

SPAIN
NATIONAL REPORT *

Patricia Faraldo Cabana/ María de los Ángeles Catalina Benavente
Professor for Criminal Law, University of A Coruña/ Professor for Procedural
Law, University of Santiago de Compostela

(B) Jurisdictional issues

(1)(a) How does your country locate the place of the commission of a crime in cyberspace?

The relevant jurisdiction is always the one corresponding to the place where the crime was committed, according to article 14 of the Criminal Procedure Act. The territorial authority should be determined for each case based on the three known case law theories of the activity, the result and the ubiquity. When determining the authority of the Spanish courts for cyber crimes committed over the Internet, in which the geographical location of the place of commission is especially difficult to specify given the territorial dispersion of the majority of the elements of the crime (starting the criminal action, location of the servers, receipt and transmission of the information, damages caused to the victims, benefits obtained by the perpetrator), our case law accepts the theory of ubiquity to admit the jurisdiction of the Spanish courts when any substantial elements of the criminal activity (executive acts of the commission of the crime, resulting damages, benefits or profit of the perpetrators) have been committed in Spain. This theory is founded on the Agreement of the full court meeting in a non-adjudicatory session of the 2nd Division of the Supreme Court, adopted in its meeting of 3rd February 2005: “Principle of ubiquity. The crime is committed in all the jurisdictions in which any element of it was carried out. Consequently, the judge of any of these jurisdictions who was the first to initiate proceedings is, in theory, competent to preside over the preliminary investigation”.

Another problem concerning jurisdiction relates to the effects of the connection in behaviours that continuous crime or mass crime frequently include. If the crimes have been committed in different national territorial constituencies the rules of article 18 of the Criminal Procedure Act will be applicable.

(b) Does your national law consider it necessary and possible to locate the place where information and evidence is held? Where is the information that one can find on the web? Is it where the computer of the user is physically present? Is it there where the provider of the network has its (legal or factual) seat? Which provider? Or is it the place where the individual who made the data available? If these questions are not considered to be legally relevant, please state why.

Spanish law does not consider these questions to be relevant for determining the relevant jurisdiction. The relevant point is the place where the crime is committed, and the theory of ubiquity is used to determine this.

(2) Can cyber crime do without a determination of the locus delicti in your criminal justice system? Why (not)?

No. The *locus delicti* has to be determined to analyse the jurisdiction. However, the Spanish courts may deal with cyber crime committed outside the country in the following cases: article 23.2 (nationality: offences committed by Spaniards abroad, whenever a) the offence is punishable in the place where it was committed, unless, under an international agreement or a legislative instrument of an international

* Important notice: this text is the last original version of the national report sent by the author. The Review has not assured any editorial revision of it.

Organisation that Spain forms part of, this requisite is not necessary; b) the aggrieved party or the Public Prosecution Service file a complaint before the Spanish courts; c) the offender has not been acquitted, pardoned or convicted in the foreign country, or, in the latter case, has not served his sentence...), 23.3 (crimes committed abroad by non-nationals against national interests) and 23.4 of the Judiciary Act (universal jurisdiction, which is limited to cyber crimes concerning pornography and the corruption of minors and computer sabotage related to crimes of terrorism).

(3) Which jurisdictional rules apply to cyber crime like hate speech via internet, hacking, attacks on computer systems etc? If your state does not have jurisdiction over such offences, is that considered to be problematic?

The same rules will be applied that generally govern the determination of jurisdiction.

Spain has jurisdiction over the crimes mentioned under the conditions included in the response to question B2.

(4) Does your national law provide rules on the prevention or settlement of conflicts of jurisdiction? Is there any practice on it?

Spanish law stipulates that it is subject to the international or bilateral agreements signed by Spain. In all cases, as a member of Eurojust, it recognises the jurisdiction of the state courts which, exercising their jurisdiction based on good faith, and guaranteeing the defendants and victims the basic right of a fair trial, are found to have the best conditions for holding the trial, evaluating various elements: the conventional obligations between the countries involved, the nature and intrinsic seriousness of the crime, the place it was committed, the nationality of the perpetrator, the nationality of the victims, the national interests affected, the availability of evidence of the crime, place it was obtained and possibilities of detection and transmission, the residence or presence of the defendant, or his place of refuge or detention, the place where the witnesses and victims are, the priority based on the date the investigations commenced, the concordance of the official language of the court and the majority of the personal and documentary evidence and the convenience of the parties involved in the case. We must not forget that intervention from the European Union is limited to striving to detect the problem and adopting a consensual solution based on the goodwill of the states. The Spanish courts have no obligation not to hear matters of their jurisdiction in accordance with national rules.

(5) Can cyber crime do without jurisdictional principles in your criminal justice system, which would in essence mean that national criminal law is applicable universally? Should this be limited to certain crimes, or be conditional on the basis of a treaty?

No. In Spain it is not possible to do without jurisdictional principles.

The application of the principle of universal jurisdiction is justified for certain crimes based on the supranational nature of the legally protected right or if it is in the common interest of all the states to particularly protect specific legal rights or to prevent impunity, but not because the crime was committed over the Internet. With regards cyber crime, in Spain the principle of universal jurisdiction is limited to crimes concerning pornography and the corruption of minors and computer sabotage related to crimes of terrorism.

(C) Substantive criminal law and sanctions

Which cyber crime offences under your national criminal justice system do you consider to have a transnational dimension?

All of them.

To what extent do definitions of cyber crime offences contain jurisdictional elements?

Definitions of cyber crime offences do not contain jurisdictional elements, with the exception of the crime of child pornography trafficking (article 189.1 b) Criminal Code), which states that it does not matter whether the material “originated abroad or if this is unknown”.

To what extent do general part rules on commission, conspiracy or any other form of participation contain jurisdictional elements?

General part rules on commission, conspiracy or any other form of participation do not contain jurisdictional elements.

Do you consider cyber crime offences a matter that a state can regulate on its own? If so, please state how a state may do that. If not, please state why it cannot do that.

I consider cyber crime offences a matter that a state can regulate on its own. Although many of them do have a transnational dimension, this is not always the case. Most of them have only a national dimension. They are planned and executed within the national territory, and the use of new technologies does not pose a problem for determining the place the crime was committed or for identifying the criminal.

Does your national criminal code provide for criminal responsibility for (international) corporations/ providers? Does the attribution of responsibility have any jurisdictional implications?

Legal entities can be found criminally responsible in Spain, regardless of their nationality (article 31 *bis* Criminal Code). Internet service providers usually adopt the legal nature of a corporation. Legal entities are subject to criminal responsibility when their legal representatives and administrators in fact or in law, or those subject to their authority, are able to commit cyber crimes because the due control is not upheld over them, as stipulated by law. This occurs in the following cases: illicit access to data and computer programmes (article 197.3); scams, computer fraud and inappropriate use of credit or debit cards, or travellers’ cheques, or the data registered on any of them (article 251 *bis*); computer damages, deletions or alterations (article 264.4); offences relating to intellectual and industrial property, to the market and consumers, and private corruption (article 288); receiving and laundering assets (article 302.2); and the falsification of credit and debit cards and travellers’ cheques (article 399 *bis* Criminal Code).

Having said this, we must mention the difficulties that exist with regards obtaining information on servers or the cessation of their activity when there is no relevant legislation on the matter in the host country, and the same thing occurs when identifying IPs and obtaining data from files downloaded using P2P networks.

(D) Cooperation in criminal matters

To what extent do specificities of information technology change the nature of mutual assistance?

The specificities of information technology change the nature of mutual assistance when they allow a Spanish judge to obtain investigative tools or to directly

examine the evidence as a consequence of using new technologies and thanks to the facilities offered by the requested state.

(2)(a) Does your country provide for the interception of (wireless) telecommunication? Under which conditions?

The legal system in force in Spain concerning the interception of electronic or computer communications is stipulated in article 18 of the Spanish Constitution (hereinafter the SC), in articles 579 and following of the Criminal Procedure Act, and in Act 25/2007, of 18th October, on the Retention of Data Relating to Electronic Communications and Public Communications Networks. This legal framework is insufficient.

Article 18.3 of the SC guarantees the privacy of communications, and especially that of postal, telegraphic and telephone communications, except in the case of a court order. It does not mention electronic communications, which is perhaps logical due to when the SC was enacted, although doctrine and case law both take the line that as a supplement article 18 of the SC should include electronic communications. Therefore, doctrine understands that although article 18.3 of the SC refers “especially” to a specific type of communications (postal, telegraphic and telephone communications), this protection should also cover all private personal communications, whatever method is used for them (fax, modem, digital communications, etc.), and regardless of whether they are sent using public or private servers.

The regulations stipulated in the Criminal Procedure Act are completely insufficient. The interception of telephone calls is regulated in two paragraphs of article 579, and the interception system for electronic communications is not mentioned.

Although the legislator has not yet addressed the extremely urgent amendment to the law on this matter, in the field of sectoral regulation and special procedural regulation steps have been made in this area, driven in many cases by the European Union. This regulation does not cover the proceedings and guarantees of the interception of communications, but rather the requisites, tools and obligations of a technical nature that allow or enable effective interception in an area that involves private operators, and in which there was no specific clarity regarding the legal basis of the data and formats that allow for monitoring the communication. With regards this issue, essentially focussing on guaranteeing the balance between the duty to maintain the privacy of communications and retain the data of these communications that may be used to identify the parties involved and for the “traceability” of the communication, we must mention, firstly, the provisions of article 33 of Act 32/2003, State Telecommunications Act.

With regards the regulation of the technical aspects that allow for effective interception of electronic and digital communications, we must note the advance made by the new provisions included in Act 25/2007, of 18th October, on the Retention of Data Relating to Electronic Communications and Public Communications Networks. This Act has incorporated into Spanish legislation the provisions of Directive 2006/24/EC of the European Parliament and of the Council, of 15th March, on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks. And the articles of this Act cover the legal system relating to the obligation of retention and disclosure of the data generated or processed by the operators in charge of providing public communications networks or electronic communications services.

To sum up, our criminal justice system guarantees the privacy of electronic communications, which include (under Act 25/2007) communication by fixed-line and

mobile telephony (with all its different versions), Internet access and browsing, the use of electronic mail along with its versions of simultaneous communication (chats) and telephony via the Internet. Article 579 of the Criminal Procedure Act is applicable, with all the interpretive baggage provided by case law, and with its suitability questioned under the doctrine of the European Court of Human Rights and of the Constitutional Court.

(b) To what extent is it relevant that a provider or a satellite may be located outside the borders of the country?

It is not relevant.

(c) Does your national law provide for mutual legal assistance concerning interception of telecommunication? Did your country conclude international conventions on it?

Telecommunication interception or intervention, along with the searches in a closed space and corporate interventions, have in common the fact that they are all procedures that restrict rights, therefore under domestic law they are usually subject to a special regime. National law establishes mutual legal assistance concerning the intervention of telecommunications under the application of the Convention on mutual assistance in criminal matters between the Member States of the European Union, enacted in Brussels on 29th May 2000 (published in the Official State Journal number 247 of 15th October 2003), modifying the combination of the Convention of 1959 and the Convention implementing the Schengen Agreement, adding new rules and repealing others. Other conventions do not contain express provisions on the interception of telecommunications.

Conventions on legal assistance concerning the interception of telecommunications signed by Spain. These are bilateral agreements of legal assistance and we can see the references to the interception of telecommunications.

1.- Bilateral Convention on legal assistance in criminal matters between the Kingdom of Spain and the People's Democratic Republic of Algeria, signed in Madrid on 7th October 2002.

The convention does not contain detailed regulations of this type of assistance. In this regard, the regulations refer to the generic provision and commitment contained in article 1 of the Treaty, under which the Parties agree to mutually grant each other, in line with the rules and conditions of the Treaty, legal assistance in all criminal matters, with article 1.2 referring to any form of assistance allowed by the legislation of the requested state.

2.- Treaty on extradition and international legal assistance between the Kingdom of Spain and Argentina, signed in Buenos Aires on 3rd March 1987.

This type of assistance is not mentioned specifically in the Treaty, but is understood to be included in the general expression of "investigative proceedings". Assistance is provided for any criminal proceedings brought about for events that concern the requesting Party at the time the assistance is requested. Similarly, with regards the rule referring to searches, as this is a restriction of basic rights it must be understood that the request is also made for the relevant criminal act to be considered an offence under the legislation of the requested Party (double criminality).

3.- Treaty on mutual assistance in criminal matters between the Kingdom of Spain and Australia, signed on 3rd July 1989.

This type of assistance is not defined specifically in the Treaty, but is understood to be included in the general expression of “carrying out investigative acts”.

4.- Convention on legal assistance in criminal matters between the Kingdom of Spain and the Republic of Bolivia signed «ad referendum» in La Paz on 16th March 1998.

This type of assistance is not defined specifically in the Treaty, but is understood to be included in the general clauses under which the Parties agree to mutually provide “all possible legal assistance in any criminal matter”, and this assistance will cover, as well as the specified matters, “any other form of assistance that is allowed under the legislation of the requested state”.

5.- Convention on legal assistance in criminal matters and extradition between Spain and the Socialist Federal Republic of Yugoslavia, signed in Belgrade on 8th July 1980.

The Treaty does not contain any specific provisions although it could be included in the provisions of articles 13 (searches and seizure of objects) and 14 (letters rogatory relating to criminal proceedings). This must be reciprocal. Assistance cannot be given unless the act is punishable under the legislation of the requested party and if their Law allows it.

6.- Convention on legal cooperation and legal assistance in criminal matters between the Kingdom of Spain and the Federal Republic of Brazil, signed in Brasilia on 22nd May 2006.

This type of assistance is not defined specifically in the Convention, but is understood to be included in the expression “obtaining and examining evidence”, and by the fact that legal assistance is given as much as possible in all proceedings concerning offences that are to be punished, at the time when the assistance is requested, by the jurisdiction of the legal authorities or by the Public Prosecution Service of the requesting party.

7.- Convention between the Kingdom of Spain and the Republic of Cape Verde regarding legal assistance in criminal matters, signed «ad referendum» in Madrid on 20th March 2007.

The convention does not contain detailed regulations of this type of assistance. In this regard, the regulations refer to the generic provision and commitment contained in article 1 of the Convention, under which the Parties agree to mutually grant each other, in line with the rules and conditions of the Convention, as much legal assistance as possible in all criminal matters. It is advisable to consider the limitations imposed specifically for registration requests.

8.- Treaty on mutual assistance in criminal matters between the Kingdom of Spain and Canada, signed in Madrid on 4th July 1994.

This type of assistance is not defined specifically in the Treaty, but is understood to be included in the expression “investigations or proceedings relating to any offence...” and by the fact that the treaty explicitly states that “as much legal assistance as possible will be mutually provided for criminal matters”.

9.- Treaty on extradition and legal assistance in criminal matters between the Kingdom of Spain and the Republic of Chile, signed in Santiago on 14th April 1992.

This type of assistance is not defined specifically in the Treaty, but is understood to be included in the expression "executing investigations and proceedings related to any criminal precept". And by the fact that assistance is provided in criminal proceedings arising from the legal authorities or from the Public Prosecution Service of the requesting party in the form of investigative acts.

10.- Treaty on legal assistance in criminal matters between the Kingdom of Spain and the People's Republic of China, signed in Peking on 21st July 2005.

Requests concerning these matters are defined in articles 1 and 2. Assistance may be denied if the act is not an offence under the legislation of the requested party, although the required assistance may be given at their discretion.

11.- Convention on legal cooperation in criminal matters between the Kingdom of Spain and the Republic of Colombia, signed in Bogota on 29th May 1997.

Requests concerning these matters are eligible under the terms of articles 1 and 3. Although the Convention does not contain explicit provisions on this matter, requests for investigative proceedings may be admitted based on the general formula of "any form of assistance that is not prohibited by the legislation of the requested state".

12.- Treaty on extradition held between Spain and the Republic of Cuba on 26th October 1905.

Although the convention has the main objective of regulating extradition, article 14 considers specific activities of criminal legal assistance, such as executing investigative proceedings or acts in general.

13.- Treaty on extradition and legal assistance in criminal matters between Spain and the Dominican Republic, signed in Madrid on 4th May 1981.

Requests of this kind are defined in article 26.

14.- Convention on legal cooperation in criminal matters between the Kingdom of Spain and the Republic of El Salvador, signed «ad referendum» in Madrid on 10th March 1997.

This type of assistance is not defined specifically in the Convention, but is understood to be included in the definitions contained in articles 1.2 and article 3. i), when it is stated that: "the parties shall provide mutual assistance, in accordance with the rulings of this Convention and in strict compliance with their respective legal systems for investigating crimes and cooperating in legal processes related to criminal matters." and "any other form of assistance in accordance with the purposes of this Convention provided it is not incompatible with the laws of the requested state".

15.- Treaty on mutual legal assistance in criminal matters between the Kingdom of Spain and the United States of America, signed in Washington on 20th November 1990.

The interception of telecommunications is not listed explicitly in the possible purposes of assistance included in article 1.2 of the Treaty. However, it is understood to be included under point b) "providing documents, records and evidence" or in the final closure clause "any other form of assistance that is not prohibited under the legislation of the requested state".

16.- Treaty on legal assistance in criminal matters between the Kingdom of Spain and the Republic of the Philippines, signed in Manila on 2nd March 2004.

The convention does not contain detailed regulations of this type of assistance. In this regard, the regulations refer to the generic provision and commitment contained in article 1 of the Treaty, under which the Parties agree, in accordance with the terms of the treaty, to provide as much legal assistance as possible in any proceedings regarding crimes for which the prosecution corresponds to the legal authorities of the requesting state; and, specifically, when the assistance is not prohibited under the laws of the requested state (article 1.2j).

17.- Treaty on extradition between Spain and Guatemala, signed in Guatemala on 7th November 1895.

Although the main objective of the convention is to regulate extradition, article 19 defines specific activities of criminal legal assistance, such as gathering incriminating evidence. It is a treaty of the 19th century, therefore it does not consider this type of measures, but it is the only useful instrument for this type of requests as it establishes the generic possibility of “gathering incriminating evidence”.

18.- Agreement on legal assistance in criminal matters between the Kingdom of Spain and the Republic of India, signed in New Delhi on 3rd July 2006.

Material scope: Mutual legal assistance in criminal matters, to the greatest extent possible.

19.- Treaty on extradition between Spain and the Republic of Liberia, signed in Madrid on 12th December 1894.

Although the main objective of the convention is to regulate extradition, article 18 includes specific activities of criminal legal assistance, such as taking statements or other acts of legal investigation. It is a treaty of the 19th century, therefore it does not consider this type of measures, but it is the only useful instrument for this type of requests.

20.- Convention between the Kingdom of Spain and the Kingdom of Morocco concerning legal assistance in criminal matters, signed in Rabat on 24th June 2009

The convention refers, generally, to providing the legal assistance “as much as possible”: • In criminal matters; • In civil actions resulting from criminal actions, while no final judgement has been passed regarding the criminal act (attachment of civil liability resulting from the crime or offence); • In investigative and notification proceedings regarding the enforcement of sentences or safety measures (although not in the actual enforcement itself).

21.- Convention on legal assistance in criminal matters between the Kingdom of Spain and the Islamic Republic of Mauritania, signed on 12th September 2006.

It is not explicitly defined in this Convention, although it may be requested if the requested state deems that it has no negative effect on its sovereignty, its safety or its public order.

22.- Treaty on Mutual Legal Assistance in criminal matters between the Kingdom of Spain and the United Mexican States, signed in Las Palmas de Gran Canaria on 29th September 2006.

Given that it is not explicitly defined in this Treaty, there may be some reluctance to consider it included in the general provision of “investigative actions”, even though in

article 1 the contracting states are obliged to provide as much legal assistance as possible.

23.- Treaty on Extradition between Spain and Monaco, signed in Madrid on 3rd April 1882.

Although the main objective of the convention is to regulate extradition, article 10 defines specific activities of criminal legal assistance, such as issuing incriminating evidence. It is a treaty of the 19th century, therefore it does not consider this type of measures, but it is the only useful instrument for this type of requests as it establishes the generic possibility of gathering and issuing “incriminating evidence”.

24.- Convention on legal assistance and cooperation in criminal matters between the Kingdom of Spain and the Republic of Panama, signed «ad referendum» in Madrid on 19th October 1998.

Given that it is not explicitly defined in this Convention, there may be some reluctance to consider it included in the general provision of “investigative actions”, even though in article 1 the contracting states are obliged to provide as much legal cooperation as possible.

25.- Convention on legal cooperation in criminal matters between the Kingdom of Spain and the Republic of Paraguay, signed «ad referendum» in Asunción on 26th June 1999.

This type of assistance is not defined specifically in the Convention, but is understood to be included in the definitions contained in articles 1.2 and article 3. i), when it is stated that: “the two Parties shall mutually provide, in accordance with the rulings of this Convention, as much legal assistance as is possible, in all proceedings concerning offences that are to be punished, at the time when the assistance is requested, by the jurisdiction of the legal authorities of the Requesting Party.” and “any other form of assistance in accordance with the purposes of this Convention provided it is not incompatible with the laws of the requested state”.

26.- Treaty on Legal Assistance in Criminal Matters between the Kingdom of Spain and the Republic of Peru, signed «ad referendum» in Madrid on 8th November 2000.

This type of assistance is not defined specifically in the Convention, but is understood to be included in the statements contained in article 1, referring to the “obligation to provide mutual legal assistance”, and in which it states that: “1. Under the terms of this Treaty the Contracting Parties shall provide as much mutual legal assistance in criminal matters as is possible. 2. Mutual legal assistance is understood to be all aid granted by the requested state concerning the investigations or proceedings regarding criminal matters that are executed in the requesting state. 3. Criminal matters are understood to be investigations or proceedings related to any offence covered by criminal law. 4. Criminal matters include investigations or proceedings relating to criminal infringements of a law of a fiscal, tariff or customs nature.” And in section 5, as a final closure clause, it establishes that the legal assistance will cover particularly, among other things, “1) the provision of other assistance compatible with the objectives of this Treaty”.

27.- Convention on legal assistance in criminal matters between the Kingdom of Spain and the Republic of Tunisia, signed in Tunis on 24th September 2001.

This type of assistance is not defined specifically in the Convention but is understood to be included in the mutual provision of legal assistance in any criminal proceedings.

28.- Treaty on mutual legal assistance in criminal matters between the Kingdom of Spain and the Oriental Republic of Uruguay, signed in Montevideo on 19th November 1991.

The requests relevant to this matter are contained in articles 1, 2, 13 and following.

(3) To what extent do general grounds for refusal apply concerning internet searches and other means to look into computers and networks located elsewhere?

The general grounds for refusal are also applicable concerning internet searches and other means to look into computers and networks located elsewhere, without exception.

(4) Is in your national law the double criminality requirement for cooperation justified in situations in which the perpetrator caused effects from a state in which the conduct was allowed into a state where the conduct is criminalised?

Cooperation is carried out under the terms of the conventions and treaties in which the general rule is that the cooperation does not require double criminality. In general, double criminality is not a requirement for cooperation under Spanish law.

(5) Does your national law allow for extraterritorial investigations? Under which conditions? Please answer both for the situation that your national law enforcement authorities need information as when foreign authorities need information available in your state.

Spanish law allows for extraterritorial investigations. Articles 4 to 11 of Act 11/2003, of 21st May, regulating the joint teams of criminal investigation within the European Union, establish the “constitution of a joint investigation team to act in Spain”. In turn, article 12 of the same act establishes the “constitution of a joint investigation team to act outside Spain”.

(6) Is self service (obtaining evidence in another state without asking permission) permitted? What conditions should be fulfilled in order to allow self service? Please differentiate for public and protected information. What is the (both active and passive) practice in your country?

Self service is not regulated in Spain. Nothing impedes self service regarding public information. With regards protected information, the conditions established by the requested state must be met and the guarantees defined for accessing the information must be observed.

The practice in Spain is unknown.

(7) If so, does this legislation also apply to searches to be performed on the publicly accessible web, or in computers located outside the country?

There is no limit with regards searching the publicly accessible web. However, if the computers are located outside the country they must be accessed under the conditions and observing the guarantees established by the requested state.

(8) Is your country a party to Passenger Name Record (PNR) (financial transactions, DNA-exchange, visa matters or similar) agreements? Please specify and state how the exchange of data is implemented into national law. Does your country have an on call unit that is staffed on a 24/7 basis to exchange data? Limit yourself to the issues relevant for the use of information for criminal investigation.

Spain is a party to all the existing agreements regarding this matter. For example, the Convention to step up cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration, signed in Prüm on 27th May 2005 (Treaty of Prüm). Data is exchanged in accordance with the provisions of the respective conventions or treaties, that are incorporated into national Law under the instrument of ratification.

Spain has a unit that is staffed on a 24/7 basis to exchange data, under the Interpol framework. The Spanish Interpol National Central Bureau (NCB) forms part of the National Police Force. It is structured in the following way: a Head Office, two Operational Sections (International Legal Cooperation and Police Cooperation) and a Technical and Support Section including the Secretariat and Department of Language Interpretation Services. Given that this Bureau deals with matters concerning police and legal cooperation on a global scale, the NCB in Madrid can respond to all the requests made relating to any investigation that is being carried out. There is also a Spanish office reporting to Eurojust, transmitting information concerning any investigation or legal proceedings within the framework of its authority.

(9) To what extent will data referred to in your answer to the previous question be exchanged for criminal investigation and on which legal basis? To what extent does the person involved have the possibility to prevent/ correct/ delete information? To what extent can this information be used as evidence? Does the law of your country allow for a Notice and Take-Down of a website containing illegal information? Is there a practice? Does the seat of the provider, owner of the site or any other foreign element play a role?

All the necessary data is exchanged on the legal basis formed by the instruments of ratification of the respective treaties and conventions.

The applicable law on data access, correction and deletion is Organic Act 15/1999, of 13th December, on Personal Data Protection. Regarding DNA data, Act 10/2007, of 8th October, is also in force, regulating the police database of identifiers obtained from DNA, which regulates the question in article 9. In practice, the data obtained during a criminal investigation is deleted once the affected person is acquitted or the criminal record is deleted. Until then, the information may be used as evidence provided it is irrefutable. If not, it can be used in the investigation but not as evidence in the trial, for which it will have to be repeated.

Act 34/2002, of 11th July, on Information Society Services and Electronic Commerce allows for Notice and Take-Down in relation to criminal investigations (art. 8). The Notice and Take-Down process can also be adopted as a precautionary measure while proceedings are ongoing.

The seat of the provider, owner of the site or any other foreign element plays an important role, since if the seat is in another country the mechanisms of police and legal cooperation must be called on to obtain information.

(10) Do you think an international enforcement system to implement decisions (e.g. internet banning orders or disqualifications) in the area of cyber crime is possible? Why (not)?

It is possible and desirable.

(11) Does your country allow for direct consultation of national or international databases containing information relevant for criminal investigations (without a request)?

Everything that allows public access may be consulted directly.

(12) Does your state participate in Interpol/ Europol/ Eurojust or any other supranational office dealing with the exchange of information? Under which conditions?

Spain participates in Interpol, Europol and Eurojust, as a full member with no reservations.

(E) Human rights concerns

Which human rights or constitutional norms are applicable in the context of criminal investigations using information technology?

All of them.

Is it for the determination of the applicable human rights rules relevant where the investigations are considered to have been conducted?

No.

How is the responsibility or accountability of your state involved in international cooperation regulated? Is your state for instance accountable for the use of information collected by another state in violation of international human rights standards?

The responsibility of the state is regulated by the conventions and treaties signed for this purpose. In the case of the European Union the responsibility of the state can be demanded before the European Union Court of Justice if there is a breach of the rules that require the transposition of community law.

Evidence that has been obtained by breaching basic rights cannot be used, regardless of which authority obtained it. The person the evidence is being used against may claim that the evidence is illegal in all cases, including before the Constitutional Court, and may appeal to the European Court of Human Rights.

(F) Future developments

Modern telecommunication creates the possibility of contacting accused, victims and witnesses directly over the border. Should this be allowed, and if so, under which conditions?

Videoconference and similar systems are allowed under article 229 of the Judiciary Act "*Ley Orgánica del Poder Judicial*" (hereinafter the LOPJ). Article 230 of the LOPJ allows the Courts and Tribunals to use any technical, electronic, computer and telematic means to develop their activity and perform their functions, with the restrictions in this usage established by Act 5/1992, of 29th October (law that has been repealed, and replaced by Act 15/1999, of 13th December, on Personal Data Protection), and other applicable laws.

The Criminal Procedure Act also allows this technique for carrying out investigative and evidentiary proceedings when its use is supported by utility, security or public order reasons (articles 325 and 731 *bis* of the Criminal Procedure Act). It is also established as an instrument of intervention of the prosecutor in proceedings before the examining judge (article 306 of the Criminal Procedure Act).

The Supreme Court understands that the possibilities of a trial via videoconference should be understood from a very restrictive approach with regards the non-intervention or non-attendance of the defendant at the trial. The High Court suggests two situations: The absolute impossibility of the defendant to attend the trial, as may occur in the case of serious illness, and their expulsion from the courtroom due

to severe public order disturbance, in which case videoconference would be useful so the defendant can follow the course of the trial from another room, as well as a means of giving statements.

If not, should the classical rules on mutual assistance be applied (request and answer) and why?

Is there any legal impediment under the law of your country to court hearings via the screen (Skype or other means) in transnational cases? If so which? If not, is there any practice?

There are no legal impediments but the Supreme Court is restrictive on this matter with regards the defendant.

Is there any other issue related to Information society and international criminal law which currently plays a role in your country and has not been brought up in all the questions before?

No.