Crime and telecommunication networks: perspectives on liability of communication providers for misconduct of third parties

The rapid advancement of technology has created new opportunities for criminal activities, often making it easier for individuals to engage in illicit behavior while remaining anonymous or difficult to trace. The misuse of Information and Communication Technology (ICT) to commit crimes poses significant challenges for law enforcement. As technology continues to evolve, so do the methods employed by criminals. Common ways that ICT can be misused to commit crimes are among others cybercrime, extortion and blackmail, human trafficking and exploitation, financial crimes as well as spreading disinformation. Often, these types of crimes are interlinked, as perpetrators may employ multiple methods and technologies to facilitate their illicit activities, creating a complex web of criminal behavior.

In such an interconnected world, the role of communication providers has expanded beyond mere service provision to encompass significant responsibilities regarding the use of their networks. A pressing question that has been emerging, together with the raising usage of ICT, is whether such providers can be held accountable for systematic criminal practices that occur across international borders using their services.

It has been documented that modus operandi of the human trafficking networks is continuously reliant on usage of ICT to exchange intelligence, extort money, as well as transmit the audio-visual record of abuse of victims of human trafficking to threaten their families. Within human trafficking networks, refugees, migrants and asylum seekers are held captive and subjected to torture in order to demand ransom from their families and communities. They are coerced into reaching out to their relatives using the phone lines, pleading for ransom payments that can amount to thousands of US dollars. Rather than being freed after the payment is made, these victims are frequently sold to other human traffickers, who then compel them to secure additional ransoms from their loved ones.

While telecom companies act as intermediaries rather than content providers, they are still subject to various legal frameworks that dictate their responsibilities and obligations in criminal investigations. This article examines the liability of telecom providers in cross-border crimes, focusing on geographical locations of Europe, Libya, Eritrea, and Ethiopia.

Telecommunication providers and the public carrier principle

Telecom providers often operate under the public carrier principle, which means that they provide services to the public without discrimination but are generally not responsible for the content transmitted through their networks. However, they are often required to comply with data retention laws, provide surveillance assistance to law enforcement, and adhere to privacy and cybersecurity regulations. The extent of their obligations varies depending on the legal framework governing each country.

Telecom providers' liability in the European Union

The European Union has established a well-defined legal structure regulating telecom providers, balancing thin line between strict data privacy and law enforcement cooperation. Key regulations governing the liability of providers include:

1. *E-Commerce Directive (2000/31/EC)*

This directive which sets up a framework for regulating online services shields service providers from liability when they act as "mere conduits" - that is, when they simply transmit information without altering it. According to Article 12 of the Directive, service providers are not responsible for the content they transmit unless they initiate the transmission, modify it, or select its recipient. Therefore, in terms of responsibility for illegal content, it is important to differentiate between liability of provider's own content and liability for content created by third parties.

2. *General Data Protection Regulation (GDPR) (2016/679)*

GDPR ensures that telecom companies protect personal data while allowing access to law enforcement under strict conditions. Cross-border investigations require legal justifications to access stored telecom data, particularly when the crime involves multiple jurisdictions.

3. *ePrivacy Directive (2002/58/EC)*

This directive further governs the confidentiality of electronic communications, preventing unauthorized interception while permitting lawful access for criminal investigations. It requires providers to ensure the confidentiality of communications and to take measures against unauthorized access. However, it does not impose a direct obligation to monitor user communications for criminal activity.

4. *Directive on European Investigation Order (EIO) (2014/41/EU)*

The EIO facilitates cross-border cooperation in criminal cases by allowing authorities in one EU country to request access to telecom data from another country under streamlined procedures.

5. *Budapest Convention on Cybercrime (ETS No. 185, 2001)*

The convention provides an international legal framework for combating cybercrime, requiring signatory states to facilitate cross-border cooperation in obtaining telecom records when necessary.

Telecommunications providers face significant concerns regarding crimes or illegal activities committed by their customers using their services. While these providers are generally not held responsible for the actions of their users, they are expected to take reasonable measures to prevent and address criminal behavior. This includes implementing robust security protocols, monitoring for suspicious activity, and cooperating with law enforcement when necessary.

Telecom providers' liability in Libya, Eritrea, and Ethiopia

Libya's framework for governing telecommunications is still evolving. Telecom providers operate under state regulation, and the government exerts significant control over communications infrastructure. Currently, there is no specific data protection law in Libya. However in recent years, Libya has witnessed a significant transformation in its legal framework with the introduction of pivotal legislation addressing cybercrime and electronic transactions. Law No. (22) of 1378 FDP (2010 AD) on telecommunications governs telecommunications in Libya and establishes the legal obligations of telecom providers. It mandates cooperation with law enforcement for national

security purposes, including lawful interception of communications and data retention requirements. The law also outlines penalties for telecom companies that fail to comply with government directives. However, this regulation does not constitute any direct liability of telecom providers for the crimes or any illicit activities carried out by their beneficiaries.

While the Law No. 5/2022 on Combating Cybercrime in Libya introduced specific provisions targeting several forms of cybercrimes, including online fraud, human trafficking, identity theft, and terrorism, it also has been criticized for incorporating controversial and vague definitions. This could grant the National Information and Security and Safety Authority (NISSA), the body responsible for monitoring and surveillance of ICTs in the country, power to censor content and go against freedom of speech. The law does not consider specific regulation of telecom providers under its articles.

Eritrea has one of the most restrictive telecommunications environments in the world. The government maintains a monopoly over telecom services through the Eritrea Telecommunication Services Corporation (EriTel), the country's sole provider. As a state-owned entity, EriTel operates under full government supervision, making telecom liability a non-issue in the traditional legal sense. The state directly oversees all communications, eliminating any notion of private-sector responsibility. The government exercises broad authority to monitor all communications, effectively eliminating privacy protections. Telecom provider acts as an arm of the government rather than an independent entity. It remains unclear how the providing telecommunication services is regulated within the state laws. Proclamation No 102/1998 on communications is aimed at regulating telecommunications, broadcasting and post in the country. While establishing, duty of confidentiality of operators, suppliers and installers, the detailed applicability and liabilities remain veiled under the current political climate in the country. The human rights situation in Eritrea remains dire. The regime has been known for its repressive tactics, including the suppression of free speech, arbitrary detention, and the absence of a free press. Reports of torture, extrajudicial killings, and widespread human rights abuses are common.

In Ethiopia, telecommunications providers are regulated primarily by the Ethiopian Communications Authority (ECA), which was established to oversee the telecommunications sector and ensure compliance with relevant laws and regulations. The regulatory framework has evolved over the past years. Ethiopian Communications Service Proclamation (No. 148/2019) primarily focuses on the establishment of a competitive telecommunications market, the licensing of service providers, and the protection of consumer rights. While the proclamation may impose certain obligations on telecommunications providers to cooperate with law enforcement and regulatory authorities, it does not specifically state that providers are liable for criminal acts committed by their users. Computer Crime Proclamation No. 958/2016 defines computer-related crimes, making it mandatory for providers to assist in investigations. While the providers have a duty to report to the police about any illegal content that is being carried out by the third parties, the liability of those crimes lies with the perpetrators not the service providers. Similarly, under the Anti-Terrorism Proclamation No. 652/2009 communication service providers are required to cooperate with the Ethiopian National Intelligence and Security Service to carry out surveillance when there is a threat of terrorism.

All three African countries of the present article - Libya, Eritrea, and Ethiopia - have mandatory SIM card registration policies as part of their national security and crime prevention strategies. These policies require mobile users to provide official identification when purchasing and activating a SIM card. Governments justify this regulation as a means to combat fraud, terrorism, and cybercrime by ensuring that every phone number is linked to a traceable individual. However, in countries with strong state surveillance, such policies have also raised concerns about privacy violations and potential misuse of personal data.

The varying approaches to liability of telecommunication service providers in Europe, Libya, Eritrea, and Ethiopia highlight the balance between security, data privacy, and regulatory oversight. While EU regulations prioritize strict data protection of users and legal oversight, African countries discussed in this article seem to emphasize national security and state control, often at the expense of user privacy. Within the EU laws telecom providers are protected from direct liability of crimes committed by their customers but must comply with regulations requiring data retention when it comes to cooperation with law enforcement. Similarly, while telecom providers in Libya and Ethiopia are not directly liable for crimes carried out by third parties, they are required to comply with government orders for surveillance and interception, particularly in cases related to national security. In Eritrea, telecom services are fully controlled by the government, liability does not apply in the same way as in private markets. The state is responsible for monitoring and enforcing communication laws. In all cases, while telephone providers are generally not held criminally responsible for cross-border crimes committed over their networks, they are required to comply with national and international laws regarding surveillance, data retention, and law enforcement cooperation. Liability for crimes committed over the phone lines or electronic platforms lies with the users rather than providers.