LAW Nº 60/2018 OF 22/8/2018 ON PREVENTION AND PUNISHMENT OF CYBER CRIMES

TABLE OF CONTENTS

CHAPTER ONE: GENERAL PROVISIONS

Article One: Purpose of this Law

Article 2: Scope of this Law

Article 3: Definitions

CHAPTER II: PREVENTION OF CYBERCRIMES

Section One: Obligations of service provider

Article 4: General obligations of service provider

Article 5: Obligations of service provider in case of illegal use of computer, computer system or electronic communications 'network

Article 6: Obligations of a service provider in respect of illegal information or activities

Section 2: Protection of critical information infrastructure

Article 7: Protection of critical information infrastructure

CHAPTER III: INVESTIGATION OF CYBERCRIMES

Article 8: Obligation to collaborate with organs in charge of investigations

Article 9: Search and seizure

Article 10: Accessing or retrieving a copy of computer or a computer system data on the system after seizure

Article 11: Disclosure of data

Article 12: Preservation of computer or computer system

Article 13: Disclosure and collection of electronic traffic data

Article 14: Court order

Article 15: Authorization to use a forensic method

CHAPTER IV: OFFENCES AND PENALTIES

Section One: Offences against the confidentiality, integrity and availability of data and computer or computer system

Article 16: Unauthorized access to a computer or a computer system data

Article 17: Access to data with intent to commit an offence

Article 18: Unauthorized modification of computer or computer system data

Article 19: Interception of computer or computer system

Article 20: Damaging or denying access to a computer or computer system

Article 21: Unauthorized disclosure of access code

Article 22: Continuous fraudulent use of an automated or non-automated data processing system of another person

Article 23: Preventing or misguiding the running automated or non-automated data processing system

Article 24: Access to a computer or computer system data

Article 25: Unlawful manufacturing, selling, buying, use, import, distribution or possession of a computer or computer system or computer or computer system data

Article 26: Unauthorized reception or giving of access to a computer or computer system program or data

Article 27: Cyber-squatting

Article 28: Unlawful acts in respect of malware

Section 2: Offences related to digital signature and certification

Article 29: Misrepresentation and suppression

Article 30: False digital signature certificate

Article 31: Fraudulent use of digital signature

Section 3: Computer-related offences

Article 32: Computer- or computer system-related forgery

Article 33: Changing computer or computer system equipment identity

Section 4: Offences related to the content of computer and computer system

Article 34: Publication of pornographic images through a computer or a computer system

Article 35: Cyber-stalking

Article 36: Phishing

Article 37: Spamming

Article 38: Publishing indecent information in electronic form

Article 39: Publication of rumours

Article 40: Impersonation

Section 5: Offences related to terrorism, trafficking in persons or narcotics committed using a computer or a computer system

Article 41: Creation or publication of a site for terrorist groups

Article 42: Creation or publication of a site for the purpose of trafficking in persons

Article 43: Creation or publication of a site for the purpose of trafficking or distributing drugs or narcotics

Section 6: Cyber offences committed by service providers

Article 44: Disclosure of data made available to third party

Article 45: Provision of access to a computer or computer system or cause them to send or use electronic content on

another person's computer or computer system

Article 46: Refusal to remove or disable access to illegal information stored

Article 47: Non reporting of cyber threats incident

Article 48: Offences related to stored information

Article 49: Illegal search results

Article 50: Failure to take action on take-down notification

Section 7: Common provisions to all offences

Article 51: Penalties imposed on a business entity having committed an offence

Article 52: Additional penalties

CHAPTER V: MISCELLANEOUS AND FINAL PROVISIONS

Article 53: Regulations on cyber security

Article 54: Drafting, consideration and adoption of this Law

Article 55: Repealing provision

Article 56: Commencement

LAW Nº 60/2018 OF 22/8/2018 ON PREVENTION AND PUNISHMENT OF CYBER CRIMES

We, KAGAME Paul,
President of the Republic;

THE PARLIAMENT HAS ADOPTED AND WE SANCTION, PROMULGATE THE FOLLOWING LAW AND ORDER IT BE PUBLISHED IN THE OFFICIAL GAZETTE OF THE REPUBLIC OF RWANDA

THE PARLIAMENT:

The Chamber of Deputies, in its session of 31 May 2018;

Pursuant to the Constitution of the Republic of Rwanda of 2003 revised in 2015, especially in Articles 29, 64, 69, 70, 88, 90, 91, 106, 112, 120 and 176;

ADOPTS:

CHAPTER ONE: GENERAL PROVISIONS

Article One: Purpose of this Law

This Law aims at preventing and punishing cyber-crimes.

Article 2: Scope of this Law

This Law applies to all cyber-crimes which are committed in Rwanda or outside Rwanda if such offences have produced effect in Rwanda.

Article 3: Definitions

As used in this Law, the following terms have the meanings ascribed to them below:

1° **computer data:** any representation of facts, information or concepts in a form suitable for processing in a computer system or a computer including a program suitable to cause a computer or a computer system to perform a function, electronic documents or electronic data

messages whether stored in local computer systems or online;

2° **critical information infrastructure:** virtual and physical information systems that provide services to the citizens and serve as a backbone of development of the national economic, social and security life;

3° **search engine:** a software system that is designed to search for or identify information that corresponds to key words on the World Wide Web;

4° **communication:** the transmission of information through Information Communication Technology media;

5° **interception:** listening to, recording, monitoring or surveillance of the content of communications, including procuring of the content of data, either directly, through access and use of a computer or a computer system or indirectly, through the use of electronic eavesdropping or tapping devices, when communication is occurring;

6° **computer:** an electronic, magnetic, optical, electrochemical or other data processing or communications device or grouping of such devices, capable of performing logical, arithmetic, routing or storage functions and which includes any storage facility or equipment or communications facility or equipment directly related to or operating in conjunction with such device. It includes any type of computer device including devices with data processing capabilities like mobile phones, smart phones, computer networks and other devices connected to the internet;

7° **computer program:** a set of instructions executed by the computer to achieve intended results;

8° **cyber security:** protection of computer systems from theft of, damage to their hardware, software or information as well as from disruption or misdirection of the services they provide;

9° **site:** a place where information is available on an information network through a specific address;

10° **information system:** all software, tools and equipment for the production, storage or processing of data or information or management of data or information;

11° **computer system:** an electronic device or combination of electronic devices composed of hardware or software, including input and output devices with data processing and storage capabilities;

12° **service provider:** a public or private entity or an individual that provides service to users by means of a computer or computer system or any other entity that processes or stores computer data on behalf of such communication service or users of such service.

CHAPTER II: PREVENTION OF CYBERCRIMES

Section One: Obligations of service provider

Article 4: General obligations of service provider

An electronic communications service provider must:

1° take reasonable steps to inform its clients of cybercrimes trends which affect or may affect them;

2° establish procedures for its clients to report cybercrimes;

3° inform its clients of measures they may take in order to safeguard themselves against cybercrimes;

4° disclose abuses to the concerned victim and to the cyber security organ that infractions are committed.

Article 5: Obligations of service provider in case of illegal use of computer, computer system or electronic communications network

Any service provider who is aware or informed that its computer or computer system or electronic communication network is being used to commit an offence provided for in this Law must:

1º immediately report what is being committed to the authority in charge of cyber security;

2º preserve any information which may be of assistance in investigating the offence, including particularly information which shows the communication's origin, destination, route, time, date, size, duration and the type of the underlying services.

Article 6: Obligations of a service provider in respect of illegal information or activities

Any service provider who has been informed by security organs or cyber-security organ of

illegal or harmful information or activity, must:

1º remove such information in the computer or computer system;

2º suspend or terminate services in respect of that illegal or harmful information or activity;

3º facilitate organs in charge of investigations or prosecution, at their request, with necessary information.

Section 2: Protection of critical information infrastructure

Article 7: Protection of critical information infrastructure

A Presidential Order determines modalities for the protection of critical information infrastructure.

This Order also prescribes minimum standards, guidelines, rules or procedure in respect of:

1º the protection and preservation of critical information infrastructure;

2º the general management of critical information infrastructure;

3º access to, transfer and control of data in critical information infrastructure;

4º infrastructural or procedural rules and requirements for securing the integrity and authenticity of data or information contained in critical information infrastructure;

5º the storage or archiving of data or information designated as critical information infrastructure;

6º data recovery plan in the event of disaster, breach or loss of the critical information infrastructure or part of it;

7º audit and inspect any critical information infrastructure at any time to ensure compliance with the provisions of this Law;

8º any other matter required for the adequate protection, management and control of data and other resources in critical information infrastructure.

CHAPTER III: INVESTIGATION OF CYBERCRIMES

Article 8: Obligation to collaborate with organs in charge of investigations

Without prejudice to other laws, a person who is required to cooperate with the organ in charge of investigations or prosecution must in particular:

1° respond to any inquiry about the investigation;

2° comply with any lawful directions including disclosing access code to a computer system;

3° disclose all data required for the purposes of investigation and of prosecution of an offence.

Article 9: Search and seizure

Without prejudice to other laws, the organ in charge of prosecution may, in case there exists reasonable grounds to suspect or believe that a computer or a computer system may be used as a proof of an offence or is acquired by any person as a result of an offence, issue an order authorizing to:

1° enter into any premise and search or seize a computer or a computer system;

2° secure the computer or computer system data accessed;

3° extend the search and access a computer or any another computer system where the data being sought is stored.

Where a computer or a computer system is relocated or rendered inaccessible following a search or a seizure, the person who conducted the seizure makes a statement indicating a list of items seized or rendered inaccessible and time of seizure. A copy of the list is issued to the person who has

control over the computer or computer system.

Article 10: Accessing or retrieving a copy of computer or a computer system data on the system after seizure

A person who has custody or control over the computer system may request organ in charge of prosecution, the permission to access or copy computer data on the computer or computer system after seizure.

The prosecution authority may refuse to issue a permission mentioned in Paragraph One of this Article, if it has reasonable grounds to believe that giving the access or providing the copy may constitute a prejudice against an investigation in connection with the search, any other ongoing investigation or any criminal proceeding pending or that may be instituted in relation to any investigation.

Article 11: Disclosure of data

If the disclosure of data is required for the purposes of a criminal investigation or the prosecution of an offence, the prosecution authority may issue an order to a person in

possession of such data compelling him/her to disclose such data.

If a material to which an investigation consists of data stored in a computer or computer system, the request is considered to require the person to produce or give access to that data in a form in which it can be taken away and in which it is visible and legible.

Article 12: Preservation of computer or computer system

If there are reasonable grounds to believe that a computer or computer system that is required for the purpose of investigation is likely to be lost or modified, the prosecution authority may issue an order requiring the person in control of such a computer or computer system to preserve it for a period not exceeding thirty (30) days. Such period may be extended once if considered necessary.

Article 13: Disclosure and collection of electronic traffic data

In case of any reasonable grounds that an electronic traffic data is required for the purpose of investigation, the organ in charge of prosecution may issue an order to any person in possession of the electronic traffic data for:

1° disclosure, collection or recording of the electronic traffic or log data associated with a specified communication during a specified period;

2° permitting and assisting the organ in charge of investigations to collect or record that data.

Article 14: Court order

If the person holding data or the evidential value of data is not willing to cooperate in disclosure or preservation of data, the prosecution authority may seek a court order compelling such person to do so.

Article 15: Authorization to use a forensic method

If the prosecution authority has reasonable grounds to believe that essential evidence cannot be collected without the use of scientific method, it may request the court to order for the use of a forensic method. The order is valid for a period of thirty (30) days. The court may, upon application made by organ in charge of prosecution, extend that period for a further period of thirty (30) days or to such other period as it considers necessary.

The application under Paragraph One of this Article must contain the following:

1° the name and full address of the suspect;

2° a description of the targeted computer or computer system;

3° a description of the intended measures, purpose, extent and duration of the utilization of computer or computer system.

A modification made to the computer or computer system of the suspect is limited to the investigation, and any change made during the investigation is restored into the computer or computer system after the completion of the investigation.

During the investigation, the prosecution authority must log:

1° the technical means used and time and date of the application;

2° the identification of the computer system and details of the modification undertaken within the investigation;

3° any information obtained.

The information obtained under this Article must be protected from any modification, unauthorized deletion or access.

The court may, in addition to the order granted under Paragraph One of this Article, order the service provider to support the installation process of the forensic tool.

CHAPTER IV: OFFENCES AND PENALTIES

Section One: Offences against the confidentiality, integrity and availability of data and computer or computer system

Article 16: Unauthorized access to a computer or a computer system data

Any person who intentionally and unlawfully gets access to computer or computer system data and he/she:

1° does not have consent from any person who is so entitled;

2° is not entitled to control and access to the computer or computer system data;

3° accesses another person's computer system without authorization, in order to know recorded or transmitted data, by all means and regardless of the location;

commits an offence.

Upon conviction of one of the offences referred to in Paragraph One of this Article, he/she is liable to imprisonment for a term of not less than six (6) months and not more than two (2) years and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than two million Rwandan francs (FRW 2,000,000).

Article 17: Access to data with intent to commit an offence

Any person who, with intent to commit an offence, causes a computer system or a computer to perform any function for the purpose of securing access to any program or data held in any computer system, commits an offence.

Upon conviction, he/she is liable to imprisonment for a term of not less than one (1) year and not more than two (2) years and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than three million Rwandan francs (FRW 3,000,000).

Article 18: Unauthorized modification of computer or computer system data

A person who knowingly commits an act which causes unauthorised modification of data held in a computer or computer system, commits an offence.

Upon conviction, he/she liable to imprisonment for a term of not less than one (1) year and not more than two (2) years and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than three million Rwandan francs (FRW 3,000,000).

Article 19: Interception of computer or computer system

Any person who, knowingly and by any means, without authorisation by law, intercepts or causes to be intercepted, directly or indirectly, any function or any data for the purpose of obtaining any computer or computer system service, any function or any data held in a computer, commits an offence.

Upon conviction, he/she is liable to imprisonment for a term of not less than one (1) year and not more than two (2) years and

a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than three million Rwandan francs (FRW 3,000,000).

If the interception under Paragraph One of this Article relates to State secrets, or national security, the offender is liable to imprisonment for a term of not less than two (2) years and not more than five (5) years and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than two million Rwandan francs (FRW 2,000,000).

Article 20: Damaging or denying access to a computer or computer system

Any person who, without lawful authority or lawful excuse, commits an act which causes directly or indirectly a degradation, failure, interruption or obstruction of the operation of a computer or computer system, or a denial of access to or damage of any program or data stored in the computer system, commits an offence.

Upon conviction, he/she is liable to imprisonment for a term of not less than three (3) years and not more than five (5) years and

a fine of not less than three million Rwandan francs (FRW 3,000,000) and not more than five million Rwandan francs (FRW 5,000,000).

Article 21: Unauthorized disclosure of access code

Any person who:

1º knowingly, discloses any access code or any other means of gaining access to a program or data held in a computer or computer system, targets a wrongful gain;

2º performs any unlawful act knowing that such act is likely to disclose access code or any other means of gaining access to a computer system;

commits an offence.

When convicted of any of the offences referred to in Paragraph One, he/she is liable to imprisonment for a term of not less than one (1) year and not more than two (2) years and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not

more than three million Rwandan francs (FRW 3,000,000).

Article 22: Continuous fraudulent use of an automated or non-automated data processing system of another person

Any person who, in any way whatsoever, fraudulently uses continuously another person's automated or non-automated data processing system or similar systems with intent to find out electronically stored or transmitted data, commits an offence.

Upon conviction, he/she is liable to imprisonment for a term of not less than two (2) years and not more than five (5) years and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than three million Rwandan francs (3,000,000 FRW).

If the acts mentioned under Paragraph One of this Article result in deletion, modification, alteration or insertion of recorded or transmitted data, the offender is liable to imprisonment for a term of not less than five (5) years and not more than seven (7) years and a fine of not less than four million Rwandan francs (FRW 4,000,000) and not

more than six million Rwandan francs (FRW 6,000,000).

Article 23: Preventing or misguiding the running automated or non-automated data processing system

Any person who intentionally prevents or misguides the running of automated or non-automated data processing system or other similar system of another person commits an offence.

Upon conviction, he/she is liable to imprisonment for a term of not less than one (1) year and not more than two (2) years and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than three (3) million Rwandan francs (FRW 3,000,000).

If the automated or non-automated data processing system or any similar system belongs to a security state organ, the offender is liable to imprisonment for a term of not less than five (5) years and not more than seven (7) years and a fine of not less than three million Rwandan francs (FRW 3,000,000) and not more than five million Rwandan francs (FRW 5,000,000).

If the automated or non-automated data processing system or any similar system is qualified as critical national information infrastructure, the offender is liable to imprisonment for a term of not less than ten (10) years and not more than fifteen (15) years and a fine of not less than ten million Rwandan francs (FRW 10,000,000) and not more than thirty million Rwandan francs (FRW 30,000,000).

Article 24: Access to a computer or computer system data

Any person who alters, hinders or interferes with the functioning of a computer, a computer system or a computer network by putting, transmitting, deleting, deteriorating, altering or suppressing of computer or computer system data, electronic document, or electronic data message, without authorization to do so, including the introduction or transmission of malicious code, commits an offence.

Upon conviction, he/she is liable to imprisonment for a term of not less than two (2) years and not more than five (5) years and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than two million Rwandan francs (FRW 2,000,000).

If the computer data belongs to a security state organ, the offender is liable to imprisonment for a term of not less than five (5) years and not more than seven (7) years and a fine of not less than three million Rwandan francs (FRW 3,000,000) and not more than five million Rwandan francs (FRW 5,000,000).

If the computer or computer system data is stored in critical national information infrastructure, he/she is liable to imprisonment for a term of not less than ten (10) years and not more than fifteen (15) years and a fine of not less than ten million Rwandan francs (FRW 10,000,000) and not more than thirty million Rwandan francs (FRW 30,000,000).

Article 25: Unlawful manufacturing, selling, buying, use, import, distribution or possession of a computer or computer system or computer or computer system data

Any person who, knowingly manufactures, sells, buys, uses, imports, distributes or possesses a computer or computer system or otherwise makes available the data or programme or computer system or possesses them, with intention to use a computer or computer system or computer data personally or make them available to another person for an unlawful purpose commits an offence.

Upon conviction, he/she is liable to imprisonment for a term of not less than two (2) years and not more than five (5) years and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than two million Rwandan francs (FRW 2,000,000).

Article 26: Unauthorized reception or giving of access to a computer or computer system program or data

Any person who:

1° receives and uses or provides access to any program or data held in a computer or computer system without authorisation;

2° is authorized to receive or to have access to any program or data held in a computer or computer system, receives and uses them from another person knowing that the other person has obtained that program or data through unauthorized means;

3° has obtained any program or data held in a computer or computer system through authorized means and gives that program or data to another person who is not authorized to receive or have access to that program or data;

commits an offence.

When convicted of any of the offences referred to in Paragraph One of this Article, he/she is liable to imprisonment for a term of not less than six (6) months and not more than two (2) years and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than two million Rwandan francs (FRW 2,000,000).

Article 27: Cyber-squatting

Any person who acquires a domain name over the internet in bad faith to profit, mislead, destroy reputation, or deprive others from registering the same, if such a domain name is:

1° similar, identical, or confusingly similar to an existing registered trademark;

2° identical or in any way similar with the name of a person other than the registrant, in case of a personal name;

3° acquired without authorization or with intellectual property interests in it;

commits an offence.

Upon conviction, he/she is liable to imprisonment for a term of not less than one (1) year and not more than two (2) years and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than three million Rwandan francs (FRW 3,000,000).

Article 28: Unlawful acts in respect of malware

Any person who intentionally assembles, obtains, sells, purchases, possesses, makes available, advertises or unlawfully and intentionally uses malware for the purposes of causing damage particularly to:

1° data;

2° a computer system;

3° a computer network;

4° a database;

5° an electronic communications network;

6° a critical information infrastructure;

commits an offence.

When convicted of any of the offences referred to in Paragraph One of this Article, he/she is liable to imprisonment for a term of not less than six (6) months and not more than two (2) years and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than two million Rwandan francs (FRW 2,000,000).

Section 2: Offences related to digital signature and certification

Article 29: Misrepresentation and suppression

Any person who intentionally makes any misrepresentation to, or suppresses any material fact from or to the controller or the certifying authority for obtaining any license or digital signature certificate, commits an offence.

Upon conviction, he/she is liable to imprisonment for a term of not less than two (2) years and not more than five (5) years and a fine of not less than three million Rwandan francs (FRW 3,000,000) and not more than five million Rwandan francs (FRW 5,000,000).

Article 30: False digital signature certificate

Any person who publishes a digital signature certificate or otherwise make it available to any other person with the knowledge that:

1° the certifying authority listed in the certificate has not issued it;

2° the subscriber listed in the certificate has not accepted it;

3° the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation;

commits an offence.

Upon conviction, he/she is liable to imprisonment for a term of not less than five (5) years and not more than seven (7) years and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than three million Rwandan francs (FRW 3,000,000).

Article 31: Fraudulent use of digital signature

Any person who knowingly creates, publishes or otherwise makes available a digital signature certificate for any fraudulent or unlawful purpose, commits an offence.

Upon conviction, he/she is liable to imprisonment for a term of not less than five (5) years and not less than seven (7) years and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than three million Rwandan francs (FRW 3,000,000).

Section 3: Computer-related offences

Article 32: Computer- or computer system-related forgery

Any person who:

1° inputs, alters or deletes any computer or computer system data without authorization resulting in inauthentic data with the intent that it be considered or acted upon as if it were authentic;

2° knowingly uses computer data which is the product of computer- or computer system-related forgery;

commits an offence.

When convicted of one of the offences referred to in Paragraph one of this Article, he/she is liable to imprisonment for a term of not less than five (5) years and not more than seven (7) years and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than two million Rwandan francs (FRW 2,000,000).

Article 33: Changing computer or computer system equipment identity

Any person who, knowingly or wilfully, while not being a manufacturer of a computer system or an authorised agent of the manufacturer, changes computer system equipment identity or the process of accessing to it, commits an offence.

Upon conviction, he/she is liable to imprisonment for a term of not less than six (6) months and not more than two (2) years and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than two million Rwandan francs (FRW 2,000,000).

Section 4: Offences related to the content of computer and computer system

Article 34: Publication of pornographic images through a computer or a computer system

Any person who:

1° publishes or causes to be published pornography through a computer system or through any other means of information and communication technology;

2° proposes, grooms or solicits, through a computer or a computer system or any network, to meet a child for the purpose of engaging in sexual activities with the child;

commits an offence.

Upon conviction, he/she is liable to imprisonment for a term of not less than three (3) years and not more than five (5) years and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than

three million Rwandan francs (FRW 3,000,000).

If the offender publishes child pornography through a computer or a computer system or makes available or facilitates the access to child pornography through a computer or a computer system, he/she is liable to imprisonment for a term of not less than five (5) years and not more than seven (7) years and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than three million Rwandan francs (FRW 3,000,000).

Article 35: Cyber-stalking

Any person who, intentionally, uses a computer or a computer system to harass or threaten with the intent to place another person in distress or fear through one of the following acts when:

1° he/she displays, distributes or publishes indecent documents, sounds, pictures or videos;

2° in bad faith, he/she takes pictures, videos or sounds of any person without his/her consent or knowledge;

3° he/she displays or distributes information in a manner that substantially increases the risk of harm or violence to any other person;

commits an offence.

Upon conviction, he/she is liable to imprisonment for a term of not less than six (6) months and not more than two (2) years and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than two million Rwandan francs (FRW 2,000,000).

The prosecution of offenses under this Article are instituted only upon complaint of the offended person.

Article 36: Phishing

A person who establishes and uses a website or sends an electronic message

using a computer or a computer system in order to have access to confidential information from a visitor of the website or recipient of the message with intent to use them for unlawful purposes, especially for the purpose of stealing money or obtaining access to a computer or a computer system, commits an offence.

Upon conviction, he/she is liable to imprisonment for a term of not less than one (1) year and not more than two (2) years and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than three million Rwandan francs (FRW 3,000,000).

Article 37: Spamming

Any person who, intentionally and without authorisation from a competent organ:

1° sends unsolicited messages repeatedly or to a large number of persons by use of a computer or a computer system;

2° after receiving a message, uses a computer or a computer system to retransmit such a message to many

persons or retransmit it several times to a person who doesn't need it;

commits an offence.

Upon conviction, he/she is liable to imprisonment for a term of not less than three (3) months and not more than six (6) months and a fine of not less than three hundred thousand Rwandan francs (FRW 300,000) and not more than five hundred thousand Rwandan francs (FRW 500,000).

The prosecution of offenses under this Article are instituted only upon complaint of the offended person.

Article 38: Publishing indecent information in electronic form

Any person who publishes, transmits or causes to be published any indecent message using a computer or a computer system, commits an offence.

Upon conviction, he/she is liable to imprisonment for a term of not less than six (6) months and not more than two (2) years and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not

more than two million Rwandan francs (FRW 2,000,000).

When the indecent message referred to in Paragraph one of this Article is not true or is directed against a child, the offender is liable to imprisonment for a term of not less than three (3) years and not more than five (5) years and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than three million Rwandan francs (FRW 3,000,000).

Article 39: Publication of rumours

Any person who, knowingly and through a computer or a computer system, publishes rumours that may incite fear, insurrection or violence amongst the population or that may make a person lose their credibility, commits an offence.

Upon conviction, he/she is liable to imprisonment for a term of not less than three (3) years and not more than five (5) years and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than three million Rwandan francs (FRW 3,000,000).

Article 40: Impersonation

Any person who intentionally uses somebody identity over the internet in bad faith to profit, mislead or destroy reputation or otherwise, if such identity is similar, undistinguishable, or confusingly similar to an existing name or description that belongs to another person or organ, commits an offence.

Upon conviction, he/she is liable to imprisonment for a term of not less than three (3) years and not more than five (5) years and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than three million Rwandan francs (FRW 3,000,000).

Section 5: Offences related to terrorism, trafficking in persons or narcotics committed using a computer or a computer system

Article 41: Creation or publication of a site for terrorist groups

Any person who establishes, publishes or uses a site of a terrorist group using Internet, a computer or a computer system in order to facilitate communication by its leadership

or its members, raise its funds or disseminate its ideas or knowledge of how it operates, commits an offence.

Upon conviction, he/she is liable to imprisonment for a term of not less than fifteen (15) years and not more than twenty (20) years and a fine of not less than twenty million Rwandan francs (FRW 20,000,000) and not more than fifty million Rwandan francs (FRW 50,000,000).

Article 42: Creation or publication of a site for the purpose of trafficking in persons

Any person who establishes or publishes a site on an information network, computer hardware or computer system for the purposes of trafficking in human beings or facilitating such a transaction, commits an offence.

Upon conviction, he/she is liable to imprisonment for a term of not less than ten (10) years and not more than fifteen (15) years and a fine of not less than ten million Rwandan francs (FRW 10,000,000) and not more than fifteen million Rwandan francs (FRW 15,000,000).

Article 43: Creation or publication of a site for the purpose of trafficking or distributing drugs or narcotics

Any person who creates or publishes a site on an information network, computer hardware or computer system act for the purposes of trafficking in or distributing drugs or narcotics or facilitating such a transaction commits an offence.

Upon conviction, he/she is liable to imprisonment for a term of not less than seven (7) years and not more than ten (10) years and a fine of not less than seven million Rwandan francs (FRW 7,000,000) and not more than ten million Rwandan francs (FRW 10,000,000).

Section 6: Cyber offences committed by service providers

Article 44: Disclosure of data made available to third party

Any service provider who does not exercise due care and skill to prevent the disclosure of computer data made available to third party, commits an offence.

Upon conviction, he/she is liable to a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than three million Rwandan francs (FRW 3,000,000).

Article 45: Provision of access to a computer or computer system or cause them to send or use electronic content on another person's computer or computer system

Any service provider who causes access to, transmission or publication of computer or computer system data or causes the use of a computer program or computer system of another person without authorization, commits an offence, if he/she:

1° initiated the transmission of data or programs;

2° selected the receiver of the transmission of data or programs;

3° selected or modified the information contained in the transmission.

Upon conviction, he/she is liable to a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than three million Rwandan francs (FRW 3,000,000).

Article 46: Refusal to remove or disable access to illegal information stored

Any hyperlink provider or hosting provider who does not remove or disable access to the information linked or stored at the request of a user of the service, infringes the rights of the recipient or of a third party after receiving an order from competent organ to disable access to or remove specific illegal information stored, or who does not inform the organ in charge of investigations or

prosecution upon becoming aware of illegal information stored, commits an offence.

Upon conviction, he/she is liable to imprisonment for a term of not less than two (2) years and not more than five (5) years and a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than three million Rwandan francs (FRW 3,000,000).

Article 47: Non reporting of cyber threats incident

Any service provider who knowingly fails to report cyber threats incident, commits an offence.

Upon conviction, he/she is liable to imprisonment for a term of not less than one (1) year and not more than two (2) years and a fine of not less than three million Rwandan francs (FRW 3,000,000) and not more than five million Rwandan francs (FRW 5,000,000).

If the failure to report referred to in paragraph One of this Article has caused a computer or computer system to be exposed to dangerous consequences resulting in cyber security threats or incident, fraud, dishonesty

or caused theft and loss of data, the offender is liable to imprisonment for a term of not less than five (5) years and not more than seven (7) years and a fine of not less than thirty million Rwandan francs (FRW 30,000,000) and not more than fifty million Rwandan francs (FRW 50,000,000).

If the offence under this Article is committed by a person other than a service provider, he/she is liable to imprisonment for a term of not less than eight (8) days and not more than two (2) months and a fine of not less than three hundred thousand Rwandan francs (FRW 300,000) and not more than five hundred thousand Rwandan francs (FRW 500,000).

Article 48: Offences related to stored information

Any service provider or who stores information data if he/she:

1° modifies the information;

2° does not comply with conditions of access to the information;

3° does not comply with rules regarding the updating of the information;

4° interferes with the lawful use of the technology widely recognized and used in the cyberspace, to obtain data on the use of the information;

5° does not immediately remove or disable access to the information he/she has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that an organ in charge of prosecution or court has ordered such removal or disablement.

commits an offence.

When convicted of one of the offences referred to in Paragraph one of this Article, he/she is liable to a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than three million Rwandan francs (FRW 3,000,000).

Article 49: Illegal search results

A search engine provider who, for search results, initiates the transmission or selects the receiver of the transmission but modifies

the information contained in the transmission, commits an offence.

Upon conviction, he/she is liable to a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than three million Rwandan francs (FRW 3,000,000).

Article 50: Failure to take action on take-down notification

Any service provider who fails to take an action on take-down done, commits an offence, if he/she was notified of any:

1° data or activity infringing the rights of the recipient or of a third party;

2° unlawful material or activity;

Upon conviction, he/she is liable to a fine of not less than one million Rwandan francs (FRW 1,000,000) and not more than three million Rwandan francs (FRW 3,000,000).

Section 7: Common provisions to all offences

Article 51: Penalties imposed on a business entity having committed an offence

Without prejudice to the provisions of this Law, a business entity that commits one of the offences provided under this Law, when convicted, it is liable to a fine equal to thirty percent (30%) and not more than seventy percent (70%) of the profits received in the accounting period of the year in which the offence was committed.

Article 52: Additional penalties

Except penalties provided for under this Law, the competent court may, in all cases, order the confiscation of a computer or a computer system, software or media used in the commission of any of the offences provided for in this Law and the proceeds gained.

The court may also, permanently or temporary for the period that it considers appropriate, order the closure of the premise or corporate body in which any of the offences provided for in this Law has been committed, if the offence was committed

with the knowledge of their owner or management.

CHAPTER V: MISCELLANEOUS AND FINAL PROVISIONS

Article 53: Regulations on cyber security

Subject to the provisions of this Law, an organ in charge of cyber security puts in place a regulation to prevent and fight cybercrimes.

Article 54: Drafting, consideration and adoption of this Law

This Law was drafted in English, considered and adopted in Ikinyarwanda.

Article 55: Repealing provision

All prior legal provisions contrary to this Law are repealed.

Article 56: Commencement

This Law comes into force on the date of its publication in the Official Gazette of the Republic of Rwanda.

Kigali, on 22/8/2018

(sé)
KAGAME Paul
President of the Republic

(sé)
Dr. NGIRENTE Edouard
Prime Minister

Seen and sealed with the Seal of the Republic:

(sé)
BUSINGYE Johnston
Minister of Justice/ Attorney General