CYBERSECURITY ASSESSMENT REPORT
DEMOCRATIC REPUBLIC OF CONGO
Articles 52 and 53 of the 2002 Framework Law concern the secrecy/confidentiality of correspondences emitted by way of telecommunications:

- Article 52 provides for confidentiality protections on correspondence transmitted through communications in the DRC. The confidentiality of correspondence can only be lifted in cases where it is strictly in the public interest as provided by the law.

- Article 53 reinforces confidentiality of communications. “The public operator, operators of utility, telecommunications and other providers of telecommunications services and members of their staff are required to respect the confidentiality of communications.”

Articles 54 (Section A) and 55 of the 2002 Framework Law: prohibits any form of surveillance on citizens’ communication, even by security agents, without prior authorisation from the General Prosecutor of the Republic. However, Articles 54(a) and 55 provides for the interception of communications in two scenarios:

- in the context of judicial cases where authorisation has been granted by the Attorney General of the Republic (“Attorney General”); and

- interceptions authorised by the Minister of the Interior concerning national security, protection of the essential elements of the scientific, economic and cultural potential of the country, or the prevention of crime and organised crime.

Article 54(a) prohibits the interception, phone-tapping, recording, transcription and disclosure of correspondence issued via telecommunications without the prior permission of the Attorney General. Article 55 addresses evidence and states that for the purpose of providing evidence in a court of law, the Attorney General must order the interception, recording and transcription of correspondence transmitted through telecommunications.

Article 59 of the 2002 Framework Law requires that interceptions authorised by the Minister of the Interior must have a purpose to: (i) seek information relating to national security; (ii) protect the essential elements of the cultural, scientific or economic potential of DRC; or (iii) prevent crime and organized crime.

Law 14/2002 on the Regulator

The Law 14/2002 on the Regulator establishes the regulatory body - Autorite de Regulation de la Poste et des Telecommunications du Congo known as the Authority of the Post and Telecommunications of Congo (ARPTC) - grants the right for the government, specifically the legislature, to “conduct site visits, conduct investigations and studies, and collect all the necessary data” from telecom service providers. This Law authorises the government to “collect all necessary data” from telecommunications companies when needed.

The Telecommunications and ICT Bill

Notably, a Telecommunications and ICT Bill (the “ICT Bill”) exists in draft which is aimed at revamping the Framework Law. The Telecommunications and ICT Bill will be known as the Telecommunications and ICT Framework when passed. In September 2019, the Telecommunications and ICT Bill was sent back from the office of the President for a further reading to remedy certain provisions.

Whilst the ICT Bill is not limited to data protection, it provides for the protection of the confidentiality of personal data, as stated in paragraph 1 of Article 125. Criticisms of the Bill, insofar as data protection and privacy are concerned, have included:

- The lack of “written consent” required from data subjects regarding the processing of their personal information; and
- Exclusions allowing the State to derogate from the confidentiality of correspondence under the Bill for reasons of internal and/or external security of the State, national defence or public order.

The ICT Bill also includes protections for the privacy of users in cases of cyber-attacks.

Other Draft Laws in Existence

Apart from the Telecommunications and ICT Bill, a Bill amending the Act that set up the regulator – the Authority of the Post and Telecommunications of Congo (ARPTC) - is in existence but is yet to be passed (CIPESA, 2017).

4.2.3. Data Protection Institutional Measures

4.3. Cybercrime and Cybersecurity

4.3.1. Overview of Cybercrime and Cybersecurity Legislation

There is currently no specific legislation for cybercrime and cybersecurity in force. However, the Democratic Republic of Congo has drafted the Telecommunications and Information Communications Bill (The “ICT Bill”).

The Telecommunications and ICT Bill

The ICT Bill exists in draft and is aimed at revamping the Framework Law. The Telecommunications and ICT Bill will be known as the Telecommunications and ICT Framework when passed. In September 2019, the Telecommunications and ICT Bill was sent back from the office of the President for a further reading to remedy certain provisions.

Whilst the ICT Bill is not limited to cybercrime and cybersecurity, its provisions define cybercrime and provide for sanctions against the perpetrators of cybercrimes. Under the ICT Bill, “cybercrime” is broadly defined as the set of offences committed employing computers or targeting them. It is also the set of offences committed against or by a computer system carried out through a telecommunications network. More simply, cybercrime is conceived as an act of intrusion for the theft, control or destruction of computer systems or databases. These may include methods of forcing access to a remote computer, modifying data and files, or implementing malicious programs on servers.

The ICT Bill has, however, been criticised for lacking enough provisions regarding cybercrime and cybersecurity.

4.3.2. Cybercrime and Cybersecurity Policy Developments

The Democratic Republic of Congo does not have a National Cybersecurity Strategy in place. A workshop was, however, organized in Kinshasa in August 2015 that assisted the country in raising awareness of cybercrime. To date, the government has not been greatly involved in working with the private sector on cybersecurity issues (African Union, Symantec, 2016).

Quoting from the Report:

“One of the biggest obstacles facing cyber security advancement in the DRC is that training remains a major obstacle. In addition, the authorities noted, computers and an internet connection are not accessible to most of the population in the first place” (African Union, Symantec, 2016, 67).
4.3.3. Cybercrime and Cybersecurity Institutional Measures

The primary institution relating to cybercrime and cybersecurity in the DRC is the Ministry of Telecommunications and New Technologies. This Ministry is responsible for cybersecurity and cybercrime-related efforts in the DRC.

At the time of writing, the DRC does not have any institutional mechanisms for responding to cyber incidents, including a CERT or other national-level cybersecurity infrastructure. Saying that, the establishment of a CERT has nonetheless been evaluated in the DRC (African Union, Symantec, 2016) and a draft decree establishing a CERT has been submitted for examination and adoption by the Council of Ministers. The strategies, operation and effective implementation of the CERT are already the subject of two bills under discussion in Parliament.

There is a plan to set up a national strategy as well as a roadmap for the effective implementation and actual operation of this centre. As at March 2019 according to the ITU, there is still no CIRT established (ITU, 2019).

4.4. ELECTRONIC TRANSACTIONS

4.4.1. Overview of Electronic Transactions Legislation

The Democratic Republic of Congo does not have a dedicated national electronic transactions law in place. Instead, it primarily relies on the revised OHADA Uniform Law, 2010 to regulate its electronic transactions and e-commerce sphere.

OHADA Uniform Law, 2010

The Republic of Congo has ratified OHADA Treaty of October 17, 1993, on May 28, 1997. Insofar as electronic commerce/transactions are concerned, the Republic of Congo relies on the 2010 revised OHADA Uniform Law on General Commercial Law which became effective in Member States in 2011.

The OHADA (Organization for Harmonization of Business Law) is the French Commercial Law common to all Francophone countries and serves as the country’s commercial law - subject to specific Congolese laws. Under the 2010 revised OHADA Uniform Law on General Commercial Law, Book V contains Chapters pertaining to the ‘Computerization of The Register Of Commerce And Securities, The National And Regional Registries’. These Chapters include provisions on general principles for use of electronic procedures; the validity of electronic documents and electronic signatures; use and conservation of electronic documents; use of electronic means for the transmission of documents; and publicity and electronic dissemination of registers information. Important provisions stemming from the Chapter on the validity of electronic documents include:

- Article 82 recognising the legal equivalence between electronic documents, electronic transmissions and paper documents - when such transmissions are established and kept in a reliable technique and which guarantee, at any time, the origin of the electronic document and its integrity during electronic processing and transmissions;

- Article 83 providing that electronic authentication and electronic signatures are given legal validity and may be lawfully utilised to identify a person/s. Article 83 also makes provision for the formation of electronic contracts consisting of intentions and obligations – providing for contractual liability for providers of goods or services by electronic means; and

- Article 84 regulates the use of electronic certificates to link signature-verification data to a person and confirm the identity of such persons. Article 84 also sets out the particulars that must be contained within an electronic certificate.

The Telecommunications and ICT Bill

Notably, a Telecommunications and ICT Bill (the “ICT Bill”) exists in draft which is aimed at revamping the Framework Law (No. 013/2002 of 16 October 2002). The Telecommunications and ICT Bill will be known as the Telecommunications and ICT Framework when passed. In September 2019, the Telecommunications and ICT Bill was sent back from the office of the President for a further reading to remedy certain provisions. The ICT Bill is unavailable for public consumption as of writing and cannot be assessed further.

Law No 86/033

Law No. 86/033 of 5 April 1986 on the Protection of Copyright and neighbouring Rights provides the basis for the protection of e-commerce Intellectual Property Rights (IPR).

Draft E-Transactions Bill

4.4.2. Electronic Transactions Policy Developments

A validation Workshop was concluded on 5 September 2019 for the Digital National Plan of the Democratic Republic of Congo (DRC) – known as “Digital Horizon 2025”, which constitutes the primary policy relating to electronic transactions and electronic commerce in the Democratic Republic of Congo.

The workshop aimed to "modernize the administration and pool resources and infrastructure to achieve significant gains in terms of efficiency and effectiveness; enable citizens and businesses to interact online with the public administration and partners; to provide users with better quality services that reduce costs and deadlines with the additional guarantee of maximum transparency " (H2T, 2019).

The National Plan was validated by various stakeholders in the DRC’s digital sector. The closing ceremony was attended by the Minister of Posts, Telecommunications and New Information Technologies and Communication, Emery Okudji, who represented the Head of State in the DRC, Felix Tshisekedi (H2T, 2019).

The national digital plan will be comprised of four core pillars, namely:

- infrastructure;
- production and hosting of content;
- application uses; and
- governance and regulation.

4.4.3. Electronic Transactions Institutional Measures
4.5. COMPARISON WITH THE AUCC PROVISIONS ON LAWS, POLICIES AND INSTITUTIONS FOR DATA PROTECTION, CYBERCRIME AND ELECTRONIC TRANSACTIONS.

<table>
<thead>
<tr>
<th>Policy and Governance Measures</th>
<th>Legislative and Regulatory Measures</th>
<th>Institutional Measures</th>
</tr>
</thead>
</table>
| **Cybersecurity Policy which recognises the Critical Information Infrastructure and identifies the risks to the nation and mitigation measures** | **Data Protection Laws and Regulations**  
No dedicated data protection law. | **Data Protection Authority whose responsibilities in regulating data protection include authorisation of data processing, authorisation of cross border transfers of personal data**  
N/A |
| **National Cybersecurity strategy to implement the Policy**  
The Democratic Republic of Congo does not have a National Cybersecurity Strategy in place. | **Electronic Commerce Laws and Regulations**  
There is a draft Electronic Transactions Bill. DRC subscribes to the OHADA Uniform Law. | **Electronic Signature Accreditation Authority that will regulate what constitutes a qualified electronic signature for the purposes of authenticating electronic records and other applications**  
N/A |
| **Public-private partnerships to engage industry, civil society, and academia in the promotion and enhancement of a cybersecurity culture**  
N/A | **Cybercrime Laws and Regulations**  
No cybercrime and cybersecurity law. There is a draft Telecommunications and ICT Bill. | **State Department to regulate and approve electronic commerce payment methods, only approved payment methods may be validly used in the Member State territory;**  
N/A |
| **Legislative and regulatory measures to identify the sectors regarded as sensitive for their national security and well-being of the economy (critical infrastructure), and measures to improve vigilance, security and management in such sectors**  
N/A | **State Department to regulate vulnerability and safety guarantee assessments of ICT product vendors including ensuring mandatory disclosures of vulnerabilities and the solutions to such vendors consumers**  
N/A | **Institutions with the statutory authority and legal capacity to respond to cyber security incidents, co-ordination and co-operation for (cybersecurity) restorative justice, forensic investigations, cybersecurity prosecution**  
N/A |
| **Institutions responsible for national and cross-border co-ordination of cybersecurity problems as well as global co-operation.**  
The Ministry of Telecommunications and New Technologies. is responsible for cyber security and cybercrime-related efforts in the DRC. | **Institutions that exchange information on cyber threats and vulnerability assessments such as the Computer Emergency Response Teams (CERTs)**  
A draft decree establishing a CERT has been submitted for examination and adoption by the Council of Ministers. | **Institutions responsible for national and cross-border co-ordination of cybersecurity problems as well as global co-operation.**  
The Ministry of Telecommunications and New Technologies. is responsible for cyber security and cybercrime-related efforts in the DRC. |
Disclaimer

This report was prepared independently by EndCode.

This report is based on a variety of inputs from multiple sources including official and private data sources such as public and governmental institutions, international organisations, academic research, news articles, sector reports and interviews with various stakeholders.

Accuracy of analysis and recommendations provided are dependent on the detail and accuracy of available and declared data. The information given herein is for informal guidance only and neither AUDA-NEPAD nor EndCode, nor any company or organisation stated within this paper makes any expressed or implied warranty, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, or process disclosed.

AUDA-NEPAD nor EndCode bear no responsibility for any use that may be made of this report. Should you have any queries about the content within this report, please contact AUDA-NEPAD.

About EndCode

EndCode is a specialist advisory firm - servicing local, regional and international organisations navigating technology laws and policies in Africa. EndCode believes that it can promote access to the benefits of technology and innovation on the continent by growing the body of insights available in technology law and policy areas. EndCode is distinguished by its multidisciplinary expertise in law, policy, research and advocacy in the technology environment.