

# Information on Legal Frameworks in Rwanda Pertaining to Privacy and Freedom of Expression

## 1. PROVISION OF REAL-TIME LAWFUL INTERCEPTION ASSISTANCE

### 1.1 Rwandan Constitution

The confidentiality of correspondence and communications is protected under article 23 of the Rwandan Constitution except in circumstances and in accordance with procedures determined by the law.

### 1.2 Law 30/2013 Relating to the Code of Criminal Procedure

Under article 72 of Law 30/2013, if all other investigative procedures for uncovering evidence to establish the truth in relation to an offence against national security have been unsuccessful then the public security organs (defined in article 158 of the Constitution as the Rwanda Defence Force, the Rwanda National Police, and the National Intelligence and Security Service) may, upon written authorisation from a competent National Prosecutor appointed by the Minister in charge of justice (the Prosecutor General of Rwanda or his delegates), intercept private communications. This may include communications made by telephone, email, over the internet or by other means.

'National security' is defined as, 'measures taken by the country to ensure its security, including those measures aimed at preventing and defending itself against attacks from inside or outside and any other acts that may undermine national safety.'

Such an authorisation must be in writing, containing details of 'items or connections' to be intercepted and indicating the relevant offence being investigated. If required by 'urgent public security interests', the interception warrant can be issued by the National Prosecutor verbally but this must be followed by a written warrant within 24 hours or the interception will be presumed illegal.

Authorisation of interceptions under this law are valid for three months, but can be renewed for one further three month period.

Under article 73, a person whose communications are unlawfully intercepted may file a complaint with the High Court (or the Military High Court for those in the military). However, the filing of such a complaint does not entail suspension of interception.

### 1.3 Law 60/2013 Regulating the Interception of Communications

Law 60/2013 reaffirms and extends the provisions under Law 30/2013 relating to interception of communications.

Article 5 of the Law 60/2013 states that the interception of any communication made by means of a public or private communication system without authorisation from a competent authority is unlawful.

Article 9 states that a warrant for lawful interception can be granted by a National Prosecutor designated by the Minister in charge of justice. Only specified security organs (the Rwanda Defence Force, Rwanda National Police and the National Intelligence and Security Service) are authorised to apply for such a warrant.

If required by 'urgent public security interests', the interception warrant can be issued by the National Prosecutor verbally but this must be followed by a written warrant within 24 hours or the interception will be presumed illegal.

Communication service providers ("**CSPs**") have an obligation under article 7 to ensure that their systems are technically capable of supporting interceptions at all times. Article 123 of Law 24/2016 also states that all entities authorised to carry out lawful interception must be notified of any upgrade to an electronic communications network or service.

However, any competent security organ making an application for an interception warrant under article 9 may request a warrant to intercept the communications directly, without recourse to a communication service provider (article 10). In practice this is conducted by the National Intelligence and Security Service of Rwanda as the entity entitled to possess the necessary equipment for such direct interception under the Law Relating to Arms 33/2009.

Article 12 provides for inspectors to be appointed by Presidential Order to monitor authorised persons and ensure that they intercept communications in accordance with the law. This role is performed by a police officer if requested by the Criminal Investigation Department or the National Intelligence and Security Service if requested by the Prosecutor General's Office.

This law strictly prohibits the interception of the Rwandan President's communications.

## **2. DISCLOSURE OF COMMUNICATIONS DATA**

The provision of metadata relating to communications is governed by the same laws and process as set out above for interception of communications.

## **3. NATIONAL SECURITY AND EMERGENCY POWERS**

### **3.1 Law 24/2016 governing Information and Communication Technologies**

'In order to protect the public from any threat to public safety, public health or in the interest of national security', the Minister in charge of ICT has the power under article 22 to direct the Rwanda Utilities Regulatory Authority ("**RURA**") to suspend or restrict a legal or natural person's entitlement to provide an electronic communications network or service or any associated facility. This enables the government to require CSPs' to shut down their networks in such situations.

Any aggrieved party can appeal such a decision to RURA itself and article 17 provides a further right to appeal its decision to the competent Court.

## **4. CENSORSHIP-RELATED POWERS**

### **4.1 Law 24/2016 governing Information and Communication Technologies**

Article 60 states that no person may send a message or any other matter that is grossly offensive or is of an indecent, obscene or menacing character by means of a public electronic communications network, or cause such a message or matter to be sent. It also states that no person may send or cause to be sent false messages by means of

a public electronic communications network or persistently using a public electronic communications network to cause annoyance, inconvenience, or needless anxiety. These terms are not defined and while the legislation states that the 'Regulatory Authority makes and publishes instructions for the implementation of this article', no such guidance has yet been published.

In matters related to national sovereignty and 'in a bid to comply with national legislation and international instruments ratified by the country', article 126 of Law 24/2016 gives the Minister in charge of ICT the power to:

- 1) interrupt or cause to be interrupted any private communication that appears to be detrimental to national sovereignty, contrary to any existing law, public order or good morals;
- 2) suspend, wholly or in part, any electronic communications service or network operations for a specified or undetermined period; and/or
- 3) requisition or cause to be requisitioned any electronic communications infrastructure.

These powers may be used by the Minister in charge of ICT to require that CSPs block IP addresses connected to websites which display illegal content or even to take control of CSPs network if deemed necessary to uphold the law.

## **5. OVERSIGHT OF THE USE OF THESE POWERS**

### **5.1 Organic Law 03/2005**

Parliament exercises oversight over the actions of government departments at all levels via oral and written questions, committee hearings, inquiries and interpellation.

## **6. PUBLICATION OF LAWS AND AGGREGATE DATA RELATING TO LAWFUL INTERCEPTION AND COMMUNICATIONS DATA REQUESTS**

### **6.1 Publication of laws**

There are no restrictions in Rwanda on the publication of laws, descriptions of legal powers or related information.

### **6.2 Publication of aggregate data**

While no CSPs currently publish such information, there are no laws which prohibit the publication of aggregated data in relation to lawful interception and communications data requests.