AFRICTIVISTES

POLICY ANALYSIS

JUNE 2020

ENDCODE
Tech. Law. Policy. Africa.

Theme: Freedom of expression

Name of Country: Niger

Relevant Legislation : Loi N•0267 sur la lutte contre la cybercriminalité au Niger, 25 juin 2019 ; Constitution of Niger

Niger is a member of Economic Community of West African States (ECOWAS) and has ratified several conventions providing for human and digital rights, such as the ECOWAS Directive C/DIR/1/08/1, and the Council of Europe Convention of 23 November 2001 on cybercriminality.

The right to freedom of expression in section 30 of the Constitution of the Republic of Niger provides for" "*the right to freedom of thought, of opinion, of expression, of conscience, of religion and of worship*". Section 30 states this right should be exercised with respect for public order, for social peace and for national unity and is accordingly balanced against these three.

The Cybercrimes Act was passed to ensure the safety and security of citizens online and address cybercrimes. The Act provides for:

a) the prevention of acts that infringe the confidentiality, integrity and availability of computer systems and data, as well as their fraudulent use, and
b) provides for the rules of criminal procedure relating to offenses relating to computer systems and data and electronic communication networks.

Penalties for infringement are set out hereunder:

- Article 30: The article provides that whoever utters any outrageous expression, any term of contempt or any criticism which is false, by way of electronic communication may be imprisoned for 6 months to 3 years or a fine of 1 million to 5 million CFA francs.
- Article 31: The article provides that whoever produces, makes available to others or disseminates data likely to disturb public order or to infringe human dignity through an information system may be imprisoned for 6 months to 3 years and from 1 million to 5 million CFA francs fine.

International best practices dictate, a limitation on rights must be reasonable and proportional, in an open and just society. The limitation to the right must be absolutely essential to achieve the said legitimate objective and meet the test of proportionality. Reasonable and proportionate limitations that are objectively justifiable are permissible in terms of international laws and norms. Therefore, each case would need to be judged on its circumstances. Imprisonment solely on the basis that the communication/ expression criticises the state, cannot qualify as a legitimate objective. However, the circumstances of a particular matter will be the deciding factor on whether the arrest of an individual for contravention of the Cybercrimes Act was done so in a reasonable and justifiable manner or not. For a punishable offence in terms of the Act, "criticism" is not the criteria but rather the truth of the information.

Policy Recommendations:

1. Awareness Building - Practical steps to foster educational training initiatives should be undertaken to provide an understanding of the law, an understanding of spreading false data (“fake news”) and the penalties for deliberately or unwittingly infringe these laws.

2. Multi-stakeholder approach to make submissions and engage in public consultations for the clarification of certain sections in the Act that are broad or unclear.

Theme: Data Protection and Privacy (Interception of Communications)

Name of Country : Niger

Relevant Legislation : Loi portant interception de certaines communications émises par voie électronique au Niger, 29 mai 2020 ("the Law")

The fight against terrorism using interception methods requires a balancing act between national security and the right to privacy (set out above). The criteria for interception of communications ought to be clearly defined through consultative and considerate policy-making and legislative drafting.

Privacy International has raised the following concerns within Niger:

a) **Authorisation and Oversight**: Currently, the discretion to approve an interception request lies exclusively with the President. The Law establishes the Committee of Control of Security Interceptions ("CCSI"), which has limited oversight powers and whose findings on an interception are not binding on the Government. The composition of the CCSI with "all but 2 [having been] appointed by the executive". Amendments to the Law must provide for a judicial oversight process - state actors who authorise any interceptions of communications are required to, after the fact, submit a written report to the allocated judicial officer, justifying the lawful basis for the interception. There must be sanctions for a failure to do so. Section 51(1)(a)(i) of South Africa's Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 provides for such an offense.

b) **Wording and Substance of the Law**: The wording and substance of the Law needs to be assessed for ambiguity and over-broadness, and then narrowed down to a point where there can be no confusion as to what lawful bases the State may rely on to intercept communications. Further, definitions should be revised for clarity and universal interpretation across the Republic.

c) **Notification**: it is important that the recognition and implementation of a duty to notify or inform individuals after they have been subjected to interception measures by the State is included in any amendments to the Law. Currently, citizens of Niger subject to monitoring and interception activities by the State have no awareness thereof.

d) **Limitations on the involvement of telecommunication operators in Niger**: under the Law, telecommunication operators cannot challenge any penalties incurred by a refusal to assist the government in surveillance activities and failure to cooperate is penalised by 1 to 3 years of imprisonment and a steep fine. Accordingly, it is recommended that amendments be made to the Law limiting the State to only be entitled to compel the cooperation of telecommunication operators in instances where a public interest is apparent, where judicial authorisation has been received and/or where a national disaster or state of emergency has been duly declared.

Article 44 of the Constitution highlights that in the interpretation and enforcement of its laws, "*especially those that concern fundamental human rights such as free expression, the Republic of Niger should be mindful of international regulations*."

Policy Recommendations:

1. **Alignment with The ITU *Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean* (HIPCAR) policy guidelines** on the interceptions of communications is a strong example of the considerations and level of detail that should be taken into account. The Model policy guidelines include:

    a) The establishment of necessary common interpretations for key terms associated with interception of communication.
    b) Defining the role of the parties in charge of managing interception of communication;
    c) Defining the legal mandates and the standards to which interception of communication shall be bound;
    d) Defining exemptions from compliance with the interception of communications;
    e) Establishment of procedures for oversight, enforcement, review and appeal in connection with interception of communication; and
    f) Establishment of a framework of interception of communication in conjunction with public policies on related matters.

2. **Awareness Building** - Practical steps to foster educational training initiatives should be undertaken to provide an understanding of the law and the requirement of consent.
3. **Multi-stakeholder approach** to make submissions and engage in public consultations for the clarification of certain sections in the Act that are broad or unclear.