Date : 06/07/2021

Vodafone's use of customer service centres in Egypt is a major threat to customers' security and privacy

Arab Organisation for Human Rights in the UK (AOHR UK) notes with concern Vodafone's continued outsourcing of call centres serving many countries – including Britain, Germany, and Ireland – to Egypt. Our concerns relate to repressive data monitoring policies employed by the Egyptian regime and how this constitutes a major threat to the data and privacy of customers and companies in these countries.

AOHR UK has sent letters to Vodafone, and other institutions concerned with monitoring telecommunications companies, but none of them responded. Despite well-documented evidence, the Egyptian regime routinely violates privacy and spies on its citizens and foreigners.

AOHR UK notes that in 2018 the regime of President Abdel Fattah Al-Sisi introduced the Law on Combating Cyber Crime, which provides the state with the authority to conduct online surveillance, block websites, and monitor internet users and communications services in Egypt. Since then, more than 500 websites have been shut down under Anti-Cyber And Information Technology Crimes legislation. Under this legislation, parliament has strengthened the government's ability to target social media accounts, which are classed as public websites, leading to at least 5,000 accounts being placed under surveillance.

These regulations also require internet service providers to retain and release personal information to security services upon their request following the issuance of a judicial order.

AOHR UK also notes that the Sisi regime uses Cerebro software from Amesys, enabling the Egyptian authorities to conduct comprehensive surveillance of communications through Deep Packet Inspection. This includes voice calls, text messages, locations, emails, instant messages, social networks and search histories.

Moreover, the Egyptian regime uses spy software produced by Israeli company NSO Group. The software works through hacking individuals using links. Users who open a link will, without their knowledge, download and install a program called Pegasus, which allows the government operator to access the user's data, including passwords, contacts, calendars, text messages and direct voice calls. The operator can even use phone cameras and microphones remotely to capture and record activity in the surroundings of the phone.

The regime's use of such software and surveillance practices, and the direct implications for freedom of expression and privacy, is well known. These issues are detailed in numerous international human rights reports.

AOHR UK also notes that the security environment in Egypt means that employees in customer services centres could be recruited to work for the security services and then leak personal and company data from the countries using Vodafone's services. AOHR UK would like to know what, if any, measures Vodafone took to avoid such threats.

AOHR UK finds it shocking that a major international company like Vodafone, which dominates much of the market in numerous countries and is highly profitable, would sacrifice the security of its own customers and staff by outsourcing call centres to a repressive kleptocratic state entwined in violent repression in its pursuit of profit.

AOHR UK is alarmed that in outsourcing customer service operations to Egyptian bodies the company leaves users of its telecommunications network open to surveillance and data capture by Egyptian security forces, in violation of the right to privacy.

Arab Organisation for Human Rights in the UK (AOHR UK)