Translated from French

LAW ON CYBERCRIME

Explanatory statement

The development of information and communication technologies (ICTs) constitutes a major turning-point in human civilization in this early part of the twenty-first century.

The Internet today is the perfect illustration of the possibilities afforded by information and communication technologies, which, through the services it offers (digital technologies for the communication, transmission and archiving of information, etc.), remains a powerful means of communication used by millions of people.

In fact, the transition from analog to digital heralds the arrival of a new age and of a genuine "digital revolution" that has profoundly changed the face of traditional society, which has very quickly been transformed into an information society where the possession of information has become a coveted strategic asset.

However, while the permanent interconnectedness of computer networks offers States a major opportunity to exploit the potential of information and communication technologies to promote the development goals set out in the Millennium Declaration and the development of commercial transactions and good governance, the digital environment offered by information and communication technologies, particularly the Internet, is increasingly a place where reprehensible acts of all kinds are committed, damaging the interests both of private individuals and of the general public.

The emergence of this new criminal phenomenon known as cybercrime, which is transnational, intangible and volatile in nature and whose perpetrators are anonymous, has contributed to the blurring of reference points in the penal system, whose traditional and ongoing responses, conceived and developed for a tangible and nationally based environment, have quickly proved to be inappropriate and unsuitable for dealing with the new reality of the digital era.

A review of Senegalese criminal legislation has thus shown that it is ill-equipped to deal with the specific nature of digital crime in terms of both substantive and procedural law.

With regard to substantive criminal law, the analysis of Senegalese legislation has revealed legal situations in which computer systems, computerized data and computer networks are targeted by cybercrime. It has also highlighted other cases in which the law has been found to be inadequate, where information and communication technologies, in particular the Internet, are used as a means to commit wrongdoing.

In criminal procedural law, the regulations that should govern all stages of cybercrime proceedings (investigation, prosecution, examination proceedings and judgment) have been found to be inadequate.

Computer-related crime concerns any offense involving the use of information and communication technologies. In this regard, the concepts of cybercrime, computer-related crime, cybercriminal, computer-related offenses, hi-tech crime, etc., have the same meaning.

Therefore, for obvious crime-policy reasons, a cyberstrategy for dealing with cybercrime needs to be developed in Senegal by adapting the penal system, in particular updating traditional definitions of criminal offenses and adjusting traditional procedural instruments in the light of information and communication technologies.

The present draft law consists of two parts:

(1) part one, relating to substantive criminal law, consists of three titles dealing with the establishment of offenses specific to information and communication technologies and the adaptation of certain definitions of offenses and certain penalties to the context of information and communication technologies;

(2) part two, relating to criminal procedural law, consists of two titles concerning, on the one hand, adjustments to traditional procedures in the light of information and communication technologies and, on the other, the adoption of a procedure specific to offenses relating to personal data.

This is the subject of the present draft law.

REPUBLIC OF SENEGAL
One People – One Goal – One Faith

Law No. 2008-11 on Cybercrime

The National Assembly adopted, at its session of Friday, November 30, 2007,
The Senate adopted, at its session of Tuesday, January 15, 2008,
And the President of the Republic hereby promulgates the Law set out below:

Article 1
Title III, "Offenses relating to information and communication technologies", consisting of Articles 431-7 to 431-65 set out below, shall be inserted after Article 431-6 of the Penal Code.

TITLE III: OFFENSES RELATING TO INFORMATION AND COMMUNICATION TECHNOLOGIES

INTRODUCTORY CHAPTER: TERMINOLOGY

Article 431-7
Under the present Law:

1. *electronic communication* means any making available to the public or a section of the public of signs, signals, writings, images, sounds or messages of any kind through an electronic or magnetic communication process;

2. *computerized data* means any representation of facts, information or concepts in a form suitable for processing in a computer system;

3. *racist or xenophobic in relation to information and communication technologies* means any piece of writing, image or other representation of ideas or theories that advocates or encourages hatred, discrimination or violence against a person or a group of persons on grounds of race, color, ancestry or national or ethnic origin, or religion insofar as it is used as the pretext for hatred, discrimination or violence on one or other of the grounds mentioned, or that incites such acts;

4. *minor* means any person below the age of 18 years, as defined in the United Nations Convention on the Rights of the Child;

5. *child pornography* means any material, irrespective of its nature and form, that visually depicts a minor engaged in a sexually explicit act or realistic images representing a minor engaged in sexually explicit conduct;

6. *computer system* means any device, whether isolated or not, or any group of interconnected devices which, in whole or in part, performs automatic processing of data pursuant to a program.

CHAPTER I: INTERFERENCE WITH COMPUTER SYSTEMS

SECTION I: INTERFERENCE WITH THE CONFIDENTIALITY OF COMPUTER SYSTEMS

Article 431-8
Anyone who fraudulently accesses or attempts to access all or part of a computer system shall be punished with a prison term of six (6) months to three (3) years and/or a fine of 1,000,000 to 10,000,000 francs.

Anyone who fraudulently obtains or attempts to obtain any advantage for himself or for another person by accessing a computer system shall be punished with the same penalties.

Article 431-9
Anyone who fraudulently maintains or attempts to maintain a presence in all or part of a computer system shall be punished with a prison term of six (6) months to three (3) years and/or a fine of 1,000,000 to 10,000,000 francs.

SECTION II: INTERFERENCE WITH THE INTEGRITY OF COMPUTER SYSTEMS

Article 431-10
Anyone who obstructs or distorts or attempts to obstruct or distort the operation of a computer system shall be punished with a prison term of one (1) to five (5) years and a fine of 5,000,000 to 10,000,000 francs.

SECTION III: INTERFERENCE WITH THE AVAILABILITY OF COMPUTER SYSTEMS

Article 431-11
Anyone who fraudulently accesses or attempts to access or fraudulently inputs or attempts to input data into a computer system shall be punished with a prison term of one (1) to five (5) and/or a fine of 5,000,000 to 10,000,000 francs.

CHAPTER II: INTERFERENCE WITH COMPUTERIZED DATA

SECTION I: GENERAL INTERFERENCE WITH COMPUTERIZED DATA

Article 431-12
Anyone who fraudulently intercepts or attempts to intercept, by technical means, non-public transmissions of computerized data to, from or within a computer system shall be punished with a prison term of one (1) to five (5) years and/or a fine of 5,000,000 to 10,000,000 francs.

Article 431-13
Anyone who fraudulently damages or attempts to damage, deletes or attempts to delete, tampers with or attempts to tamper with, alters or attempts to alter, modifies or attempts to modify computerized data shall be punished with a prison term of one (1) to five (5) years and/or a fine of 5,000,000 to 10,000,000 francs.

Article 431-14
Anyone who produces or manufactures a set of digitized data through the fraudulent inputting, deletion or suppression of computerized data that have been stored, processed or transmitted by a computer system, resulting in forged data, with the intent that they be considered or acted upon for legal purposes as if they were original, shall be punished with a prison term of one (1) to five (5) years and/or a fine of 5,000,000 to 10,000,000 francs.

Article 431-15
Anyone who knowingly uses or attempts to use data obtained under the conditions set out in Article 431-14 of the present Law shall be punished with the same penalties.

Article 431-16
Anyone who fraudulently obtains any advantage for himself or for another person by inputting, altering, deleting or suppressing computerized data or by any form of interference with the operation of a computer system shall be punished with a prison term of one (1) to five (5) years and/or a fine of 5,000,000 to 10,000,000 francs.

SECTION II: SPECIFIC INTERFERENCE WITH THE RIGHTS OF THE INDIVIDUAL RELATING TO THE PROCESSING OF PERSONAL DATA

Article 431-17
Anyone who, even through negligence, processes or arranges the processing of personal data without having complied with the formalities set out in the Law on Personal Data prior to using such data shall be punished with a prison term of one (1) to seven (7) years and/or a fine of 500,000 to 10,000,000 francs.

Article 431-18
Anyone who, even through negligence, carries out or arranges processing that is subject to the measure provided for in Article 30, subparagraph 1, of the Law on Personal Data shall be punished with a prison term of one (1) to seven (7) years and/or a fine of 500,000 to 10,000,000 francs or both.

Article 431-19
Where personal data are processed or the processing thereof is arranged under the conditions set out in Article 19 of the aforementioned Law on Personal Data, anyone who fails to comply, including through negligence, with the simplification or exemption regulations established for that purpose by the Commission on Personal Data shall be punished with a prison term of one (1) to seven (7) years and/or a fine of 500,000 to 10,000,000 francs or both.

Article 431-20
Apart from cases where processing is authorized under the conditions set out in the aforementioned Law on Personal Data, anyone who processes or arranges the processing of personal data that include the registration numbers of natural persons in the national personal identification directory shall be punished with a prison term of one (1) to seven (7) years and/or a fine of 500,000 to 10,000,000 francs.

Article 431-21
Anyone who processes or arranges the processing of personal data without taking the measures set out in Article 71 of the aforementioned Law on Personal Data shall be punished with a prison term of one (1) to seven (7) years and/or a fine of 500,000 to 10,000,000 francs.

Article 431-22
Anyone who collects personal data by fraudulent, dishonest or unlawful means shall be punished with a prison term of one (1) to seven (7) years and/or a fine of 500,000 to 10,000,000 francs.

Article 431-23
Anyone who processes or arranges the processing of personal data relating to a natural person in spite of an objection by that person under Article 68 of the Law on Personal Data, where the processing is for marketing purposes, particularly commercial marketing, or where there are legitimate grounds for the objection shall be punished with a prison term of one (1) to seven (7) years and/or a fine of 500,000 to 10,000,000 francs.

Article 431-24
Apart from cases provided for by law, anyone who places or retains on a data medium or in a computer memory, without the express consent of the interested party, personal data that directly or indirectly indicate racial or ethnic origin, political, philosophical or religious beliefs or trade-union membership, or that relate to the interested party's health or sexual orientation shall be punished with a prison term of one (1) to seven (7) years and/or a fine of 500,000 to 10,000,000 francs.

The provisions of the first paragraph of the present Article shall apply to non-automatic processing of personal data, the use of which is not limited to exclusively personal activities.

Article 431-25
Apart from cases provided for by law, anyone who places or retains on a data medium or in a computer memory personal data relating to offenses, convictions or safety measures shall be punished with the same penalties.

Article 431-26
Anyone who processes personal data for the purposes of health-related research shall be punished with the same penalties if:

1. he has not informed, individually and in advance, the persons whose personal data have been collected or transmitted on their right of access, correction and objection, the nature and addressees of the data transmitted, and the steps taken to process, preserve and protect the data;

2. the processing is carried out in spite of an objection by the person concerned or, where it is provided for by law, without the express informed consent of the person or, in the case of a deceased person, in spite of a refusal expressed by that person while he was still alive.

Article 431-27
Anyone who retains personal data beyond the necessary period set out in Article 35 of the Law on Personal Data, unless they are retained for historical, statistical or scientific purposes under conditions provided for by law, shall be punished with a prison term of one (1) to seven (7) years and/or a fine of 500,000 to 10,000,000 francs.

Article 431-28
Apart from cases provided for by law, anyone who, for purposes other than historical, statistical or scientific reasons, processes personal data that have been retained beyond the necessary period set out in Article 35 of the Law on Personal Data shall be punished with the same penalties.

Article 431-29
Anyone who is in possession of personal data in connection with the recording, classification, transmission or any other form of processing thereof and diverts said data to a purpose other than that defined by the law, regulation or decision of the Commission on Personal Data authorizing automated processing or by statements made prior to such processing shall be punished with a prison term of one (1) to seven (7) years and/or a fine of 500,000 to 10,000,000 francs.

Article 431-30
Anyone who, in connection with the recording, classification, transmission or any other form of processing thereof, collects personal data the disclosure of which would damage the interested party's consideration or privacy and, without the authorization of the interested party, brings these data to the attention of a third party who is not entitled to receive them shall be punished with a prison term of one (1) to seven (7) years and/or a fine of 500,000 to 10,000,000 francs.

Where the disclosure referred to in the previous paragraph of the present Article is carried out through negligence, the person responsible shall be punished with a prison term of six (6) months to five (5) years and/or a fine of 300,000 to 5,000,000 francs.

In the cases referred to in the first two paragraphs of the present Article, prosecution may be initiated only on a complaint by the victim or his legal representative or successors in title.

Article 431-31
A prison term of six months to two years and/or a fine of 200,000 to 1,000,000 francs shall be imposed on anyone who obstructs the activity of the Commission on Personal Data in the following ways:

1. by obstructing the performance of the tasks entrusted to its members or authorized officials in implementation of the Law on Personal Data;

2. by refusing to communicate to its members or authorized officials, in implementation of the Law on Personal Data, information and documents necessary for the performance of their tasks or by concealing said documents or information or causing them to disappear;

3. by communicating information that is not consistent with the content of the data recorded as at the time when the request was made or that fails to present the content in a directly accessible form.

CHAPTER III: OTHER ABUSES

Article 431-32
Anyone who produces, sells, imports, holds, distributes, offers, assigns or makes available a piece of equipment, a computer program or any device or datum designed or specially adapted for committing one or more of the offenses set out in Articles 431-8 to 431-16 of the present Law, or a password, access code or similar computerized data that enables access to all or part of a computer system shall be punished with the penalties established respectively for the offense itself or for the most severely punished offense.

Article 431-33
Anyone who joins an association or enters into an agreement for the purpose of preparing or committing one or more of the offenses established by the present Law shall be punished with the penalties established respectively for the offense itself or for the most severely punished offense.

CHAPTER IV: CONTENT-RELATED OFFENSES

SECTION I: CHILD PORNOGRAPHY

Article 431-34
Anyone who produces, records, offers, makes available, distributes or transmits an image or representation that constitutes child pornography through a computer system shall be punished with a prison term of five (5) to ten (10) years and/or a fine of 5,000,000 to 15,000,000 francs.

Article 431-35

Anyone who procures, for himself or for another person, imports or arranges the import of, or exports or arranges the export of an image or representation that constitutes child pornography through a computer system shall be punished with a prison term of five (5) to ten (10) years and/or a fine of 5,000,000 to 15,000,000 francs.

Article 431-36
Anyone who possesses an image or representation that constitutes child pornography in a computer system or on any computerized data-storage medium shall be punished with the same penalties.

Anyone who facilitates access by a minor to pornographic images, documents, sound or representations shall be punished with the same penalties.

Article 431-37
Where the offenses established by the present Law are committed by an organized gang, they shall be punishable by the maximum penalty provided for in Article 431-23 of the present Law.

SECTION II: OTHER CONTENT-RELATED OFFENSES

Article 431-38
Anyone who creates, downloads, distributes or makes available in any form writings, messages, photos, drawings or any other representation of ideas or theories of a racist or xenophobic nature through a computer system shall be punished with a prison term of six (6) months to seven (7) years and a fine of 1,000,000 to 10,000,000 francs.

Article 431-39
A threat, issued through a computer system, to commit a criminal offense against a person on grounds of his membership of a group characterized by race, color, ancestry or national or ethnic origin, or religion insofar as it is used as the pretext for a threat on one or other of the grounds mentioned, or against a group of persons distinguished by one of these characteristics shall be punishable by a prison term of six (6) months to seven (7) years and a fine of 1,000,000 to 10,000,000 francs.

Article 431-40
Abuse perpetrated through a computer system against a person on grounds of his membership of a group characterized by race, color, ancestry or national or ethnic origin, or religion insofar as it is used as the pretext for abuse on one or other of the grounds mentioned, or against a group of persons distinguished by one of these characteristics shall be punishable by a prison term of six (6) months to seven (7) years and a fine of 1,000,000 to 10,000,000 francs.

Article 431-41
Anyone who intentionally denies or expresses approval of or justification for acts constituting genocide or crimes against humanity through a computer system shall be

punished with a prison term of six (6) months to seven (7) years and a fine of 1,000,000 to 10,000,000 francs.

Article 431-42
In the event of conviction, the court may order the confiscation of materials, equipment, instruments, computer programs or any devices or data belonging to the convicted person that have been used to commit the offenses established in Articles 431-8 to 431-41 of the present Law.

CHAPTER V: OFFENSES RELATING TO THE ACTIVITIES OF TECHNICAL PROVIDERS OF ELECTRONIC COMMUNICATION SERVICES TO THE PUBLIC

Article 431-43
Anyone who, with the aim of securing the withdrawal of content or of an activity or of stopping the dissemination thereof, presents said content or activity to the persons mentioned in Article 3, paragraph 2, of the Law on Electronic Transactions as unlawful while knowing that it is not shall be punished with a prison term of six (6) months to one (1) year and/or a fine of 200,000 to 1,000,000 francs.

Article 431-44
Any natural person or de jure or de facto director of a legal entity engaged in one of the activities set out in Article 3, paragraphs 1 and 2, of the Law on Electronic Transactions who fails to fulfill the obligations set out in the fourth subparagraph of Article 3, paragraph 5, of the Law on Electronic Transactions, or fails to retain the information referred to in the first paragraph of Article 4 of the aforementioned Law or fails to comply with a request from a judicial authority to provide said information shall be punished with a prison term of six (6) months to one (1) year and/or a fine of 100,000 to 500,000 francs.

Article 431-45
Any natural person or de jure or de facto director of a legal entity engaged in the activity set out in Article 3 of the Law on Electronic Transactions who fails to comply with the requirements of that Article shall be punished with a prison term of six (6) months to one (1) year and/or a fine of 200,000 to 1,000,000 francs.

Article 431-46
Any natural person or de jure or de facto director of a legal entity engaged in the activity set out in Article 3 of the Law on Electronic Transactions who fails to comply with the requirements of Article 5 of that Law shall be punished with a prison term of six (6) months to one (1) year and/or a fine of 200,000 to 2,000,000 francs.

Article 431-47
Any editor of a publication who is requested to publish a reply relating to the exercise of the right of reply, in implementation of Article 6 of the Law on Electronic Transactions, shall be obliged to do so within twenty-four (24) hours of receipt of the request; failure

to do so shall incur a fine of 200,000 to 20,000,000 CFA francs, without prejudice to any other penalties established by the legislation in force.

Article 431-48
The provisions of Article 431-44 of the present Law shall apply to any failure to fulfill the obligation to inform the consumer, as set out in Article 10 of the Law on Electronic Transactions.

Article 431-49
The refusal by an electronic provider of goods or services to reimburse the sums received from a consumer who exercises his right of retraction shall be punishable by a prison term of six (6) months to one (1) year and/or a fine of 200,000 to 2,000,000 francs.

Article 431-50
Anyone who deceives a buyer as to the identity, nature or origin of a good sold, by fraudulently supplying a good other than the one ordered and paid for by the consumer, shall be punished with a prison term of one (1) month to one (1) year and/or a fine of 500,000 to 10,000,000 francs.

CHAPTER VI: OFFENSES RELATING TO ELECTRONIC ADVERTISING

Article 431-51
Anyone who disregards the conditions set out in Article 15 of the Law on Electronic Transactions for benefiting from promotional offers and for participation in promotional competitions or games, where these offers, competitions or games are presented digitally, shall be punished with a prison term of six (6) months to two (2) years and/or a fine of 100,000 to 500,000 francs.

Article 431-52
Anyone who creates advertising material, in particular promotional offers, such as discounts, bonuses or gifts, and promotional competitions or games distributed by electronic mail in violation of Article 14 of the Law on Electronic Transactions shall be punished with a prison term of six (6) months to two (2) years and/or a fine of 100,000 to 500,000 francs.

CHAPTER VII: INTERFERENCE WITH PROPERTY

Article 431-53
Misappropriation of information from another person shall be regarded as theft.

Article 431-54
Where an offense is committed through a computer system, the sentence may not be suspended.

Article 431-55

Where a misdemeanor is committed through a computer system, the penalties set out in the first paragraph of Article 379 may be doubled.

Article 431-56
Anyone who obtains personal, confidential or privileged information by any fraudulent means or by using false names or acting under false pretences shall be punished with the penalties set out in the first paragraph of Article 379.

Article 431-57
Anyone who harbors information that has been removed, held or obtained by means of a crime or misdemeanor shall be punished with the penalties referred to in the previous paragraph.

CHAPTER VIII: OFFENSES COMMITTED BY ANY MEANS OF PUBLIC DISSEMINATION

Article 431-58
The following are considered to be means of public dissemination: radio and television broadcasting, cinema, the press, billposting, exhibitions, the distribution of writings or images of all kinds, speeches, singing, shouts or threats uttered in public places or at public meetings, any technical process intended to reach the public and, in general, any means of digital communication that is delivered electronically.

Article 431-59
A prison term of six (6) months to seven (7) years and/or a fine of 500,000 to 10,000,000 francs shall be imposed on anyone who carries out the following acts in respect of any immoral printed matter, writings, drawings, posters, engravings, paintings, photographs, films or negatives, photographic matrices or reproductions, emblems, objects or images:

1. manufacturing or holding them with a view to trading, distributing, renting, displaying or exhibiting them;

2. importing them or arranging their import, exporting them or arranging their export, or transporting them or arranging their transport knowingly for the same purposes;

3. displaying, exhibiting or projecting them for public view;

4. selling or renting them or offering them for sale or rent, even if not publicly;

5. making them available, even free of charge and even if not publicly, in any form, directly or indirectly;

6. distributing them or supplying them for distribution by any means.

The maximum penalty shall be imposed where the acts referred to above relate to pornographic material.

A convicted person may also, for a period of no more than six months, be prohibited from performing, directly or through an intermediary, de jure or de facto, management functions in any company that prints, publishes, consolidates or distributes newspapers or periodicals.

Anyone who breaches the prohibition referred to above shall be punished with the penalties set out in the present Article.

CHAPTER IX: OFFENSES AGAINST NATIONAL SECURITY

Article 431-60
Any Senegalese national shall be guilty of treason and sentenced to life imprisonment if he:

1. supplies a foreign Power or its agents, in any form or by any means, with any information, object, document, process, digitized data or computerized file that has to be kept secret in the interests of national security;

2. secures, by any means, possession of such information, object, document, process, computerized data or computerized file with a view to supplying it to a foreign Power or its agents;

3. destroys or arranges the destruction of such information, object, document, process, digitized data or computerized file for the benefit of a foreign Power.

Article 431-61
Any Senegalese national or foreign national who, with the intention of supplying them to any third country, gathers information, objects, documents, processes, data or computerized files, the gathering and exploitation of which are likely to harm national security, shall be punished with a maximum penalty of hard labor for a specific term.

A penalty of 10 to 20 years' imprisonment shall be imposed on anyone with the function or title of custodian or depositary of any information, object, document, process, digitized data or computerized file that has to be kept secret in the interests of national security or the knowledge of which could lead to the discovery of a national security secret who, without the intention of committing treason or espionage:

1. destroys or removes it, arranges for the destruction or removal thereof, or reproduces it or arranges for the reproduction thereof;

2. brings it to the attention or arranges for it to be brought to the attention of an unqualified person or a member of the public.

The penalty shall be five to 10 years' imprisonment if the custodian or depositary has acted in error, carelessness, lack of attention, negligence or failure to observe regulations.

CHAPTER X: CRIMINAL LIABILITY

Article 431-62
Legal entities other than the State, local authorities and public establishments shall be held criminally liable for the offenses set out in the present Law, where committed on their behalf by their organs or representatives.

Where legal entities are held liable, this shall not rule out the liability of the natural persons who committed or were complicit in the same acts.

The penalties incurred by legal entities shall be:

(1) a fine, the maximum amount of which shall be five times that imposed on natural persons by the law establishing the penalty for the offense;

(2) dissolution, where the legal entity has been established for the purpose of committing the criminal acts in question or, in the case of a crime or misdemeanor for which natural persons are liable to a prison term of more than five (5) years, where it has been diverted from its purpose in order to commit said acts;

(3) a prohibition, either permanent or for a period of up to five (5) years, on carrying out, directly or indirectly, one or more professional or social activities;

(4) closure, either permanent or for a period of up to five (5) years, of one or more of the establishments of the company used to commit the criminal acts;

(5) exclusion from public procurement, permanently or for a period of up to five (5) years;

(6) a prohibition, either permanent or for a period of up to five (5) years, on making a public offering;

(7) a prohibition for a period of up to five (5) years on issuing checks other than those that allow the drawer to withdraw funds from the drawee or those that are certified, and on using payment cards;

(8) confiscation of the item used or intended to be used to commit the offense, or of the proceeds of the offense;

(9) display of the verdict handed down or publication thereof either in the press or by any electronic means of communication to the public.

Article 431-63
With the exception of press-related offenses committed via the Internet, the crimes, misdemeanors and infringements set out in book III, title I, chapter IV, section IV, of the

Penal Code, where they are committed through a digital communication medium, shall be subject to the common law liability regime.

Article 431-64
In the event of a conviction for an offense committed through a digital communication medium, the court may order, as additional penalties, a prohibition on sending digital communication messages, a temporary or permanent prohibition on access to the site used to commit the offense, the cutting of access to the site by all available technical means or even a prohibition on hosting the site.

The court may order any person legally responsible for the site used to commit the offense, or any person qualified to use the necessary technical means, to guarantee the prohibition on accessing or hosting the site in question or the cutting of access to it.

The breach of prohibitions ordered by the court shall be punishable by a prison term of six (6) months to three (3) years and a fine of 300,000 to 5,000,000 francs.

Article 431-65
In the event of conviction for an offense committed through a digital communication medium, the court shall order, in addition, the publication through the same medium of an extract of the decision at the convicted person's expense.

The publication referred to in the previous paragraph shall be carried out within 15 days of the day on which the conviction becomes final.

A convicted person who does not publish or arrange for the publication of the extract referred to above shall be punished with the penalties set out in the Penal Code.

If the convicted person does not publish or arrange for the publication of the extract within fifteen (15) days of the conviction becoming final, the penalties provided for in the present Article shall be doubled.

Article 2
Title XVI, "Proceedings relating to offenses committed by means of information and communication technologies", consisting of Articles 677-34 to 677-42 set out below, shall be inserted in book IV of the Code of Penal Procedure.

TITLE XVI: PROCEEDINGS RELATING TO OFFENSES COMMITTED BY MEANS OF INFORMATION AND COMMUNICATION TECHNOLOGIES

CHAPTER I: STATUTE OF LIMITATIONS FOR OFFENSES COMMITTED THROUGH DIGITAL NETWORKS

Article 677-34
The crimes, misdemeanors and infringements set out in book III, title I, chapter IV, section IV, of the Penal Code, where they are committed through computer networks,

shall be subject to the time limits and conditions set out in Articles 431-12 to 431-16 of the Law on Cybercrime, starting from the date of cessation of the offending activity online.

CHAPTER II: EXPEDITED PRESERVATION OF ARCHIVED COMPUTERIZED DATA

Article 677-35
Where necessary for information purposes, in particular where there are grounds to believe that computerized data archived in a computer system are particularly vulnerable to loss or modification, the investigating judge may order any person to preserve and maintain the integrity of the data in his possession or under his control for a maximum period of two years, in order to facilitate judicial investigations.

The custodian of the data or any other person who is to preserve them shall keep them confidential.

Any breach of confidentiality shall be punishable by the penalties applicable to the offense of breach of professional secrecy.

CHAPTER III: SEARCH AND SEIZURE OF COMPUTER DATA

Article 677-36
Where data stored in a computer system or on a computerized-data storage medium in Senegalese territory are needed in order to ascertain the truth, the investigating judge may search or access a computer system or a part thereof or another computer system, provided that such data are accessible from or available to the initial system.

If it is established in advance that such data, accessible from or available to the initial system, are stored in another computer system situated outside the national territory, they shall be collected by the investigating judge, subject to the access conditions set out in the international agreements in force.

Article 677-37
Where the investigating judge discovers in a computer system stored data that are needed in order to ascertain the truth, but seizure of the medium does not appear desirable, these data, together with those necessary in order to understand them, shall be copied onto computer storage media that can be seized and sealed.

Any person qualified to use the appropriate technical means shall be appointed by the investigating judge to prevent access to the data referred to in the previous Article that are in the computer system or copies of the data available to persons authorized to use the computer system, and to ensure their integrity.

If the data relating to the offense, whether they are the object or the product thereof, offend against *ordre public* or morality or constitute a threat to the integrity of computer

systems or of data stored, processed or transmitted through such systems, the investigating judge shall order the necessary precautionary measures, in particular by appointing any qualified person to use all appropriate technical means to render the data inaccessible.

Where it is not possible, for technical reasons or because of the volume of data, to take the measure provided for in the second paragraph of Article 677-37 of the present Law, the investigating judge shall use appropriate technical means in order to prevent access to the data in the computer system and to copies of the data that are available to persons authorized to use the computer system, and also in order to ensure their integrity.

The investigating judge shall inform the person responsible for the computer system that a search of the system has been carried out and shall send him a copy of the data that have been copied, rendered inaccessible or withdrawn.

CHAPTER IV: INTERCEPTION OF COMPUTERIZED DATA

Article 677-38
Where necessary for information purposes, the investigating judge may use appropriate technical means to collect or record content data, in real time, of specified communications transmitted by means of a computer system, or may compel a service provider, within its existing technical capability, to collect or record said computerized data through the application of existing technical means or to cooperate and assist the competent authorities in the collection or recording thereof.

The access provider shall maintain confidentiality.

Any breach of confidentiality shall be punishable by the penalties applicable to the offense of breach of professional secrecy.

Article 677-39
A criminal investigation officer may, for the purposes of an investigation or in execution of powers delegated to him by a court, carry out the operations provided for in Articles 667-35 to 677-38 of the present Law.

CHAPTER V: ELECTRONIC EVIDENCE IN CRIMINAL CASES

Article 677-40
Writings in electronic form shall be admissible as evidence in criminal cases on the same basis as writings in hard copy, in accordance with the provisions of Article 40 of the Law on Electronic Transactions.

Article 677-41
In the cases provided for in Articles 431-17 to 431-30 of the present Law, the deletion of all or part of the personal data that were the object of the processing that constituted the

offense may be ordered. The members and officials of the Commission on Personal Data shall be authorized to record the deletion of such data.

Article 677-42
The Public Prosecutor shall inform the chairman of the Commission on Personal Data of all prosecutions relating to infringements of the present provisions and, where appropriate, their outcome. He shall inform the chairman of the date and reading of the judgment.

The investigating judge or trial court may require the chairman of the Commission on Personal Data or his representative to submit comments or to present them orally at the hearing.

The competent judge may, at his own initiative or at the request of the interested party, order the release of a seizure at any time.

Article 3
The procedure for the implementation of the present Law shall be established by decree.

The present Law shall be enforced as the law of the land.

Done at Dakar, January 25, 2008

By
Abdoulaye WADE
President of the Republic

Cheikh Hadjibou SOUMARÉ
Prime Minister