Mapping Tech Companies' Cloud Expansion in the Gulf and Its Human Rights Implications-Policy Brief

SMEX

Executive Summary

Since 2018, major US and Chinese tech companies have increasingly invested in data centers in the GCC[1] states, whose financial incentives have made them a regional digital hub. However, the collaboration between corporations that lack transparency about data processing and security measures, and states that restrict freedom of expression, dissent, and media access, raises serious human rights concerns.

This report based on SMEX's research titled **Mapping Tech Companies' Cloud Expansion in the Gulf and its Human Rights Implications,** introduces how data centers work and maps the factors driving the investments of nine US and Chinese tech companies in the Gulf. Finally, the report highlights the human rights risks associated with constructing data centers in the Gulf, including inadequate data protection laws, oppressive state practices, and the lack of transparency around business activities. The report concludes with recommendations addressed to companies, civil society, and the US Congress.

Research Overview

Given that publicly available sources were limited, the research process was primarily based on a literature review of announcements published on companies' and governments' websites and news sources covering investments in data center projects. This phase of quantitatively mapping data centers by foreign tech companies in the Gulf lasted eight months. The nine tech companies (Amazon, Equinix, IBM, Google, Microsoft, Oracle, Alibaba, Huawei, and Tencent) were selected due to their current or planned investments in six GCC states. The companies' public commitment to support GCC governments in implementing their national visions and ambitions of digital transformation, together with the governments' poor data protection legal framework and severe repression of civil liberties, is concerning for the protection of human rights in the region, not only in the Gulf but the WANA in general.

Discussion/Analysis

A data center is a physical facility comprising servers, networked computers, storage systems, and computing infrastructure. It serves as fundamental infrastructure in the broader digital ecosystem and is integral to the functioning of the internet and digital economies at large.

Data localization (keeping data within the region/country it originated from) and data sovereignty (subjecting data to its hosting country's laws and governance structure) are two important factors when deciding where to build a new data center. By applying these two principles, we find that the nine companies' current and future investments in constructing data centers in the Gulf could enable host governments to have unobstructed access and legal control over a massive amount of data in the Gulf and the WANA region at large. For companies, their expansion towards states that aim to establish their position in the digital sphere by becoming a hub for the digital economy is perceived as a chance for high economic profits.

[1] **The Gulf Cooperation Council is a regional political and economic institution comprising Saudi Arabia, the United Arab Emirates, Qatar, Bahrain, Kuwait and Oman.**

The main political and economic factors underlying growing cloud investments in the GCC include the rapid growth of the data center infrastructure market, the projected increase in data consumption, as well as the GCC states' diversification away from an oil-dependent economy to digital infrastructure through the establishment of Economic Free Zones. To attract investors, states adopt modernizing "national visions" and "digital transformation programs" through regulations that offer companies massive financial benefits. Aiming for digital transformation across various sectors of society (i.e., health, housing, industry, etc.) through digitizing government services, GCC states obtain unimpeded access and control over massive amounts of data. At the same time, investment companies create most of the digital infrastructure of government entities.

For several reasons, the large-scale construction of data centers in GCC states, mainly Saudi Arabia and the UAE, is alarming from a human rights perspective. First, these states have been criticized for systematically violating a number of fundamental human rights principles, including the UNDHR's Articles 12 (right to privacy) and Article 19 (freedom of opinion and expression). They have also used surveillance systems and spyware (i.e., Pegasus) to discourage dissent and track and punish critics. The recently adopted personal data protection laws in Saudi Arabia and the UAE contain vague decrees and various legal loopholes. These laws favor government control, allowing authorities to oversee data stored within their borders. While it is common for governments to have control over data stored within their borders, the real concern lies in the track record of human rights violations in these countries. Given their history of infringing on rights like freedom of expression, this control raises significant red flags regarding protecting personal data.

Tech corporations must also be held accountable. They implicitly support these states by providing them with the essential infrastructure to enable these regimes to gain control over the region's localized data. Without giving any public evidence of their human rights impact assessments, there is no guarantee that these corporations will abide by their business and human rights obligations. Due diligence before initiating a project and transparency regarding the process' findings are necessary for respecting and promoting human rights.

While this research primarily focuses on US-based companies, it is essential to acknowledge the implications of investments by Chinese companies in the Gulf region. There are concerns regarding the potential for technologies developed by these companies to be utilized in ways that could enhance surveillance capabilities within GCC states. Given that the digital infrastructure is built within their jurisdiction, there are some ambiguities about the extent of data access and the potential for sensitive information to be exposed to external entities.

Recommendations:

The report concludes with recommendations to:

Tech companies:

a. Conduct thorough Human Rights Impact Assessments (HRIA) before launching data centers in new markets and make the findings of these assessments public.

b. Delineate the users' or companies' legal liability for human rights violations.

c. Disclose the process for handling government demands for users' data.

d. Publicize data on numbers and types of government demands.

Civil society:

a. Research, document, and publicize the implications of data centers in the Gulf on human rights. Conduct extensive research on:

- **i)** possible implications of technologies that will be transferred to GCC countries through the construction of these data centers;
- **ii)** the impact of the construction of these data centers on data flows around the wider WANA region.

b. Pressure Big Tech companies operating in the Gulf to ensure transparency and respect for human rights through public campaigns.

US Policymakers:

a. US policymakers should create a law that requires US-based companies to manage human rights risks related to their activities.

- **i)** The law should regulate the activities of subsidiaries, suppliers, and subcontractors connected to the company, especially when they have access to data.
- **ii)** The law should state that companies must:
  - Establish, implement, and publish their own HRIA.
  - Include risk mapping, a risk mitigation plan, periodic compliance assessments, and an efficiency monitoring scheme in their HRIA.

b. Finalize the National Action Plan on Responsible Business Conduct.