Coloquio Preparatorio
Verona (Italia), 28-30 noviembre 2012
Sección I – Sociedad de la información y Derecho penal

SPAIN*

Fernando MIRÓ LLINARES[1]

B) Criminalization

(1) What specific juridical interests should be protected by criminal law (i.e., integrity of data processing systems, data privacy)?

Those crimes which fall within the category of cybercriminality generally protect individual interests directly such as privacy, wealth, or personal identity, but the ultimate reason for this classification is the indirect protection of cyber-security,a supra-individual macro interest which encapsulates all the diffuse interests without which secure communication is impossible in cyberspace. Within this global interest, we may differentiate security over particular systems; security of the data contained in them;and total control over identity and privacy.In all these cases we are dealing with interests in the sense of negative liberties: the right to total exclusion of third parties from the system, the data, or the identity.

(2) Please provide typical examples of relevant criminal laws:

All regulation of cybercriminality may be found in the Spanish Penal Code, which as recently as 2010 included an important reform which has clearly affected cybercrimes, that is, the modification of Arts. 264 and 197.3 to incorporate hacking or illicit system access.

In reality, many of the attacks pointed out by the AIDP (International Association of Penal Law) are penalized by these same criminal precepts. On occasion, nevertheless, such attacks are not punished in their totality, but only in part.

(a) Attacks against IT systems

Spanish Penal Code Art. 197.3. "Whoever, by any means or procedure and in breach of the security measures established to prevent it, obtains unauthorized access to computer data or programs within a computer system or part thereof, or who remains within it against the will of whoever has the lawful right to exclude him, shall be punished with a prison sentence of six months to two years."

Spanish Penal Code Art. 264.2. "Whoever, by any means, without authorization and in a serious way, hinders or interrupts operation of a computer system belonging to another by introducing, transmitting, damaging, erasing, degrading, altering, suppressing or making computer data inaccessible, when serious harm results, shall be punished, with a sentence of imprisonment of six months to three years."

---

* Atención: El texto que se publica constituye la última versión original del informe nacional enviado por el autor, sin revisión editorial por parte de la Revista.

[1] Profesor titular de Derecho penal de la Universidad Miguel Hernández.

In other words, unauthorized access to the system is punished in the same way as the act of impeding the system's activities by means of saturation: this is what is referred to as "hacking" in article 197.3 and "denial of service" in article 264.2.

(b) Invasion of IT privacy

Spanish Penal Code Art. 197. "1. Whoever, in order to discover the secrets or to breach the privacy of another, without his consent, seizes his papers, letters, electronic mail messages or any other documents or personal belongings, or intercepts his telecommunications or uses technical devices for listening, transmitting, recording or playing sound or image, or any other communication signal, shall be punished with imprisonment of one to four years and a fine of twelve to twenty- four months.

2. The same penalties shall be imposed upon whoever, without authorization, seizes, uses or alters, to the detriment of a third party, saved personal or family data that are recorded in computer, electronic or telematic files or media, or in any other kind of file or public or private record. The same penalties shall be imposed on whoever, without authorization, accesses these by any means, and whoever alters or uses them to the detriment of the owner of the data or a third party.

3. Whoever, by any means or procedure and in breach of the security measures established to prevent it, obtains unauthorized access to computer data or programs within a computer system or part thereof, or who remains within it against the will of whoever has the lawful right to exclude him, shall be punished with a prison sentence of six months to two years."

These penal categories are in a chapter that describes"Crimes against privacy," which implies that according to the courts'interpretation the data involved must be of an "intimate" or "private" nature. The regulations accordingly punish illicit seizure of information (Art. 197.1); theseizure, use, or modification of data contained in files to the detriment of a third party, as well as the access and alteration of such data (197.2); and finally, mere access to the system as a form of anticipatory prohibition of potential access to private data. (197.3)

(c) Falsehood, forgery and manipulation of digitally stored data

Spanish Penal Code Art. 197.2. 2. "The same penalties shall be imposed upon whoever, without authorization, seizes, uses or alters, to the detriment of a third party, saved personal or family data that are recorded in computer, electronic or telematic files or media, or in any other kind of file or public or private record. The same penalties shall be imposed on whoever, without authorization, accesses these by any means, and whoever alters or uses them to the detriment of the owner of the data or a third party."

Spanish Penal Code Art. 264.1. 1. "Whoever, by any means, without authorization and in a serious way, erases, damages, deteriorates, alters, suppresses, renders inaccessible data, computer programs or electronic documents belonging to others, resulting in serious harm, shall be punished with a sentence of imprisonment of six months to two years."

In the first provision, access, seizure, and modification of digitally stored data are punished; in the second provision, alteration of and damage to data are punished as long as the data has economic value.

(d) Dissemination of computer viruses

Spanish Penal Code Art. 264."1. Whoever, by any means, without authorization and in a serious way, erases, damages, degrades, alters, suppresses, or renders inaccessible data, computer programs or electronic documents belonging to others, resulting in serious harm, shall be punished with a sentence of imprisonment of six months to two years.

2. Whoever, by any means, without authorization and in a serious way, hinders or interrupts operation of a computer system belonging to another by introducing, transmitting, damaging, erasing, degrading, altering, suppressing or making computer data inaccessible, when serious harm results, shall be punished, with a sentence of imprisonment of six months to three years."

The dissemination of a virus as such is not prohibited in Spain. Causing economic damages by such means as Denial of Service attacks is prohibited, however, according to the provisions we have seen.

(e) Crimes related to users' virtual identities, e.g., forgery, theft, or damage to virtual personalities

In Spain the mere theft of or damage to a virtual identity is not a crime.

(f) Other innovative criminal prohibitions in the areas of information technology and the Internet, e.g., prohibitions on the creation and possession of certain virtual images,violation of authors' rights in the virtual sphere.

In addition to the provisions analyzed above, the Spanish Penal Code provides that crimes of child pornography (Art. 189), intellectual property (Art. 270), and computer fraud (Art. 248.2), as well as other cybercrimes such as online harassment in the form of slander, libel, and threats, may be punished criminally.

It is important to note the criminalization of online child grooming by the 2010 legislature in the new Art. 183 bis:

"Whoever uses the Internet, telephone or any other information and communication technology to contact a person under the age of thirteen years and proposes to meet that person in order to commit any of the offenses described in Articles 178 to 183 and 189, as long as such a solicitation is accompanied by material acts aimed at such an approach, shall be punished with a penalty of one to three years imprisonment or a fine of twelve to twenty-four months, without prejudice to the relevant penalties for the offenses actually committed. The penalties shall be imposed in the upper half when the approach is obtained by coercion, intimidation or deceit. "

But the greater innovation is still yet to come. On October 11, 2012, the Spanish Ministry of Justice announced a new reform of the Penal Code which, among other crimes, will include a new provision which will punish "with a penalty of three months to one year in prison or a fine of six to twelve months anyone who, without the authorization of the affected person, broadcasts, reveals or provides to a third party images or audiovisual recordings of the affected person that were obtained with his consent in a home or any other place out of the sight of third parties, when the revealing of such image seriously undermines the personal privacy of that person."

(3)How is criminal conduct (*actusreus*) typically defined in these crimes (describing the act, the result, other)?

(a) Attacks against IT systems

Penal Code Art. 264.2 describes the typical result, which is blocking or interrupting the functioning of another person's computer system. It also makes reference to conduct, which consists of introducing, transmitting, damaging, erasing, degrading, altering, suppressing, or rendering inaccessible computer information.

Moreover,Art. 197.3 describes the typical result, which is accessing without authorization data or computer programs contained in a computer system or in part of the system or remaining within the system. At the same time, this article makes reference to conduct, which is breaching security measures.

(b) Violation of IT privacy

Penal Code Art. 197 describes the typical result, which is illicit seizure of information (art. 197.1); seizing, utilizing, or modifying data contained in computer files, software, or hardware (Art. 197.2); or finally, accessing without authorization data or computer programs contained in a computer system or in part of the system or remaining within the system (Art. 197.3). This last section makes reference to conduct, which is breaching security measures.

(c) Falsehood, forgery and manipulation of digitally stored data

Penal Code Art. 197.2 describes the typical result, which is seizing, utilizing, or modifying data contained in computer files, software, or hardware, as well as accessing and altering such data.

Moreover, Art. 264.1 also describes the typical result, which is erasing, damaging, degrading, altering, suppressing, or making inaccessible data, computer programs, or electronic documents of others.

(d) Dissemination of computer viruses

Penal Code Art. 264.1 describes the typical result, which is erasing, damaging, degrading, altering, suppressing, or making inaccessible data, computer programs, or electronic documents of others. Article 264.2 also describes the typical result, which is blocking or interrupting the functioning of the computer system of another. It also makes reference to conduct, which consists of introducing, transmitting, damaging, erasing, degrading, altering, suppressing, or rendering inaccessible computer information.

(e) Crimes related to users' virtual identities, e.g., forging, theft, or damage to virtual personalities

In Spain the mere theft of or damage to a virtual identity is not a crime.

(f) Other innovative criminal prohibitions in the areas of information technology and the Internet, e.g., prohibitions on the creation and possession of certain virtual images,violation of authors' rights in the virtual sphere

In the crime of child pornography (Art. 189), conduct is described, which consists of recruiting or utilizing minors or disabled persons for exhibitionist or pornographic performances, whether public or private, or producing any type of pornographic material, on any platform; and possessing pornographic material in whose production minors or disabled

persons were used. For crimes related to intellectual property (Art. 270), the conduct consists of reproducing, plagiarizing, distributing or communicating publicly, in whole or in part, a literary, artistic, or scientific work, or its transformation, interpretation, or artistic execution based on any platform orcommunicated in any medium. In the crime of computer fraud (Art. 248.2.a), the conduct described is that of using computer manipulation or any similar artifice, but it also describes the typical result, which is transferring without consent any property to the detriment of another. In Art. 248.2 c), conduct is described, which is using credit or debit cards, travelers'cheques, or the data contained in any of them, but it also describes the typical result, which is carrying out any type of act to the detriment of the owner or a third party.Finally, for the crime of child grooming in Art. 183 bis, the typical result is described, which is contacting a minor under thirteen years of age and proposing an encounter with the goal of committing any of the crimes described in Arts. 178-183, as long as the proposal is accompanied by material acts connected to that goal.

How is the subject matter defined ("data,""writing,""content")?

There is no definition in criminal law of data, writings, nor information systems. General opinion of the doctrine is that we must look to the Council Framework Decision 2005/222/JHA, of February 24, 2005. Nor is there a definition of "falsehood forgery and manipulation of digitally stored data," nor of virus dissemination, etc.

(4) Is criminal responsibility for certain cybercrimes limited to certain groups of perpetrators and/or victims?

In the case of the crime of child pornography, criminal responsibility is limited to those cases in which the victims are minors; and in the case of child grooming to cases in which the victim is under thirteen years old. For the rest of the crimes there are no restrictions. In fact, crimes under Art. 264 that punish computer damage and Denial of Service attacks allow for punishment of juridical persons.

(5) Does criminal responsibility in the area of information technology extend to conduct that is merely reckless or negligent?

No. There is no type of reckless crime in information technology.

(6) Are there specific differences between the definition of cybercrimes and "traditional" crimes?

In the Spanish juridical-criminal framework, the categorization of cybercrimes occasionally relies on the creation of "result" crimes, including the drafting of "traditional" criminal paradigms, formulas such as "by any means," (Art. 189.1.b) or "communicated via any medium" (Art. 270 CP). On occasion we turn to the inclusion of formulas such as "whatever its basis" (Art. 189.1.a CP), or "on any basis" (Art. 270). In these cases the same punishment is consequently applied as for the traditional crime.

In other cases, a specific criminal category is created for the cybercrime, as occurs with computer damage (Art. 264.2), anticipated in a different article as the basic type of damage (Art. 263), or as also occurs with the crime of illicit access or hacking (Art. 197.3)

(C) Legislative drafting

(1) Are there specific problems with respect to the principal of legality (i.e., vagueness, open references from the penal category to other norms)?

As has been stated, there is no criminal definition of key elements such as the system or computer data, for which it is sufficient to refer to European regulations, such as the Council Framework Decision 2005/222/JHA, of February 24, 2005.

The principal problem, in any case, lies in the fact that the Spanish legislature has not created a cybercrimes chapter but has instead included them in existing chapters such as "crimes against privacy" or "crimes against property." This produces distortions in the judicial interpretation of the provisions, which leads to their not being applied as they should be from the perspective of criminal policy. For example, not every malware violation is punishable, only those that cause economic damages; and it remains doubtful whether illicit access that does not affect privacy can be punished underArt. 197.3 within this chapter.

(2) How does the legislation avoid undue chilling effects on the legitimate use of information technologies or the Internet?

In some instances, by restricting the definition of a crime to those cases in which serious harm results, as in the crime of damages ofArt. 264.2, and in others by restricting the legal description of the conduct to those cases in which it is carried out without the authorization of the legitimate owner of the property that is damaged, as in the crime of Art. 270.

(3) How does criminal legislation avoid the danger of becoming obsolete given rapid innovations? E.g.,

-how are changes in Internet use and social networks taken into account?

The Spanish legislature of recent decades is populist, punitivist, and reactive, legislating "straight from the headlines," which makes adequate response to the challenges of evolving technologies even more complicated. In matters of cybercrime, the definition of child grooming by reference to a penal paradigm that is impossible to apply is only one example. Recently, the dissemination of a video of a politician engaged in sexual acts has led to the explicit definition of broadcast of private images on the Internet.The legislature should instead develop a coherent, rational legislative policy on the need for protection in cyberspace.

- how does legislation adapt to technological progress (e.g., through reference to administrative norms)?

Curiously, the norms that regulate cybercrime are not "blank penal categories" and barely contain normative elements. Nor, in reality, is there sufficient administrative regulation of the Internet given that its decentralized nature means there can be no reference to what is "contrary to administrative law in cyberspace." Legislation adapts itself very poorly to technological progress; the most obvious change may be seen in the area of intellectual property, where the Spanish Penal Code only allows for punishment of the street distribution of physical copies and is barely adequate to respond to intellectual piracy for financial gain on the Internet.

(D) The reach of criminalization

(1) To what extent does criminal legislation reach mere preparatory acts that carry an underlying risk of abuse, e.g. acquisition or possession of software that may be used for hacking, "phishing," computer fraud, or bypassing firewalls?

Spanish legislation is fairly comprehensive in this sense. As was seen earlier, Art. 197.3 penalizes anyone who "by any means or procedure and in breach of the security measures established to prevent it, obtains unauthorized access to computer data or programs within a computer system or part thereof, or who remains within it against the will of whoever has the lawful right to exclude him, shall be punished with a prison sentence of six months to two years." Thus, hacking is penalized without requiring that data be seized. Of course, the law does not punish the preparatory act to hacking, that is the advance possession of software. On the other hand, related to fraud, Art. 248.2 b) penalizes "the manufacture, introduction, possession, or provision of computer programs intended to commit computer fraud and fraud through the use of credit or debit cards or travelers'cheques." In addition, Art. 270.3 also penalizes similar preparatory acts to crimes against intellectual property. Specifically, and carrying the same punishment as the corresponding crime,the law penalizes "whoever manufactures, imports, puts into circulation or possesses any means specifically intended to facilitate unauthorized suppression or neutralization of any technical device that has been used to protect computer programs or any of the other works, interpretations or performances under the terms foreseen in Section 1 of this Article shall also be punished with the same penalty."

If so, did the introduction of such laws cause controversy?

Yes, especially with relation to the punishment, which is the same as for completed acts, since this law has broken with the criteria normally followed by the Penal Code of punishing preparatory acts with a lighter punishment than the underlying crimes. In our view, this approach of punishing the attempt to commit a crime with the same penalty as the completed crime clearly violates the principle of proportionality.

Have there been specific legislative efforts to prevent overcriminalization?

Not only have there been no specific legislative efforts yet to prevent overcriminalization, the reforms of 2010 have increased the expansive tendency by incorporating the new Art. 248.2, the new Art. 264.2, the aforementioned Art. 197.3, and Art. 183 bis.

(2) To what extent is the mere possession of certain data considered incriminating? In what areas and on what basis?

Only the possession of child pornographic material (Art. 189.2) is punished with a penalty of three months to one year in prison or a fine of six months to two years, based on the protection of the sexual integrity of minors. At present it is not necessary to prove that possession will lead to later distribution.

How is "possession"of data defined? Does the definition include temporary possession of mere viewing?

The possession of child pornographic material implies an effective use of such material that excludes typical access to web pages containing pornography without downloading and saving them. Possession only exists if the file or document

is saved for later viewing. Nevertheless, in the next reform of the Penal Code this will be modified so that streaming will also be a crime.

(3) To the extent that possession or preferential access to certain data have been defined as infractions, does criminal responsibility extend to service providers (e.g, providers of web access or storage)?

In spite of an absence of jurisprudential unanimity, it still may be possible to extend criminal responsibility to service providers as defendants if it can be demonstrated that the service provider knew what was being undertaken and failed to halt the damage that was occurring. Thus, recently the Cáceres Provincial Court, in a May 16 decision, convicted the owner of a web page comments against the honor of the victims were posted as a perpetrator of an ongoing crime of defamation and libel with publicity. The reasoning of the opinion is particularly interesting: it points out in the conclusion that "as administrator of the forum the accused was its guarantor and responsible party, and therefore he had an obligation to monitor that comments on the forum were innocuous and not offensive to anyone,"from which the court concludes that the defendant knew of the defamatory messages being posted about the victims, and finds the decision not to provide the IP addresses of those leaving the defamatory and insulting messages to the police to be especially relevant, to the point of considering that "refusing to provide the identity of those who wrote in the forum was what made him responsible for the criminal act."

What are the requirements for their responsibility, especially as regards the subjective aspect (*mens rea*)?

To build a juridical basis of criminal responsibility for these intervenors, a central question is the establishment of at what point, when it comes to raising a duty in the ISPs, "effective knowledge" of the existence of illegal behavior exists. Focusing on the perhaps more relevant case of subjects who host websites and make illicit content available to third parties,Art. 16 of the Social Services Law establishes that the obligation to act diligently to remove data or block access to it arises only if providers have "effective knowledge that the activity or the stored information is illicit or causes damage to property or rights of a third party that are susceptible to indemnification," and the law adds that "it will be understood that the service provider has the effective knowledge referenced in paragraph a) when a competent body has declared the illicitness of the data, ordered that they be withdrawn or that access be blocked, declared the existence of damage, and the provider is aware of the correspondent resolution, without affecting the procedures and withdrawal of content applied by providers by virtue of voluntary accords and by other means of effective knowledge that may be established." This formula has given way to a debate between those (the majority of the doctrine and a large part of the jurisprudence until recently) who argue that effective knowledge should be restricted to the formal-judicial, and those who recognize that itis not the only possible way to acquire knowledge. The Supreme Court has placed itself in this line recently with decisions from December 9, 2009 ("Putasgae" case), May 18, 2010 ("Quejas online" case),and more recently in a decision from February 10, 2011 (Ramoncín case). In these cases the Court holds that it is possible to prove effective knowledge in the absence of a judicial declaration, specifically by means of communication effected by a victim or through other data that lead to explicit proof.Thus, the December 9, 2009 decision signals that knowledge obtained by the service provider "through facts or circumstances that may permit, even if mediated or through reasonable logical inference, an effective understanding of the reality at issue" seems to be enough to construe responsibility, as long as the provider has not acted

diligently to withdraw the content. In any case, it is necessary to clarify this doctrine so that it does not assume an obligation on the part of service providers "to evaluate the illicitness of everything on the Internet." What the High Court is saying, and I believe it is coherent within the normative framework, is that there are cases in which it is obvious that a communication really does constitute an infraction even in the absence of a formal judicial declaration, and that in those cases the service providers have an obligation to intervene.But below the level of the obvious, there will be a great number of cases in which the parties, the one who communicates and the one who is supposedly damaged, are not in agreement, and it would be erroneous and truly dangerous to attempt to turn service providers into interpreters of lawfulness with the ability to censor under the threat of legal responsibility if they are wrong.The philosophy of the LSSI (Law of Information Society Services) is constructed around the idea that the appropriate role for the service provider is to guarantee respect for legality *ex post*, but not *ex ante*, so that only in cases in which the infraction is self-evident, because it has been affirmed by a competent body or because it is obvious even without a formal declaration, must the provider cease the activity which allows the commission of the infraction.

Do providers have a duty to monitor and control the information they provide or to which they offer access?

No.

Do they have a duty to provide information about users' identities?

Only when ordered by a judge in relation to a criminal investigation.

Do they have a duty to block access to certain kinds of information?

Information within individuals' zone of privacy may not be revealed except by judicial order; as long as this is not the case, they have no duty to block access to such information.

If so, under what conditions and at what cost? Could the violation of these obligations result in criminal liability?

The act of revealing such information would constitute a crime of disclosure and revelation of secrets.

(4) What general, and specifically constitutional, limitations have been debated in the criminalization of conduct related to crimes connected with information technology and the Internet (e.g., freedom of expression, freedom of press, freedom of association, privacy, "principle of offensiveness," act requirement, not mere responsibility for the result (*mensrea* requirement))?

In relation to crimes of defamation and insults committed through the Internet, they have been objects of debate because of their conflict with the right to freedom of expression and also press because of the possibility of attributing responsibility to communications media or to service providers.

In relation to the crime of possession of child pornography, it has been the object of debate in connection with the complication of proving malice, as child pornography is often disguised by its circulation on the Internet.

(5) Does the law foresee criminal penalties aimed specifically at cybercriminals (e.g., bans or temporary suspensions of Internet use)?

No.

(E) Alternatives to criminalization

(1) What role does criminal law play in relation to other means of combatting abuse of information technology and the Internet?

It plays a very important role, as the majority of information technology-related behaviors that are made illicit are made so through juridical-criminal regulation.

(3) To what extent are IT users expected to apply means of self-protection (e.g., message encryption, use of passwords, use of protective software)?

To the extent that they wish.

Are any penalties foreseen for the failure to protect one's own computer up to a point, e.g., using anti-virus software or protecting private networks with passwords?

No.

Does the absence of reasonable self-protection presume a line of defense for those accused of illicit entry or illicit abuse of another person's network or data?

In connection with the crime of illicit access, the absence of reasonable protection provides a line of defense in a way since the crime of illicit access requires that it be undertaken by "violating security measures."

(F) Limits to anonymity

(1) Are there laws or regulations that compel internet providers to store users' personal data, including their internet use histories?

No.

May providers be compelled to provide that data to the police?

In the case that they have stored data, they may be obliged to provide that data to police if subject to a judicial order.

(2) Do laws or regulations compel internet service providers to register users before providing services?

No.

(3) Do laws or regulations limit encryption of files or messages on the Internet?

No.

May suspects be compelled to disclose their passwords?

No, because of the right against self-incrimination.

(G) Internationalization

(1) Does domestic law apply to data uploaded to the Internet from abroad?

Yes.

Is there a "double jeopardy"requirement for the entry of data from abroad?

No.

(2) To what extent has the criminal law of your country in the area of IT and Internet been influenced by international legalinstruments?

To a great extent, especially by European legal instruments, such as the Council Framework Decision 2005/222/JHA of February 24, 2005, relating to attacks on information systems, although also inspired bythe Budapest Convention of the Council of Europe.

(3) Does your country participate in debates on the harmonization of legislation related to cybercrimes (such as the UN group of intergovernmental experts on cybercrime)?

Yes, Spain does participate in meetings of cybercrime experts organized by the Conference of Ministers of Justice of Ibero-American Countries.

(H) Future developments

Describe, please, current lines of juridical and legislative debate in your country concerning Internet and IT crimes.

There are many ongoing debates. With respect to the classification of new crimes, the criminalization of cyberbullying, cyberstalking, identity theft, and other acts has been proposed. With respect to crime prevention, it seems clear that in cyberspace the conduct of the potential victim affects his future condition as a real victim, which means that we must improve the education of users, promote knowledge of the tools of protection, and redesign the duties of service providers.