IX CONSTITUTIONAL GOVERNMENT

MINISTRY OF JUSTICE

Proposal for Law no. º...../2024

Of ... of ...

Cybercrime

Draft 6 June 2024

EXPLANATORY MEMORANDUM

It is undeniable that the internet has become part of our lives, an information revolution that has created a veritable virtual world, with social networks used for communication between people, the purchase of goods and services carried out via the internet, to such an extent that the use of information and communication networks and technologies has become a ubiquitous reality in everyday life. Almost all the activities of modern societies and economies use the Internet to support them, and not only do citizens use it for their day-to-day activities, but the traditional functions of the state are also carried out and their services made available via the Internet. Many of the activities of modern societies today depend on the Internet, and others have emerged specifically on and for the Internet, making it an unavoidable reality that modern societies can no longer do without in their development process.

Naturally, the day-to-day use of information and communication technologies and IT resources for the activities of citizens, companies and the state entails risks and vulnerabilities that can be used and exploited in an illegal manner, thus making cybercrime a real and genuine threat.

In order to deal with the illicit and abusive use of communication networks, states have undertaken legislative measures with a preventive and repressive dimension, through the approval of specific legislation which, in addition to criminalizing this type of phenomenon, establishes specific rules for investigation and collection of evidence and also encourages cooperation between states in these cases.

Over the years, the international community has taken steps not only to encourage cooperation between states, but also to harmonize national legislation in order to combat cybercrime more effectively. The Council of Europe Convention on Cybercrime, also known as the Budapest Convention, has been open for signature in Budapest since 23 November 2001. It is the first and most important international instrument on crime in cyberspace. It is still the only normative instrument in force in this field. It has a universal vocation and aims to be accepted by most countries in the world. Its primary aim is to contribute to the harmonization of national legislation on cybercrime, and also to encourage and facilitate international cooperation by establishing procedural mechanisms that make criminal investigations effective. It deals with substantive criminal law (defining crimes against the confidentiality, integrity and availability of computer systems, crimes relating to content and

crimes committed by means of information technology) but also contains procedural measures relating to the collection and preservation of evidence and also international judicial cooperation.

In addition to the EU Member States, the Convention includes countries from all continents, including the United States of America, Canada, Argentina, Chile, Colombia, Ghana, Morocco, Cape Verde, Australia, Japan, Sri Lanka and the Philippines.

Accession to the Convention will, when the time comes, have the advantage of belonging to a global area of police and judicial cooperation. Specifically, it will bring the possibility of using new forms of investigation and new avenues of cooperation in ongoing cases, when it becomes necessary to resort to international cooperation. These new ways of investigating and cooperating can be used not only for crimes covered by the Convention, but also for the investigation of other crimes, as long as they are committed using computer systems, and for any type of crime, as long as there is evidence of them in digital format.

From another perspective, the Budapest Convention has been used as a model for legislation for most countries in the world. The Convention establishes, from the outset, a catalogue of crimes which constituted a true lowest common denominator of crimes in this area. None of them are enshrined in Timorese law, with the exception of computer fraud, which is already provided for in Article 268 of the Penal Code. The domestic legal system is clearly lacking in this area.

And the same can be said in procedural matters, because as far as criminal procedural law rules are concerned, the national legal system is even more inadequate to this new reality: Timorese criminal procedural legislation does not have any rules specifically geared towards the effective investigation of cybercrime phenomena, if digital evidence is involved.

This legislative option is to condense all the rules relating to cybercrime into a single piece of legislation and not to introduce changes to the various legislative sources on this matter, i.e. the Penal Code, the Code of Criminal Procedure, and also the general regime of international judicial cooperation in criminal matters (Law no. 15/2011, of 26 October).

This legislative option seems to be more advantageous, as there is a need to adapt national legislation to the cross-realities of the criminal and criminal procedural areas. On the other hand, since specific procedural rules are being introduced, it would be inappropriate to introduce special rules into the structuring legislation of the criminal system (especially the Code of Criminal Procedure), which are only applicable to a restricted number of types of offense. On the other hand, this model saw the practical convenience for judicial operators of systematizing all the rules relating to a specific sector of crime.

With regard to substantive criminal law, in line with the Budapest Convention, the crimes of computer fraud (Article 3), damage to computer programs or other data (Article 4), computer sabotage (Article 5), unlawful access (Article 6), unlawful interception (Article 7), and child pornography (Article 9) and revenge pornography (Article 10) have been introduced. The crime of misuse of a device (Article 8) has also been introduced.

With regard to the liability of legal persons, considering that the penal code refers to special legislation when and under what conditions they are held liable and in line with the recommendation of the Budapest Convention, it was decided to establish a special regime for the criminal liability of legal persons, in relation to the crimes typified in this law and also for all crimes committed via computer systems and also for any type of crime, as long as there is evidence of them in digital format.

With regard to jurisdiction in Timorese criminal law, adjustments have been made to what is already provided for in the Penal Code. In particular, provision has been made for the

possibility that, regardless of the place where the acts were committed, Timor-Leste will declare itself competent to prosecute acts committed by its nationals, if the criminal law of no other state is applicable to them, and the same applies to acts committed for the benefit of legal persons based in Timor-Leste territory. On the other hand, Timor-Leste declares itself competent to judge acts physically committed in Timorese territory, even if they target computer systems located outside that territory, or acts that aim to "attack" computer systems located in Timorese territory, regardless of where those acts are physically committed.

With regard to procedural provisions, the expeditious preservation of data stored on a computer and the expeditious preservation and disclosure of traffic data were introduced (clearly inspired by Articles 16 and 17 of the Budapest Convention) and the injunction mechanism was introduced (also provided for in Article 18 of the Convention). On the other hand, specific regimes were established to adapt classic searches and seizures, already provided for in existing criminal procedural legislation, to investigations into crimes committed in the virtual environment. In fact, the essence of these procedural measures coincides, in the cyberspace environment, with the classic forms of search and seizure in criminal proceedings; however, the way in which search and seizure are described in the Code of Criminal Procedure does not fit in with these new realities.

As far as the system for intercepting electronic communications is concerned, which is already detailed in the Code of Criminal Procedure, this new law has only established that it applies to the crimes typified in this law and also to all crimes committed via computer systems - which would not result from the application of the general system. In fact, the Code of Criminal Procedure already provides for the application of the telephone interception regime to communications other than the telephone, such as electronic communications. However, the list of crimes in which it is permitted to carry out these procedural measures does not include the crimes now introduced by this law. Nor does it include other types of crime, of various kinds, committed via computer systems. In both cases, it is often essential to use interception of communications as the only or essential way of investigating them.

The admissibility of undercover actions as a special investigative mechanism has been provided for and regulated, thus providing the system with special forms of investigation both for the crimes provided for in this law and for those committed via computer systems when they carry a maximum sentence of more than five years or even if the sentence is lower, when it comes to crimes against sexual freedom and self-determination in which the offenders are minors or incapacitated and also in relation to economic and financial offenses.

Inevitably, the approval of special procedural measures in the context of the investigation of computer crimes constitutes a compression of citizens' freedoms in cyberspace.

Everyone can understand the enormous advantage of a free and virtually unregulated space, where everyone can freely communicate, inform themselves and others, as well as - and perhaps above all - express themselves and speak out without censorship or constraints. The legal use of communication networks has brought immeasurable advances to modern society.

However, no one today is unaware that in the opposite direction, communication networks have been used to carry out illegal activities, benefiting from the advantages of mass, effective and extremely low-cost communication, choosing their victims almost indiscriminately, located anywhere in the world and shielding themselves from the authorities behind trans-territoriality, anonymity and technical complexity.

While it is true to say that the Internet is nobody's property, it is also true to say that nobody is directly responsible for it or for what happens on it. It has no headquarters and no place where those responsible can be found.

Modern laws must deal adequately with these new criminal realities, incriminating them and

providing the competent authorities with the necessary tools to investigate and prosecute them.

With regard to international cooperation, as a rule, reference is made to the legal regime already in force. In addition, it is assumed that the Timorese authorities can request international cooperation - and also receive and execute requests for cooperation from foreign authorities - under the same conditions and circumstances in which they would act if the criminal facts were being investigated in Timor-Leste. A permanent 24-hour/7-day point of contact is created within the Criminal Investigation Police (PCIC), which is responsible for ensuring emerging international cooperation in the area covered by this bill.

By mandate of the people, the National Parliament decrees, under the terms of Article 96(1)(a) and (b) of the Constitution, as follows:

CHAPTER I
Purpose and definitions

Article 1
Purpose

This law establishes substantive and procedural criminal provisions, as well as specific provisions on international cooperation in criminal matters, relating to cybercrime and the collection of evidence in electronic form.

Article 2
Definitions

For the purposes of this law, the following are considered

a) "Computer system" means any device or set of interconnected or associated devices in which one or more of them carries out, in execution of a program, the automated processing of computer data, as well as the network that supports communication between them and the set of computer data stored, processed, retrieved or transmitted by that or those devices, with a view to their operation, use, protection and maintenance

b) "computer data" means any representation of facts, information or concepts in a form capable of being processed in a computer system, including programs capable of making a computer system perform a function

c) 'traffic data' means computer data relating to a communication carried out by means of a computer system, generated by that system as part of a communication chain, indicating the origin of the communication, the destination, the path, time, the date, the size, the duration or the type of the underlying service

d) "Service provider" means any entity, public or private, which provides users of its services with the possibility of communicating by means of a computer system, as well as any other entity which processes or stores computer data in the name of and on behalf of that service provider or its users

e) "Interception" means the act of capturing information contained in a computer system by means of electromagnetic, acoustic, mechanical or other devices

f) *'topography'* means a series of linked images, irrespective of how they are fixed or encoded, which represent the three-dimensional configuration of the layers making up a semiconductor product and in which each image reproduces the design, or part

thereof, of a surface of the semiconductor product, irrespective of the stage of manufacture

g) *"semiconductor product" means* the final or intermediate form of any product, composed a substrate comprising a layer of semiconductor material and consisting of one or more layers of conductive, insulating or semiconducting materials, arranged in a three-dimensional configuration and intended to fulfill, exclusively or not, an electronic function

h) *"subscriber data" means* any information which a service provider possesses about subscribers to its services, in the form of computer data or in any other form, other than traffic or content data, and which makes it possible to determine the type of communication service used, the technical measures adapted in this respect, the duration of the service, the identity, postal or geographical address and telephone number of the subscriber and any other access number, as well as billing and payment data available on the basis of the contract or a service agreement, or any other information on the location of communication equipment available on the basis of a contract or a service agreement.

CHAPTER II
Criminal provisions

Article 3
Computer fraud

1. Anyone who, with the intention of causing deception in legal relations, introduces, modifies, deletes or suppresses computer data or in any other way interferes with the computer processing of data, producing non-genuine data or documents, with the intention that they be considered or used for legally relevant purposes as if they were, shall be punished with imprisonment of 1 to 5 years.
2. When the actions described in the previous paragraph concern data registered or incorporated into a bank payment card or any other device that allows access to a payment system or means of payment, a communications system or a conditional access service, the penalty is 1 to 5 years in prison.
3. Anyone who, acting with intent to cause harm to others or to obtain an illegitimate benefit for themselves or for a third party, uses a document produced from computer data that was the subject of the acts referred to in paragraph 1 or a card or other device on which the data that was the subject of the acts referred to in the previous paragraph is recorded or incorporated, shall be punished with the penalties provided for in one and the other paragraph, respectively.
4. Anyone who imports, distributes, sells or holds for commercial purposes any device that allows access to a payment system or means of payment, a communications system or a conditional access service, on which any of the actions provided for in no. 2 has been carried out, shall be punished with imprisonment of 1 to 5 years.
5. If the acts referred to in the preceding paragraphs are committed by an official in the exercise of his duties, the penalty shall be imprisonment for 2 to 5 years.

Article 4
Damage to programs or other data

1. Anyone who, without legal permission or without being authorized to do so by the owner or other right holder of the system or part of it, deletes, alters, destroys, in whole or in

part, damages, suppresses or renders unusable or inaccessible programs or other computer data or in any way affects their usability, shall be punished with imprisonment of up to 3 years or a fine of up to 200 days.

2. Attempt is punishable.
3. Anyone who unlawfully produces, sells, distributes or in any other way disseminates or introduces into one or more computer systems devices, programs or other computer data intended to produce the unauthorized actions described in that paragraph shall incur the same penalty as in paragraph 1.
4. If the damage caused is of high value, the penalty is imprisonment for up to 5 years or a fine of up to 600 days.
5. If the damage caused is of considerably high value, the penalty is imprisonment for 1 to 10 years.
6. In the cases provided for in paragraphs 1, 2 and 3, criminal proceedings shall be subject to a complaint.

Article 5
Informatic sabotage

1. Anyone who, without legal permission or without being authorized to do so by the owner or other right-holder of the system or part of it, hinders, prevents, interrupts or seriously disturbs the operation of a computer system by introducing, transmitting, deteriorating, damaging, altering, erasing, preventing access to or deleting programs or other computer data or by any other form of interference with a computer system, shall be punished with imprisonment for up to 5 years or a fine of up to 600 days.
2. The same penalty shall apply to anyone who unlawfully produces, sells, distributes or otherwise disseminates or introduces into one or more computer systems devices, programs or other computer data intended to produce the unauthorized actions described in the previous paragraph.
3. In the cases provided for in the previous paragraph, the attempt is not punishable.
4. The penalty is imprisonment for 1 to 5 years if the damage resulting from the disturbance is of high value.
5. The penalty is imprisonment for 1 to 10 years if:
   a) The damage resulting from the disturbance is of considerably high value;
   b) the disruption causes serious or lasting damage to an IT system that supports an activity intended to ensure critical social functions, such as supply chains, the health, safety and economic well-being of individuals, or the smooth operation of public services.

Article 6
Illegitimate access

1. Anyone who, without legal permission or without being authorized to do so by the owner or other right-holder of the system or part of it, accesses a computer system in any way, shall be punished with imprisonment of up to one year or a fine of up to 120 days.
2. The same penalty shall apply to anyone who unlawfully produces, sells, distributes or otherwise disseminates or introduces into one or more computer systems devices, programs, an executable set of instructions, code or other computer data intended to produce the unauthorized actions described in the previous paragraph.

3. In the case provided for in paragraph 1, the penalty shall be imprisonment for up to 3 years or a fine if access is gained by violating security rules.
4. The penalty is imprisonment for 1 to 5 years when:
   a) Through access, the agent has learned a commercial or industrial secret or confidential data protected by law;
   b) The benefit or advantage obtained is of a considerably high value.
5. Attempt is punishable, except in the cases provided for in paragraph 2.
6. In the cases provided for in paragraphs 1 and 3, criminal proceedings shall be subject to a complaint.

Article 7
Illegitimate interception

1. Anyone who, without legal permission or without being authorized to do so by the owner or other right holder of the system or part of it, and using technical means, intercepts computer data transmissions that are processed within a computer system, intended for it or originating from it, shall be punished with imprisonment of up to 3 years or a fine.
2. Anyone who unlawfully produces, sells, distributes or in any other way disseminates or introduces into one or more computer systems devices, programs or other computer data intended to produce the unauthorized actions described in paragraph 1 shall incur the same penalty.
3. Attempt is punishable.

Article 8
Misuse of devices

1. Anyone who unlawfully produces, sells, acquires or holds, for the purposes of use, import or distribution for commercial purposes, any device that allows access to a system or means of payment, including a computer program, designed or adapted to allow access to a communications system or conditional access service, on which any of the offenses provided for in articles 4 to 7 has been committed, shall be punished with imprisonment of 1 to 5 years.
2. The same penalty shall apply to anyone who unlawfully reproduces the topography of a semiconductor product or commercially exploits or imports, for these purposes, a topography or a semiconductor product made from that topography.
3. Attempt is punishable.

Article 9
Child pornography

1. Whoever, in addition to the provisions of article 176 of the Penal Code:
   a) to produce, distribute, import, export, disseminate, exhibit or assign, in any way or by any means, a pornographic photograph, film or recording of a person under age 17;
   b) acquiring or possessing materials as referred to in a), with the purpose of distributing, importing, exporting, disseminating, exhibiting or transferring them; shall be punished with imprisonment of 1 to 5 years.
2. Anyone who produces, distributes, imports, exports, disseminates, exhibits or transfers, in any way or by any means, a photograph, film or recording using pornographic material with a realistic representation of a person under the age of 17 shall be punished with

imprisonment of up to 2 years.

3. Anyone who carries out the acts described in the previous paragraphs professionally or for profit shall be punished with imprisonment of 1 to 8 years.
4. Anyone who acquires or detains the materials provided for in paragraphs 1(*a*) and 2 shall be punished with imprisonment of up to one year.
5. Attempt is punishable.
6. The penalties provided for in paragraphs 1 to 4 shall be increased by one third in their minimum and maximum limits, if the victim is an ascendant or descendant, or is under the guardianship of the perpetrator, provided that the circumstances of the case reveal a marked degree of unlawfulness of the act or of the perpetrator's guilt.
7. The penalties provided for in paragraphs 1 to 4 shall be increased by half, in their minimum and maximum limits, if the victim is under 14 years of age.
8. If more than one of the circumstances referred to in the preceding paragraphs occur in the same conduct, only the one with the strongest aggravating effect shall be considered for the purpose of determining the applicable penalty, and the other shall be assessed in the measure of the penalty.
9. Anyone convicted of a crime provided for in this article may, in view of specific gravity of the fact and its connection with the function exercised by the agent, be disqualified from exercising parental authority, guardianship or curatorship, or prohibited from exercising a profession, function or activity that involves having minors under their responsibility, education, treatment or supervision, for a period of 2 to 15 years.

Article 10
Vengeance pornography

Anyone who, without legal permission or without being authorized to do so, discloses or threatens to disclose through a computer system photos, videos or any other material with sexually intimate and private content, whether consensual or not, of a person with whom they have or have had intimate relationship, with the intention of causing moral and psychological damage to the victim, is punished with imprisonment of up to 2 years or a fine of 80 to 200 days.

Article 11
Criminal liability of legal persons and entities

1. Legal persons and similar entities, with the exception of the State, other public legal persons and international organizations governed by public law, are liable for the crimes typified in this law, for crimes committed through computer systems and for any type of crime, provided that there is proof of them in digital format, when committed:
   a) On their behalf and in the collective interest of people in a leadership position;
   b) By anyone acting under the authority of the persons referred to in the previous paragraph as a result of a breach of their duty of supervision or control;
2. For the purposes of this law, the term public legal persons includes:
   a) Legal persons governed by public law, including public business entities;
   b) Public service concessionaires, regardless of ownership;
   c) Other legal persons exercising prerogatives of public power.
3. It is understood that the bodies and representatives of the legal person who have the authority to exercise control over its activities are in a leadership position.

4. For the purposes of criminal liability, civil companies and de facto associations are considered to be equivalent to legal persons.
5. The liability of legal persons and similar entities is excluded when the agent has acted against the express orders or instructions of those in authority.
6. The liability of legal persons and similar entities does not exclude the individual liability of their agents, nor does it depend on their accountability.
7. The demerger or merger does not determine the extinction of the criminal liability of the legal person or similar entity, which is still liable for the crime:
   a) The legal person or equivalent entity in which the merger took place; and
   b) The legal persons or equivalent entities that result from the demerger.
8. Without prejudice to the right of recourse, persons in a position of leadership are subsidiarily liable for the payment of fines and compensation to which the legal person or similar entity is sentenced in relation to crimes:
   a) Carried out while in office, without their express opposition;
   b) Previously practiced, when it was due to their fault that the assets of the legal person or similar entity became insufficient to pay for them;
   c) previously committed, when the final decision to apply them was notified during the period in which they held office and they are responsible for non-payment.
9. If several persons are responsible under the terms of the previous paragraph, they shall be jointly and severally liable.
10. If the fine or compensation is imposed on an entity without legal personality, the common assets and, in the absence or insufficiency thereof, jointly and severally, the assets of each of the members, shall be liable for them.
11. For the crimes provided for in paragraph 1 of this article, the main penalties of a fine or dissolution shall apply to legal persons and similar entities.
12. The following penalties may be imposed on legal persons and similar entities for the same crimes:
    a) Judicial injunction;
    b) Prohibition of activity;
    c) Prohibition on entering into certain contracts or contracts with certain entities;
    d) Deprivation of the right to subsidies, grants or incentives;
    e) Closure of establishment;
    f) Publicizing the condemnatory decision at your expense.

Article 12
Penalty of a fine

1. The minimum and maximum limits of the fine applicable to legal persons and similar entities are determined by reference to the prison sentence provided for natural persons.
2. One month's corresponds, for legal persons and similar entities, to 10 days' fine.
3. Whenever the penalty applicable to natural persons is determined exclusively or alternatively as a fine, the same fine days shall apply to legal persons or similar entities.
4. The fine shall be set in days in accordance with the criteria established in article 51.1 of the penal code.

5. Each day of the fine corresponds to an amount of between 100 and 10,000 US dollars, which the court shall determine in accordance with the economic and financial situation of the convicted person and their employee costs, and the provisions of Article 75.3 of the Penal Code shall apply.
6. Once the deadline for payment of the fine or any of its installments has passed without payment being made, the assets of the legal person or similar entity shall be forfeited.
7. A fine that is not voluntarily or coercively paid cannot be converted into subsidiary imprisonment.

Article 13
Forfeiture of assets

1. Without prejudice to the application of the general regime provided for in article 102 et seq. of the Penal Code, the court shall order the forfeiture to the State of objects, materials, equipment or devices that have been used to commit the crimes provided for in this law and belong to a person who has been convicted of committing them.
2. The assets referred to in paragraph 1 may be used provisionally by criminal police bodies, by means of a declaration of operational utility, from the moment they are seized until they are declared forfeit or returned, when they are likely to be declared to the State at the end of the process.
3. For the purposes of the preceding paragraph, interested parties shall be notified.
4. Once the asset has been seized and its operational usefulness has been verified, it will be registered, examined and valued.
5. The value of the appraisal determines the amount to be paid to the owner as compensation if the asset is not ultimately declared forfeit to the State.
6. The valuation of the property shall be carried out by experts appointed by the judicial authority to whom the commitment to carry out the task is entrusted.
7. The declaration of cessation of operational utility ceases with declaration of loss in favor of the State or the restitution to the owner or legitimate holder.

CHAPTER III
Procedural provisions

Article 14
Scope of application of Procedural provisions

With the exception of the provisions of Articles 21 and 22, the procedural provisions of this Chapter shall apply to criminal proceedings:

a) Provided for in this law;
b) committed by means of a computer system; or
c) For which it is necessary to collect evidence in electronic form.

Article 15
Expedited data preservation

1. If, in the course of the proceedings, it is necessary for the production of evidence, with a view to discovering the truth, to obtain specific computer data stored in a computer system, including traffic data, in relation to which there is a fear that it may be lost, altered or no longer available, the Public Prosecutor or the judge, depending on the procedural stage, shall order whoever has availability or control of that data, namely the

service provider, to preserve the data in question.

2. Preservation may also be ordered by the criminal police, with the authorization of the Public Prosecutor's Office or the judge, depending on the procedural stage, or when there is urgency or danger of delay, in which case Public Prosecutor's Office or the judge must be notified immediately, with a description of the facts found and the evidence collected.
3. The preservation order discriminates, under penalty of nullity:
   a) The nature of the data;
   b) Their origin and destination if known;
   c) The period of time for which they should be preserved, up to a maximum of six months.
4. In compliance with a preservation order addressed to them, those who have availability or control over such data, namely the service provider, shall immediately preserve the data in question, protecting and preserving its integrity for the set period of time, so as to allow the Public Prosecutor's Office or the judge to obtain it, and shall be obliged to ensure the confidentiality of the application of the procedural measure.
5. The Public Prosecutor's Office or the judge may order the measure to be renewed for periods subject to the limit provided for in paragraph 3(*c*), provided that the respective admissibility requirements are met, up to a maximum of one year.

Article 16
Expedited disclosure of traffic data

In order to ensure the preservation of traffic data relating to a given communication, regardless of the number of service providers that participated in it, the service provider to whom such preservation has been ordered under the terms of the previous article shall inform the public prosecutor, the judge or the criminal police body, as soon as it becomes aware of it, of other service providers through which that communication was made, with a view to making it possible to identify all the service providers and the means by which that communication was made.

Article 17
Injunction to provide or grant access to data

1. If, in the course of the proceedings, it becomes necessary for the production of evidence, with a view to discovering the truth, to obtain specific and determined computer data stored in a given computer system, the Public Prosecutor's Office or the judge, depending on the procedural stage, shall order whoever has availability or control of this data to communicate it to the proceedings or to allow access to it, under penalty of punishment for disobedience.
2. The order referred to in the previous paragraph identifies the data in question.
3. In compliance with the order described in paragraphs 1 and 2, whoever has availability or control of such data shall communicate it to the Public Prosecutor's Office or the judge, or allow access to the computer system where it is stored, under penalty of disobedience.
4. The provisions of this article shall apply to service providers, who may be ordered to communicate to the procedure data relating to their customers or subscribers, including any information other than traffic or content data, contained in form of computer data or in any other form, held by the service provider, which be determined
   a) The type of communication service used, the technical measures taken in this regard and the period of service

b) The identity, postal or geographical address and telephone number of the subscriber, and any other access number, billing and payment data available on the basis of a contract or service agreement;

c) Any other information on the location of the communication equipment, available on the basis of a contract or service agreement.

5. The order provided for in this article may not be addressed to a suspect or defendant in the proceedings.

6. The injunction provided for in this article may not also be used with regard to computer systems specifically used in the exercise of the professional activity of persons subject to the duty of secrecy referred to in Article 126.1 of the Code of Criminal Procedure.

7. The rules on professional or official secrecy and state secrecy set out in articles 126, 127 and 128 of the Code of Criminal Procedure shall apply *mutatis mutandis*.

Article 18
Computer data search

1. When, in the course of the proceedings, it becomes necessary for the production of evidence, with a view to discovering the truth, to obtain specific and determined computer data stored in a certain computer system, the Public Prosecutor's Office or the judge, depending on the procedural stage, shall authorize or order by order that a search be carried out in that computer system, and shall, whenever possible, preside the procedure.

2. The order provided for in the previous paragraph shall be valid for a maximum of 30 days, after which it shall be null and void.

3. The criminal police body may carry out a search, without prior authorization from the Public Prosecutor's Office or a judge, when:

a) It is voluntarily consented to by whoever has the availability or control of such data, provided that the consent given is documented in any way

b) In cases of terrorism, violent crime or highly organized crime, when there are well-founded indications of the imminent commission of a crime that seriously endangers the life or integrity of any person.

4. When the criminal police agency carries out the search under the terms of the previous paragraph:

c) In the case provided for in point *b*), the diligence shall, under penalty of nullity, be immediately communicated to the Public Prosecutor's Office or the judge, depending on the procedural stage, and shall be examined by the latter in order to validate it;

d) In any case, the Public Prosecutor's Office or the judge, depending on the procedural stage, will draw up a report summarizing the investigations carried out, the results of the investigation, a description of the facts found and the evidence gathered.

5. When, in the course of the search, there is reason to believe that the data sought is in another computer system, or in a different part of the system searched, but that such data is legitimately accessible from the initial system, the search may be extended the authorization of the Public Prosecutor's Office or the judge, under the terms of paragraphs 1 and 2.

6. The search referred to in this article shall be subject, mutatis mutandis, to the rules governing the execution of searches laid down in the Code of Criminal Procedure.

Article 19
Seizure of data

1. When, in the course of a computer search or other legitimate access to a computer system, computer data or documents necessary for the production of evidence are found, with a view to discovering the truth, the Public Prosecutor's Office or the judge, depending on the procedural stage, shall authorize or order their seizure.
2. The criminal police body may carry out seizures, without prior authorization from the judicial authority, in the course of a computer search legitimately ordered and carried out under terms of the previous article, as well as when there is urgency or danger of delay.
3. If computer data or documents are seized whose content is likely to reveal personal or intimate data that could jeopardize the privacy of the respective holder or a third party, under penalty of nullity, such data or documents shall be submitted to the judge, who shall consider their inclusion in the case file, taking into account the interests of the specific case.
4. Seizures made by the criminal police are always subject to validation by the judicial authority within a maximum of 72 hours.
5. The seizure of data relating to computer systems used for the exercise of secret professions or functions is subject, with the necessary adaptations, to the rules and formalities laid down in article 226 of the Code of Criminal Procedure.
6. Seizures relating to computer systems used to carry out the activities of the persons indicated in articles 126, 127 and 128 of the Code of Criminal Procedure are subject, with the necessary adaptations, to the rules and formalities laid down in the Code of Criminal Procedure.
7. The seizure of computer data, depending on whether it is more appropriate and proportionate, taking into account the interests of the specific case, may, in particular, take the following forms:
   a) Seizure of the medium on which the system is installed or seizure of the medium on which the computer data is stored, as well as the devices needed to read it;
   b) Making a copy of the data, on a stand-alone medium, which will be attached to the file;
   c) Preservation, by technological means, of the integrity of the data, without copying or removing it;
   d) Non-reversible deletion or blocking of access to data.
8. In the case of a seizure made under the terms of paragraph *b*) of the previous number, the copy is made in duplicate, one of the copies is sealed and entrusted to the court clerk of the departments where the proceedings are taking place and, if technically possible, the seized data is certified by means of a digital signature.

Article 20
Seizure of emails and records of similar communications

1. If, in the course of a computer search or other legitimate access to a computer system, electronic mail messages or records of communications of a similar nature are found stored in that computer system or in another to which legitimate access is allowed from the former, they shall be provisionally seized by the criminal police carrying out the search or other legitimate access to the system.
2. Once the records have been viewed, they shall be taken to the judge to order that they be

added to the case file, if the seizure appears to be of great interest to the discovery of the truth or to evidence.

3. Insofar as not provided for in the preceding paragraphs, the system for the seizure of correspondence provided for in the Code of Criminal Procedure shall apply in the alternative.

Article 21
Interception of communications

1. The interception of communications is admissible in criminal proceedings:
   a) Provided for in this law;
   b) Committed by means of a computer system or in relation to which it is necessary to collect evidence on an electronic medium, when such crimes are provided for in Article 177 of the Code of Criminal Procedure.
2. The interception and recording of computer data transmissions may only be authorized during the investigation if there is reason to believe that the procedure is indispensable for discovering the truth or that the evidence would otherwise be impossible or very difficult to obtain, by reasoned order of the competent judge and at the request of the Public Prosecutor's Office.
3. The interception may be aimed at recording data on the content of communications or only at collecting and recording traffic data, and the order referred to in the previous paragraph must specify the respective scope, according to the specific needs of the investigation.
4. In everything that is not contradicted by this article, the interception and recording of computer data transmissions shall be subject to the rules governing the interception and recording of telephone conversations or communications set out in articles 177 and 178 of the Code of Criminal Procedure.

Article 22
Covert actions

1. The use of covert actions is admissible in the course of investigations into the following crimes:
   a) Those provided for in this law;
   b) Those committed by means of a computer system, in the abstract, with a maximum prison sentence of more than 5 years or, even if the sentence is less, and being intentional, crimes against freedom and sexual self-determination in cases where the offenders are minors or incapacitated, qualified fraud, computer and communications fraud, racial, religious or sexual discrimination, economic and financial offenses.
2. If the use of computer means and devices is necessary, the rules laid down for the interception of communications shall be observed, where applicable.
3. Undercover actions are those carried out by criminal investigation officials or third parties acting under the control of the Criminal Investigation Police, in the investigation of the crimes indicated in this law, with concealment of their quality and identity.
4. Authorization to carry out an undercover operation is given by the judge on duty, within a maximum of 48 hours, on a proposal from the Public Prosecutor's Office, which must include the reasons for the operation, a summary description of the operation and, whenever possible, the need for and safety of the operation.

5. The Criminal Investigation Police shall report on the undercover officer's intervention to the Public Prosecutor's Office no later than 48 hours after the end of the intervention.
6. No one can be forced to take part in an undercover action.
7. The presence of a criminal investigation official or a third party who has concealed their identity may be waived, under the terms of Law no. 2/2009, of May 6, which regulates the application of protection measures for witnesses and other actors in criminal proceedings.

CHAPTER IV
International cooperation

Article 23
Scope of international cooperation

The competent national authorities shall cooperate with the competent foreign authorities for the purposes of investigations or proceedings concerning crimes related to computer systems or data, as well as for the purposes of gathering evidence, in electronic form, of a crime under the terms of this law and, where not provided for herein, under the terms of the general regime of international judicial cooperation in criminal matters, provided for in Law no. 15/2011, of 26 October.

Article 24
Permanent contact point for international cooperation

1. For the purposes of international cooperation, with a view to providing immediate assistance for the purposes referred to in the previous article, the Attorney General's Office shall ensure that a structure is maintained which guarantees a permanently available point of contact, twenty-four hours a day, seven days a week, without prejudice to the delegation of powers to the Criminal Investigation Police.
2. This contact point may be contacted by other contact points, under the terms of agreements, treaties or conventions to which Timor-Leste is bound, or compliance with international cooperation protocols with judicial or police bodies.
3. The immediate assistance provided by this permanent contact point includes:
   a) Providing technical advice to other points of contact;
   b) The expeditious preservation of data in cases of urgency or danger of delay, in accordance with the provisions of the following article;
   c) The taking of evidence for which it is competent in cases of urgency or danger of delay;
   d) Locating suspects and providing legal information in cases urgency or danger of delay;
   e) The immediate transmission to the Public Prosecutor's Office of requests relating to the measures referred to in points *b*) to *d*), outside the cases provided for therein, with a view to their swift execution.
4. Whenever the Criminal Investigation Police act in accordance with points *b*) to *d*) of the previous paragraph, they shall immediately notify the Public Prosecutor's Office and send it a report summarizing the investigations carried out, results, a description of the facts found and the evidence collected.

Article 25
Expeditious preservation and disclosure of computer data in international cooperation

1. Timor-Leste may be requested to expeditiously preserve computer data stored in a computer system located here, relating to crimes provided for in article 14, with a view to submitting a request for legal assistance for the purpose of searching, seizing and disclosing it.
2. The request specifies:
   a) The authority that calls for preservation;
   b) The offense that is the subject of the investigation or prosecution, as well as a brief description of the related facts;
   c) The computer data to be stored and its relation to the infringement;
   d) All available information to identify the person responsible for the computer data or the location of the computer system;
   e) The need for the preservation measure;
   f) The intention to submit a request for legal aid for the purpose of searching, seizing and disclosing the data.
3. In execution of a request from a competent foreign authority under the terms of the preceding paragraphs, the Public Prosecutor's Office or the judge, as the case may be, shall order whoever has availability or control of such data, namely a service provider, to preserve it.
4. Preservation may also be ordered by the Criminal Investigation Police upon authorization from the Public Prosecutor's Office or the judge, or when there is urgency or danger of delay, in which case the provisions of paragraph 4 of the previous article shall apply.
5. The preservation order specifies, under penalty of nullity:
   a) The nature of the data;
   b) If known, their origin and destination;
   c) The period of time for which the data must be preserved, up to a maximum of six months.
6. In compliance with a preservation order addressed to it, whoever has availability or control of such data, namely the service provider, shall immediately preserve the data in question for the specified period of time, protecting and preserving its integrity.
7. The Public Prosecutor's Office or the judge, as the case may be, or the Criminal Investigation Police, with their authorization, may order the measure to be renewed for periods subject to the limit provided for in paragraph 5(*c*), provided that the respective admissibility requirements met, up to a maximum of one year.
8. When the request for assistance referred to in paragraph 1 is submitted, the Public Prosecutor's Office or the judge, as the case may be, shall order the preservation of data until a final decision on the request has been adopted.
9. Data preserved under this article may only be provided:
   a) to the competent foreign judicial authority, in execution of the request for assistance referred to in paragraph 1, in the same way as they could be assisted in a similar domestic case under Articles 16 to 20;
   b) To the national authority that issued the preservation order, in the same terms as they could in a similar national case under Article 16.

10. The national authority to which, under the terms of the previous paragraph, traffic data identifying the service provider and the route through which the communication was made are communicated, shall promptly communicate them to the requesting foreign authority, in order to allow that authority to submit a new request for the expeditious preservation of computer data.

11. Paragraphs 1 and 2 shall apply *mutatis mutandis* to requests made by the Cape Verdean (sic) authorities to foreign authorities.

Article 26
Grounds for refusal

1. A request for the expeditious preservation or disclosure of computer data shall be refused when:
   a) the computer data concerned relate to a political offence or a related offence under Timor-Leste law, or
   b) Acts against the sovereignty, security, public order or other constitutionally defined interests of the Republic of Timor-Leste;
   c) The requesting third State does not offer adequate guarantees for the protection of personal data
2. A request for the expeditious preservation of computer data may also be refused where there are well-founded reasons to believe that the execution of a subsequent request for legal assistance for the purpose of searching for, seizing and disclosing such data will be refused on the grounds that the dual criminality requirement has not been met.

Article 27
Access to computer data in cooperation

1. In execution of a request from a competent foreign authority, the Public Prosecutor's Office or judge, as the case may be, may order the search, seizure and disclosure of computer data stored in a computer system located in Timor-Leste, relating to crimes provided for in article 14, when this is a situation in which the search and seizure would be admissible in a similar national case.
2. The public prosecutor or the judge shall order the search and seizure as quickly as possible when there is reason to believe that the computer data in question is particularly vulnerable to loss or modification or when rapid cooperation is provided for in an applicable international instrument.
3. The provisions of paragraph 1 shall apply *mutatis mutandis* to requests made by the Timorese authorities to foreign authorities.

Article 28
Cross-border access to computer data stored when publicly available or with consent

The competent foreign authorities may, without prior request to the Timorese authorities, respect the rules on the transfer of personal data:

   a) Access computer data stored in a computer system located in Timor-Leste, when publicly available;
   b) Receive or access, through a computer system located in its territory, computer data stored in Timor-Leste, with the legal and voluntary consent of a person legally authorized to disclose it.

Article 29
Interception of communications in international cooperation

1. In execution of a request from the competent foreign authority, a judge may authorize the interception of computer data transmissions carried out via a computer system located in Timor-Leste, provided that this is provided for in an international agreement, treaty or convention and that it is a situation in which such interception is admissible, under the terms of article 21, in a similar national case.
2. The Criminal Investigation Police is responsible for receiving requests for interception and will submit them to the Public Prosecutor's Office, which will present them to the competent judge at the Judicial Court of First Instance for authorization.
3. The authorization referred to in the preceding paragraph shall also permit the immediate transmission of the communication to the requesting State, if this procedure is provided for in the international agreement, treaty or convention on the basis of which the request is made.
4. The provisions of paragraph 1 shall apply *mutatis mutandis* to requests made by the Timorese judicial authorities to foreign authorities.

CHAPTER V
Final and transitional provisions

Article 30
Application of Timor-Leste criminal law and jurisdiction of Timorese courts

1. In addition to the provisions of the Penal Code regarding the application of Timor-Leste criminal law in space, and unless there is a treaty or international convention to the contrary, for the purposes of this law Timor-Leste criminal law shall also apply to facts:
   a) Committed by Timor-Leste, if the criminal law of any other state does not apply to them;
   b) Committed for the benefit of legal persons based in Timorese territory;
   c) Physically committed in Timorese territory, even if they target computer systems located outside that territory;
   d) That target computer systems located in Timorese territory, regardless of where the acts are physically committed;
   e) Committed by Timor-Leste or a foreigner who is in Timor-Leste territory or moves to or is found there.
2. If, depending on the applicability of Timorese criminal law, Timorese courts and foreign courts have simultaneous jurisdiction over one of the crimes provided for in this law, and criminal proceedings can be validly initiated or continued in either of them on the basis of the same facts, the competent judicial authority shall use the bodies and mechanisms provided for in the law on judicial cooperation in criminal matters to facilitate cooperation and coordination of the respective actions, in order to decide who initiates or continues proceedings against the perpetrators of the offense, with a view to the effectiveness of the criminal proceedings.
3. The decision to accept or transfer proceedings shall be taken by the competent judicial authority, taking into account the following elements in turn:
   a) The place where the offense was committed;
   b) The nationality of the perpetrator;
   c) The place where the perpetrator was found.

4. The general rules on court jurisdiction set out in the Code of Criminal Procedure shall apply to the crimes provided for in this law.
5. If there is any doubt as to which court territorial jurisdiction, namely because the place where the agent physically acted and the place where the computer system targeted by his action is physically installed do not coincide, jurisdiction shall lie with the court where the facts were first reported.

Article 31
General rules

In everything that does not contradict the provisions of this law, the provisions of the Penal Code, the Code of Criminal Procedure and Law no. 15/2011 of 26 October 2011 shall apply to the crimes, procedural measures and international cooperation in criminal matters provided for therein, respectively.

Article 32
Competence of the Criminal Investigation Police for international cooperation

The competence attributed by this law to the Criminal Investigation Police for the purposes of international cooperation in criminal matters provided for in this law is carried out by the organic unit responsible for investigating the crimes provided for in this law.

Article 33
Protection of personal data

The processing of personal data under this law is carried out in accordance with the provisions of specific legislation approved.

Article 34
Entry into force

This law comes into force 30 days after its publication.

Approved on ...

The President of the National Parliament,

Maria Fernanda Lay

Promulgated on ...

Publish it.

The President of the Republic,

José Manuel Ramos Horta