillance, arrests, and legal restrictions on online expression. These violations infringe on individuals' rights to

freedom of expression, privacy, and association, undermining democratic principles and stifling dissent and activism in the digital sphere. The government heavily censors the internet, blocking access to websites promoting political dissent, human rights activism, LGBTQ+ rights, and religious pluralism. Social media platforms are also subject to censorship, with authorities targeting content critical of the government or religious authorities. Surveillance technology, including deep packet inspection, is used to monitor internet traffic, social media platforms, and communication channels, enabling authorities to track users' online behaviour and access personal data without consent. Stringent cybercrime laws criminalise online activities such as defamation, spreading false information, and criticising the government or religious authorities, providing legal cover for the suppression of digital dissent. Additionally, women's rights activists advocating against discriminatory practices face online censorship and harassment, further limiting their ability to express themselves freely online. These violations undermine individuals' rights to freedom of expression, privacy, and association, stifling dissent, and activism in the digital sphere. Below are a few case studies of the imprisonment of human rights activists for expressing their views online, highlighting the Saudi government's repression of digital political dissent and their perpetual violation of fundamental human rights:

Case studies:

Raif Badawi

Raif Badawi, a blogger and activist, was arrested in 2012 and later sentenced to 10 years in prison, 1,000 lashes, and a substantial fine. His charges included "insulting Islam through electronic channels" due to his creation of the website "Free Saudi Liberals," which encouraged political and social debate. The punishment was widely condemned as a violation of freedom of expression and the right to be free from inhuman treatment.

Loujain al-Hathloul

Loujain al-Hathloul, a prominent women's rights activist, was arrested multiple times for her activism, including her campaign against the ban on women driving and advocating for the end of the male guardianship system. In 2018, she was detained and later sentenced to nearly six years in prison under broad anti-terrorism laws, largely for her online activism and social media use. Her case highlights the suppression of digital activism and the punishment of those who use the internet to campaign for human rights, she was released in 2021, reporting torture, and is still subject to a travel ban.

Jamal Khashoggi

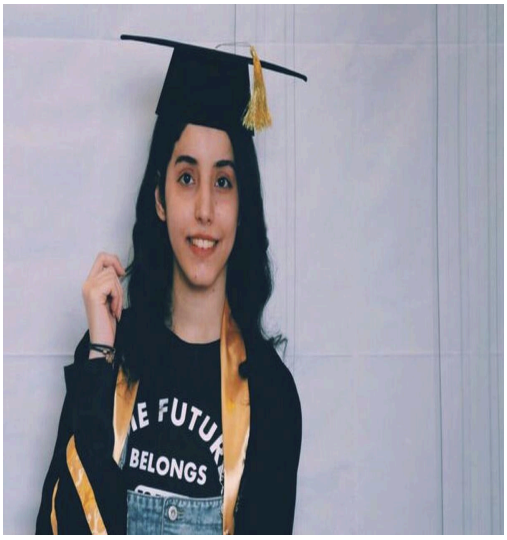
Although not a digital rights case in the strictest sense, the murder of journalist Jamal Khashoggi in 2018 is deeply linked to his online criticism of the Saudi government. Khashoggi was a vocal critic of the Saudi regime on various platforms, including social media and his columns in The Washington Post. His assassination in the Saudi consulate in Istanbul was reported as an "extrajudicial execution" for which the Saudi state was responsible, yet the trial was the "antithesis of justice" according to a UN expert, as the hitmen were sentenced to death, but the Saudi state was not held accountable, highlighting also the country's culture of impunity.

Ashraf Fayadh

Ashraf Fayadh, a poet and artist, was sentenced to death in 2015 for apostasy, largely based on the content he shared online and accusations stemming from his poetry and social media posts. Fayadh was accused of promoting atheism and blasphemy through his writings and social media activities, more specifically, the violation of Article 6 of the Law on the fight against cybercrime. This represents a grave infringement on freedom of expression and the right to life, as he was punished for his online and artistic expression. He was freed after more than eight years, having endured torture during his sentence.

Essam Koshak

Essam Koshak, a human rights defender and social media activist, was arrested in 2017 and sentenced to four years in prison and a four-year travel ban. He was charged with "inciting public opinion" and "insulting the authorities" based on his tweets and social media activities advocating for political reform and human rights.



Manahel al-Otaibi

Manahel al-Otaibi, a women's rights activist, was arrested in 2023 for her social media posts advocating for women's rights and criticising the guardianship system. She was charged with "violating public morals" and "inciting public opinion" through her online activities, including advocating for the right of women to live independently without male guardians. Al-Otaibi's case highlights the ongoing repression of online activism and the severe penalties imposed on those who use social media to challenge restrictive societal norms and advocate for human rights.

This January, she was sentenced to 11 years in prison, the court found her guilty of terrorism offences. Lina al-Hathloul, the head of advocacy of a prominent NGO in the region, ALQST said Manahel al-Otaibi's "confidence that she could act with freedom could have been a positive advertisement for Mohammed bin Salman's much-touted narrative of leading women's rights reforms in the country". "Instead, by arresting her and now imposing this outrageous sentence on her, the Saudi authorities have once again laid bare the arbitrary and contradictory nature of their so-called reforms, and their continuing determination to control Saudi Arabia's women," she said.

b. Internet censorship and mass surveillance

The way in which the Saudi state is truly able to monitor, limit and suppress online content is through an extensive surveillance and censorship infrastructure to control the public digital sphere and its population:

Saudi Arabia has heavily invested in sophisticated **surveillance technology** to monitor internet traffic, prominently employing Deep Packet Inspection (DPI). This technology allows authorities to inspect data packets as they pass through network routers. By analysing these packets, the government can identify individuals by matching data packets to specific users, effectively tracking who is accessing which sites. This enables comprehensive monitoring of online activities, including websites visited, emails exchanged, and social media interactions. Furthermore, DPI facilitates the interception of communications, allowing the government to read emails, instant messages, and other forms of communication in real-time. This level of control over internet traffic is bolstered by the regulation of Internet Service Providers (ISPs), which further aids in the enforcement of surveillance measures.

In Saudi Arabia, **ISPs** operate under stringent government regulation and censorship. The government ensures that ISPs implement robust filtering mechanisms to block access to websites deemed objectionable or politically sensitive. This is typically achieved through URL filtering and DNS tampering. Additionally, ISPs are mandated to

maintain detailed logs of users' internet activities, including websites visited and data exchanged. These logs are accessible to government agencies, thus facilitating comprehensive surveillance of individuals' online behaviour. This tight control over internet service providers complements the government's active monitoring of social media platforms, where much of the public discourse takes place.

Social media platforms are a significant focus of Saudi surveillance efforts. The government employs dedicated teams to actively monitor platforms like Twitter, Facebook, and WhatsApp. These teams track and analyse posts, conversations, and user activities for signs of dissent or political activism. In addition to human monitoring, authorities utilise automated tools to scan for keywords and hashtags associated with political dissent or criticism of the regime, ensuring that even subtle expressions of discontent are detected and addressed. This vigilant scrutiny of social media is supported by broad cybersecurity laws that provide a legal framework for these surveillance activities.

Indeed, Saudi Arabia's legal framework provides robust support for its surveillance activities. **The Cybercrime Law**, for instance, criminalises a wide range of online activities, including defamation, hacking, and spreading false information. The broad definitions within this law grant the government extensive powers to prosecute individuals for their online behaviour. Furthermore, these laws bestow authorities with broad powers to monitor, intercept, and access electronic communications without the need for judicial oversight, thus institutionalising the surveillance apparatus. These laws also compel technology companies to cooperate with government surveillance efforts.

The Saudi government collaborates closely with the latter to access user data. Authorities routinely request user information, metadata, and communication records from social media companies, email providers, and other online services. These requests are often legally binding under Saudi law, compelling **technology companies** to comply or face significant penalties, including fines or restrictions on their operations within the country. This **cooperation** ensures that the government has access to a wealth of user data, enhancing its surveillance capabilities.

Case study: Neom

Within Neom, a multi-billion dollar special economic zone being built by Saudi Arabia, there is a futuristic mega-city project envisioned called The Line, aiming to transform the economic landscape of the region with advanced technology and sustainable living. However, it also epitomises the kingdom's extensive surveillance culture, raising significant concerns about privacy and digital rights.

The city is designed with artificial intelligence at its core, using data to manage various urban functions such as power, water, waste, transport, healthcare, and security.

Joseph Bradley, the chief executive of NEOM Tech & Digital Co., emphasises that "without trust, there is no data. Without data, there is no value." This highlights NEOM's reliance on a vast data collection framework to function effectively. Residents' data will be collected

through smartphones, homes, facial recognition cameras, and numerous other sensors, creating a comprehensive surveillance system intended to predict and cater to user needs.

However, Saudi Arabia's poor human rights record raises doubts about the responsible usage and protection of personal data. Digital rights experts caution that NEOM's extensive data collection infrastructure could lead to severe privacy violations. Vincent Mosco, a researcher on the social impacts of technology, describes NEOM as "in effect, a surveillance city," reflecting broader concerns about the invasive nature of its data practices.

Residents will be able to use a consent management platform to review and manage their data permissions, potentially receiving financial rewards for sharing their data. Despite these assurances, critics argue that financial incentives could distort genuine consent and normalise the commodification of personal data. Marwa Fatafta from Access Now calls it a "privacy disaster waiting to happen," as it undermines the fundamental right to privacy and data protection. Not to mention the human rights violations which have already occurred during the construction of the city, leading to the displacement of indigenous communities, particularly the Huwaitat tribe. Reports indicate that these communities have been forcibly removed from their ancestral lands, many jailed and some executed, causing international outcry over human rights abuses.

The Line, a core component of NEOM, exemplifies the integration of surveillance into everyday life, from tracking residents' health and movements to deploying drones for welfare checks. While this may offer some practical benefits, it also deepens concerns about the extent and purpose of data collection.

NEOM's approach reflects broader global trends towards increased digitisation and smart city development. However, the context of Saudi Arabia's extensive surveillance culture and human rights issues makes NEOM a particularly troubling case. The lack of robust data protection regulations and the potential for abuse of collected data pose serious threats to individual privacy and freedoms.

c. Propaganda and threatening

- Informant Networks and Citizen Surveillance

  To supplement technological surveillance, the Saudi government employs a network of informants and encourages citizen reporting. Official channels such as hotlines and online reporting platforms are available for citizens to report suspicious or subversive behaviour. This network of informants fosters a culture of fear and self-censorship, as individuals are wary of being reported by neighbours, colleagues, or even family members for expressing dissenting views. This pervasive surveillance culture effectively stifles free expression and reinforces government control. The combined effect of these surveillance measures results in a tightly controlled environment where privacy is routinely invaded.

  Authorities maintain extensive censorship and surveillance systems, supporting online networks of bots and accounts that spread pro-government messages and target perceived dissenters, particularly the infilitration of X, formerly known as

Twitter, spreading propaganda in support of Saudi Arabia. The goal of these domestic manipulation operations is to fabricate an appearance of widespread support for the state and its leaders while silencing dissenting voices, thereby eroding the right to information and democratic principles. In fact, Saudi Arabia is the second country after China, with the highest number of removed accounts by Twitter, and one of the most censored countries globally, blocking vast swathes of the internet deemed objectionable under their respective cybercrime legislation, especially regional human rights monitoring organisations

4. Involvement of the West

It is important to note that the West is somewhat involved, in the way in which nations are tacit when it comes to economic, strategic, and military interests in the region. Major corporations invest in sectors like oil, technology, and construction, sometimes supporting industries linked to worker exploitation. Western countries are significant arms suppliers to Saudi Arabia, indirectly supporting actions like the Yemen conflict, which has resulted in civilian casualties and alleged war crimes. Diplomatic and political alliances further enable Saudi repression of political dissent, suppression of women's rights, and exploitation of migrant workers, as muted criticism from Western nations often serves as tacit approval. This relationship underscores the need for a more conscious approach that acknowledges the upholding of human rights as sine qua non- alongside their economic and strategic interests. In this section, the Western involvement in Neom will be exposed, as well as Information and Communications Technology (ICT) sales in the region, with three case studies on BAE Systems, Pegasus spyware and on Google Cloud.

- Investment in Neom

Western companies have significant investments in the NEOM project, the $500 billion mega-city initiative. Notable companies like IBM, Cisco, and McKinsey & Company are involved as strategic partners, providing advanced AI, smart city infrastructure, and consultancy services. Additionally, Siemens and General Electric contribute sustainable energy solutions and smart infrastructure, while tech giants Microsoft and Google supply cloud computing and AI technologies. Construction and engineering firms such as Bechtel and AECOM are also pivotal, leveraging their expertise to develop NEOM's advanced urban environment. The centralised nature of data collection and the lack of robust privacy protections in Saudi Arabia pose risks for abuse, indeed, the state's ability to monitor and control digital and physical movements could lead to severe restrictions on personal freedoms.

There is limited transparency regarding how data will be used, stored, and protected. This lack of clarity exacerbates concerns about potential misuse of data for purposes beyond urban management, such as political repression or social control.

This involvement has raised significant ethical concerns. Amnesty International's Peter Frankental highlights the "moral dilemma" faced by architecture studios like Morphosis, Zaha Hadid Architects, and UNStudio, which are involved in designing NEOM despite reported human rights violations, including forced evictions and death sentences for those resisting displacement. Frankental argues that while the Saudi government is responsible for these abuses, the firms benefit financially and should reconsider their participation, given the project's association with severe human rights issues. This includes the treatment of migrant workers and the extensive surveillance planned for NEOM, emphasising the need for companies to perform due diligence and hold the Saudi government accountable.

However, these companies should not even be investing in the first place, as they should follow and implement the UN Guiding Principles on Business and Human Rights upon their consideration of investing in a country which is notorious for its poor human rights record.

- **Information and Communication Technology (ICT) deals and sales**

International trade in the ICT sector can bring a certain degree of development and innovation in a country, but can also introduce increased human rights risks to the importing country. It is important to emphasise the human rights implications in the export of ICT and surveillance technology to authoritarian countries. Reports have highlighted that European and American companies have exported surveillance technologies in response to the Arab Spring, from 2010 to 2012, to countries such as Syria, United Arab Emirates, Qatar, Oman, Algeria, and notably Saudi Arabia: these technologies have facilitated the advancement of their respective mass surveillance systems.

- **Case studies:**

A. BAE Systems

British arms giant BAE Systems is one of the world's most advanced, technology-led defence, aerospace, and security solutions. In 2017, reports uncovered that the company made significant sales of mass surveillance software called Evident, acquired after the purchase of Danish company ETI in 2011, to governments in the Middle East, including those involved in crackdowns on pro-democracy activists, including Saudi Arabia.

The UK government has approved more than $4.2bn of arms to Saudi since the start of the conflict in Yemen 2015, and last month The Times reported that the British government supported the company to secure a long-awaited Typhoon jet contract with Saudi Arabia for 48 new aircrafts.

Furthermore, Olly Sprague, Amnesty UK's programme director for military, security and police, criticised the fact that BAE is hiding behind the UK's "warped rules on arms exports. BAE Systems acknowledge they have more than 6,000 people working in Saudi Arabia helping to strengthen the country's arms capability – so it is outrageous that they continue to hide behind the UK Government's warped 'rules' on arms exports as a justification for their work".

This British technology is being used to endanger the security of activists and dissident groups, enabling severe human rights violations.

B. Pegasus spyware

Pegasus is a spyware developed by the Israeli[1]cyber-arms company NSO group, which "helps government agencies to detect and prevent a wide range of local and global threats". It was sold to Saudi Arabia in 2017. Other Israeli surveillance technologies have been purchased by the Kingdom, including Quadream. However, Pegasus has more advanced technology than other spyware and has changed cyber warfare.

Pegasus spyware can infect devices through spear-phishing via text messages or emails, or by exploiting app or operating system vulnerabilities, allowing zero-click exploits. Once installed, Pegasus can access virtually all data on the infected device, including emails, text messages, call logs, contacts, and browsing history. It can activate the device's microphone and camera for real-time surveillance and capture encrypted messages from secure apps like WhatsApp, Signal, and Telegram. Marketed as a tool for combating terrorism and crime, Pegasus has been widely misused by governments to target journalists, human rights activists, political dissidents, and critics. Investigations, such as those by the Pegasus Project, have revealed extensive unlawful surveillance. Known for its technical sophistication, Pegasus remains hidden on devices and can self-remove to avoid detection. Its use has raised significant legal and ethical concerns, prompting lawsuits, investigations, and calls for stricter regulation and oversight of cyber surveillance tools.

Reports say that Pegasus was used to track and spy on Jamal Khashoggi before his killing, as discussed earlier in this paper.

This technology is severely endangering the lives of journalists and activists in Saudi Arabia, once again allowing digital rights violations leading to human rights abuses.

C. Google Cloud

[1] Israel is seen as a Western-inspired nation-state, integrated in the "international community", this is why Pegasus spyware is under the section of case studies of western involvement.

US tech giant Google has installed a new Cloud Region in Saudi Arabia, facilitating small to medium-sized businesses' operations by eliminating the need for their own data centers and servers. This project, a joint venture with Saudi state-owned oil company Aramco, raises significant concerns as it enables the state to access vast quantities of personal data. Marwa Fatafta, Middle East and North Africa policy manager for digital rights group Access Now, emphasises the lack of safeguards in place, suggesting the initiative prioritises profit over human rights. Google's longstanding commitment to respecting human rights, as claimed by a spokesperson, contrasts sharply with the reality highlighted by advocates, who argue that the company's disclosures and commitments are insufficient. The partnership between Google and the Saudi government enhances the potential for national digital repression, allowing for extensive surveillance and control over citizens' digital activities. It is important to urge Google to delay cloud projects in regions lacking robust data protection frameworks. By providing infrastructure that could be used for mass data collection and analysis, Western companies like Google are indirectly contributing to human rights abuses in Saudi Arabia, enabling the government to monitor and suppress dissent more effectively.

5. Conclusion:

Saudi Arabia's hosting of the Internet Governance Forum (IGF) highlights the country's hypocrisy regarding digital rights and human rights. The IGF, a United Nations initiative, aims to promote open and inclusive dialogue on public policy issues related to the internet, emphasising the importance of human rights in the digital age. However, Saudi Arabia's record in this domain is marred by extensive violations, including severe restrictions on freedom of expression, pervasive surveillance, and systematic censorship. Saudi Arabia's investment in advanced surveillance technologies and its collaboration with international technology companies further entrench its capacity to monitor, censor, and suppress dissent. Projects like NEOM epitomise this surveillance culture, raising significant concerns about privacy and digital rights. The involvement of Western corporations and governments in these initiatives underscores a troubling complicity, prioritising economic and strategic interests over the upholding of fundamental human rights.

By hosting the IGF, Saudi Arabia projects an image of commitment to digital innovation and global dialogue on internet governance. However, this facade masks a reality of systematic human rights abuses and digital rights violations. The Kingdom's participation in such an international forum should serve as a reminder of the urgent need for genuine reforms and accountability. The international community must not overlook these contradictions and should continue to press for substantive changes that align with the principles and values the IGF represents.

The decision to award the hosting of the IGF to Saudi Arabia is a reminder of the complexities and contradictions in the global landscape of digital and human rights. It is a call to action for all stakeholders to ensure that the fundamental principles of human rights are upheld, not just in rhetoric but in practice, adhering to the United Nation's Universal Declaration on Human Rights.