TRANSNATIONAL CYBER CRIME, DIFFERENCES BETWEEN NATIONAL LAWS AND DEVELOPMENT OF EUROPEAN LEGISLATION: BY REPRESSION?

by

NADINA FOGGETTI*

Computer crime or cyber-crime, i.e. unlawful conduct committed over the Internet, is spilling over national borders and causing a huge legal headache, particularly in the matter of deciding which jurisdiction such crime should fall under. The law is not always prepared for meeting the demands of globalisation and new unlawful activities based on the illicit use of ICTs. The intrinsic cross-border character of this new type of crime also creates a need for improved cross-border law enforcement co-operation at European and international level.

As EU integration continues, the need for better coordination of criminal policies is accentuated. This is true in particular for the field of fight against cyber crime. There are different multinational projects to interconnect these policies. Despite the existence of organs and structure such as the Europol High Tech crime group, it cannot be claimed that an elaborated coherent horizontal policy in Europe on the fight against cyber crime exists. A continuing situation of uncoordinated policy in Europe would increase the problem by leading to fragmented anti cyber crime actions, a state of affairs which could potentially be exploited by criminals.

In this article we analyse, from the perspective of Italian and foreing criminal law a cross border cyber crime. The problem of cross border cyber crime reinforces the need to globalise the law and the way we respond to a problem that transcends national borders.

* PhD – University of Bari, Department of International law and UE law, nadinafoggetti@gmail. com.

KEYWORDS
Cyber crime, jurisdiction, CoE convention about cyber crime, transnational crime, Framework decision on Attack against Information System.

EUROPEAN LEGAL INSTRUMENTS IN THE FIGHT AGAINST CYBER CRIME [1]

The rapid development of Internet and other information system has given rise to a completely new economic sector and to new rapid flows of information, products and services across the internal and external borders of the EU. The new sector also contributes considerably to the economic growth in many areas in Europe. However, the same development has also opened many new possibilities for criminals. A pattern of new criminal activities against the Internet, or with the use of information systems as a criminal tool, is clearly discernible. These criminal activities are in permanent evolution and legislation and operational law enforcement have obvious difficulties in keeping pace. The intrinsic cross-border character of this new type of crime also creates a need for improved cross-border law enforcement co-operation.

All Member States have national policies against cyber crime or certain aspects of cyber crime. There are also different multinational projects to interconnect these policies. These projects often concern particular aspects of the problem area, such as the fight against child pornography or the fight against illegal trade.

There are also more relevant legal acts and instrument regarding the policy against cyber crimes at international and EU level.

The Council of Europe Convention[1] on cyber crime is no doubt the most important and comprehensive international instrument in this field, but its significance depends also on its application. About this specific problem, we can see that same States have not ratified the CoE Convention on 19 November 2007. The CoE Convention aims to facilitate international co-operation, detection, investigation and prosecution of cyber crime and calls for establishing a common basis for substantive and procedural law and for jurisdiction.

[1] CoE Convention on cyber crime, December 21, 2001. http://www.coe.int/

With respect to the CoE Convention, the Framework Decision (FD) on Attacks against Information Systems 2005/222/JHA[2] places emphasis rather on approximation of criminal law improving cooperation between judicial and other authorities, calling for the use of existing networks of operational points.

The FD on combat Child Pornography on Internet 2004/68/JHA[3] calls Member States to promote and facilitate investigation and prosecutions, to cooperate with Europol and Interpol and also to build up dialogues with the industry.

The Directive on Electronic Commerce 2000/31/EC[4] is important in relation to issues of responsibility as it excludes same obligations of network operators to monitor the information they transmit or store.

The Directive on Privacy and Electronic Communication 2002/58/EC,[5] besides containing provision on spam, envisages also an obligation for service providers to take measures to safeguard security and to inform users in case of particular risk or breach of security of the network. The Directive on the Retention of Data 2006/24/EC[6] is particularly relevant for the purpose of prevention, investigation, detection and prosecution of criminal offences as it ensures at EU level that certain data, in the course of the supply of communications services, are retained for a certain period of time.

As EU integration continues, the need for better coordination of criminal policy is accentuated. This is true in particular of the field of fight against cyber crime. A continuing situation of uncoordinated policies in Europe and the International law, would increase the problem by leading to fragmented anti cyber crime actions, a state of affairs which could potentially be exploited by criminals.

---

2 Framework decision, 2005-02-24, on Attacks against Information System, 2005/222/JHA, *Official Journal* L 69, 2005-03-16, p. 67.

3 Framework decision, 2004-01-20, on combat Child Pornography on Intenet, *Official Journal* L 13/44, 2004-01-20, p. 45.

4 Directive, 2000-06-08, on Certain Legal Aspects of Information Society Services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), in *Official Journal*, L 178, 2000-07-17, p. 34.

5 Directive, 2002-07-02, on Privacy and Electronic Communication, in *Official Journal* L 201, 2002-07-31, p. 45.

6 Directive, 2006-03-15, 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 Amending Directive 2002/58/EC, 2006/24/EC, in *Official Journal*, L 105 , 2006-04-13

The risk that criminal would exploit differences between Member States is even more concrete when it comes to differences in legislation. Criminals may choose to set up shop in a country in which a specific activity is punished more mildly or is not even criminalized.

JURISDICTIONAL PROBLEMS IN THE FIGHT AGAINST CYBER CRIME [2]

As a consequence of the technical evolution, criminals are now using fast networks allowing them to commit crimes over different national judicial territories in a very short period of time and also to eliminate evidence, just as quickly. Due to the across border nature of cyber crime, criminals can also easily obtain significant comparative advantages in relation to law enforcement authorities. Law enforcers also have the problem of getting used to continuous new forms of crime, of handling the increasing number of cases and of reacting quickly within the national jurisdiction as well as across other jurisdiction. In the field of the fight against cyber crime, there are relevant problems in order to determine the jurisdiction and the law enforceable.

A specific issue, in this field is the freedom of the States in international law to determine their jurisdiction to prescribe.[7]

Every State establishes the operativeness of its own jurisdiction to prescribe and it can expand the national jurisdiction by establishing other criteria, such as the principle of defence, the principle of criminal citizenship.[8] The changes of policy of legislative objectives, change highly influence the operation of national jurisdiction. The difference between the criteria of jurisdiction of the States determines positive and negative conflicts of jurisdiction.

It is therefore necessary to create uniform rules at the international level to encourage coordination between national courts and cooperation between States in the fight against transnational crime.

In the field of transnational cyber crimes, there are the CoE Convention and the FD. These instruments contain specific rules concerning the prob-

[7] Picotti, R.I. 1996, *La legge penale*, in Bricola-Zagrebelsky (a cura di), *Giurisprudenza sistematica del diritto penale*, Parte generale, I, Torino.

[8] Cfr. Woolsey, L.M. 1926, *Extraterritorial Crime*, in *American Journal Int. Law*, pp. 757-765; Chilstein, R.I. 2003, *Droit penal international et lois de polis: essai sur l'application dans l'espace du droit pénal accessoire*, Paris.

lem of jurisdiction. However there are more differences between these instruments.

The CoE Convention establishes a jurisdiction criterion that is based on the principle of territoriality.

Art. 22 of the CoE Convention states that:

"Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence … when the offence is committed in its territory".

There is no change compared with traditional principles. The most important principle is always the place in which the criminal has committed a crime: the principle of territoriality. The option chosen by the CoE Convention is not adequate in the fight against cyber crime.

The cross-border character of cyber crime makes it easy for criminal to move their activities from one state of another at short time. In fact it is very difficult to determinate the locus *committi delicti*.

It is possible, moreover, to note that in the CoE Convention there is an "opening clause".

Letter "d" in Art. 22 states that *"by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State"*. This article establishes the application of the principle of criminal citizenship as an alternative to the principle of territoriality. Its implementation is possible in two cases: if there is the respect of the principle of dual criminality. This condition is met if the conduct is punishable in application of the law of the State in which the fact has been committed and also in application of the law of the criminal citizenship.

The second case: this principle is applicable if there is a negative conflict of jurisdiction.

The jurisdictional criterion of the FD, conversely, are more adequate to the transnational nature of cyber crime. Article 10 of the FD, establishes that:

"Each Member State shall establish its jurisdiction … where the offence has been committed: a) in whole or in part within its territory; or b) by one of its nationals; or c) for the benefit of a legal person that has its head office in the territory of that Member State".

The FD chooses the principle of ubiquity, in fact it establishes jurisdiction of the State in which the offence has been committed in whole in its territory and also of the State in which it has been committed only in part within its territory.

The applicability of this principle is very important in the fight against cyber crime. The application of the principle of territoriality causes problems in the field of definition the competent jurisdiction.

There will be really risk of the negative jurisdictional conflict. This situation can produce a benefit for cyber crime.

The CoE Convention establishes in Art. "d" a rule for the resolution of the negative conflict of jurisdiction.

In this case in application of Art. 22 it is possible to enforce the principle of criminal citizenship. Art. 22 only partially solves the problem, because in order to apply it in national law, it is necessary that this principle is enforceable in the national law. In the cases of cyber crime, there is frequently a positive conflict of jurisdiction and many States claim jurisdiction over a same crime. The CoE Convention states, with regard to this problem, that:

> *"When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution".*

The CoE convention does not define uniform criteria in order to resolve the possible positive conflict of jurisdiction, unlike the FD on Attacks against information system. The FD, in fact, states that:

> *"Sequential account may be taken of the following factors: the Member State shall be that in the territory of which the offences have been committed according to paragraph 1(a) and paragraph 2, – the Member State shall be that of which the perpetrator is a national, – the Member State shall be that in which the perpetrator has been found".*

The FD, in fact, establishes that the State can use these criteria in order to resolve the positive conflict of jurisdiction. Each State must include these criteria in its national law.

The field of application and the addressees of two legal instruments, are different. The CoE Convention is universal, because it can be signed by all States, and not only by the States Members of the CoE.

Conversely, the FD is addressed to the Member States of EU. It is based on the mutual trust between Member States and also on the harmonization activity in this matter at EU level.

For this issue, the FD can produce more effects than those established in the Convention of the Council of Europe.

The difference between the jurisdiction criteria produces a lot of problems in the contest of the fight against cyber crime at international and national level.

The FD requires the Member States to modify their principles of jurisdiction in conformity with its norms while the other States must apply the Coe Convention about cyber crime.

This could cause two different consequences.

The States can bind a reserve about the jurisdiction rule (Art. 22). Secondly, if all States implement the CoE Convention, regarding the jurisdictional criteria, there is anyhow the problem of the difference between the jurisdiction rule of the Member States and those of the other States.

These differences enhance difficulties to prevent and prosecute crime.

A CASE OF CROSS-BORDER CYBER CRIME [3]

The case that we will analyse here can describe same problems concerning the fight against transnational cybercrimes.

In this particular case, the attacker violated a public interest system in Switzerland affecting Italian users connected to the compromised system. The attacker made use of a local vulnerability of the system thanks to which he modified his privileges from 'normal user' to 'root user'. In the end he has the power of the Swiss cluster of PCs.

Also, in this case the attacker went on to install a 'rootkit' which makes a Trojan-like attack. The software used was complex and included a 'sniffer' to copy the passwords keyed online on the violated system, and programmes which set up 'backdoors', in other words privileged access which, after the initial attack, can later be used to get back into the system. The 'rootkit' also contains tools to hide any trace of the attack, by altering the system commands which enable the intrusion to be verified, cancelling the activity logs.

The system compromised by the attacker is of 'public interest' since thousands of users from all over the world are connected to the system and

because experiments are conducted using the hardware and software resources located in Geneva. The system also hosts the necessary databases to conduct such experiments since they are essential for the purposes of scientific and technological research. There is also an e-mail service for registered users. Finally we know that the attack was launched from Geneva, the passwords belonged to Italian users who were connected to the violated computer system.

PASSWORD COPY AND THE PRINCIPLE OF TERRITORIALITY [4]
In the case we are studying here, the first problem is to determine if the Italian law can be applied.

To answer this question it is necessary to analyse the presupposition for the Territorial applicability of Italian Criminal law.

The principle of territoriality is dealt with in Art. 6, par. 1, of the ICC, which defines Criminal Law as being applicable within the whole of territory of the State. It is therefore essential to define where the offence was committed. The offence is considered to have been committed within the territory of the State, when the action or omission giving rise to the offence carried out fully or partially there, or if the consequence of the action or omission was suffered there.[9]

Our criminal code, therefore, aims to expand the jurisdiction of Italian Criminal Law by establishing a principle of ubiquity, raising the question of how to define the 'smallest part' of a criminal act that can cause the offence to be considered as committed in Italy. The resulting problem of interpretation has found no unanimous solution at a doctrinal level and also creates divergences in case law.[10]

Conversely, according to another criterion based on a literal interpretation of the norm, the offence should be considered as coming under Italian jurisdiction when only part of it, whether completed or attempted, has been committed in Italian territory, provided that the 'part' was an essential component of the offence. Such a decision must be taken after the event (*ex post*)

[9] Fiandaca & Musco, R.I. 1989, *Manuale di diritto penale*, Bologna.

[10] Cfr. Judgemnt of Corte di Cassazione, Sez. I, 1980-11-28, Cassazione Penale, 1982, p. 735; Judgement of Corte di Cassazione, Sez. III. 1984-11-27, Cassazione Penale, 1986, p. 476; Judgement of Corte di Cassazione, Sez. I, 1984-11-30, Giustizia Penale, 1985, vol II; Judgement of Corte di Cassazione, Sez. VI, 1988-01-19, Rivista Penale, 1989, p. 416.

and specifically, and not merely before the event (*ex ante*) and abstractly. Prevailing case law seems to accept this latter interpretation.

The jurisprudence would seem to accept the theory of the "potential commission of the deed". However, the same ruling continues with a restrictive interpretation requiring that "an attempted criminal act carried out in Italy must have some corresponding objective impact on the outside world".[11] The criterion of ubiquity is particularly applicable to offences committed over the Internet.[12]

The Italian Supreme Court of Appeal states that, on the basis of that principle, an Italian judge can try such an offence, either if it has been committed in national territory or if the *iter criminis* (crime route) initiated abroad has been completed with a crime committed in Italy. But in this case it is not applicable to Art. 6, because the attacker acted from Geneva, Suckit tools were installed on machines belonging to the Geneva's system, copying the passwords keyed in by the users who were connected to the violated system.

The fact that the passwords were keyed in by Italian users, from computers located in Italian territory, means that the 'minimum requirement' needed for Italian law to apply is not fulfilled. In this case, therefore, the principle of the 'territoriality' cannot be applied. In the case we are studying, however, for all the above reasons it is not Italian Criminal Law that can be applied but Swiss law, which we will analyse in the following sections.

THE INAPPLICABILITY OF THE CRIME WITH RESPECT TO THE PASSWORD COPY [4.1]

In this case it is necessary to analyse the concrete applicability of the crime of illegal access to a computer system (Art. 143-*bis* SCC) and of the crime of data theft (Art. 143 SCC).

Article 143-*bis* states that "Anyone, who without authorization, and without the intent of procuring an unlawful gain, accesses a data processing system which is specially protected against unauthorized access, by elec-

[11] Cass. Sez. III., January 10, 1961, *Cass. pen*., II, 811; for recent case law cfr. Cass. Sez. I, March 20, 1963, Rivista italiana diritto e procedura penale, 1965, p 118; Cass. Sez. IV, 1993-02-22, Giustizia penale, 1993, II, n. 517, 629.

[12] Picotti, L.M. 1999, *I profili penali delle comunicazioni illecite via internet, Diritto dell'informazione e dell'informatica*, p. 322-340.

tronic devices, shall be sentenced to imprisonment or fines". But in order to apply this article the system should be equipped with special security measures and there should not be any personal gain motive on the part of the offender. This article is applicable if the attacker has acted simply to "get to know" the violated system.[13] The absence of any personal gain motive on the part of the offender is an important feature of this new offence, although in early drafts the lack of any profit motive was merely a mitigating circumstance of the offence. Prevailing doctrine is of the opinion that if Art. 143-*bis* of the SCC does in fact define an abstract endangerment offence, this norm would not, however, be applicable in the case of concurrent circumstances making the offence punishable under Art. 143 of the SCC which, although this norm also provides for the concept of abstract endangerment, it also provides by law (*ex lege*) for specific intent, that is the intention to obtain gain either for the offender himself or for others. In the light of this interpretation, Art. 143-*bis* of the SCC takes on a role as a residual norm, applicable in those limited cases in which an attacker has acted with the purpose of simply breaking in to the computer system, without intending to do any damage or remove any of the data in the system. Article 143 of the SCC states: "Anyone, to give himself or others an undue profit, power of attorney, for himself or others, given he is not assigned and especially protected against non-authorized access, he records or transmits electronically or in a similar way, he is punished with confinement up to five years or with detainment". As we have seen, Art. 143 of the SCC criminalizes the unlawful acquisition of data. The systematic position of this article which is included among crimes against property, and the meaning of the French term "*soustraction*", have prompted doctrine to quietly interpret the term "acquisition" as having the same meaning as the French used in the legislative definition of the offence of theft referred to in Art. 139 of the SCC. According to the Swiss doctrine, in order to include the offence of "*soustraction des données*" it is essential that there be a theft ("*soustraction*" in the French text and "*wegnehmen*" in the German version) of the data, causing harm to the rightful owner. According to this approach, the mere fact of copying the data

[13] Schwbarth, R.I. 1990, *Kommentar zum Schweizerischen Strafrecht*, Bes. Tail., 2 Band; Trechsail, R.I. 1989, *Schweizerischs Strafgesetzvbuch* Kurkkommentar, Zurich.

does not in itself constitute an offence under Art. 143 of the SCC.[14] In this case, doctrine considers that Art. 143-*bis* could be applicable, provided that there is no intent to make any unlawful profit nor, therefore, any specific intent. In the light of the prevailing interpretation, it must be stressed that the abovementioned norm will only be applicable in the rarest of cases, since it is easily avoidable by the attacker, who can just copy the data – even with the purpose of unlawful gain – and still not be liable to be tried for any of the offences we have been studying. The fact that the attacker copied the passwords could be understood as fulfilling the requirement referred to in Art. 143 of the SCC. However the requirement of "material theft" of data from the violated system has not been met. For the conduct to be punishable, Swiss legislation also requires the offender to have acted with the purpose of obtaining an unlawful gain either for himself or for others. In the case we are studying, the intention of obtaining some gain cannot be proved and, if we wanted to interpret the norm in its broadest possible sense, by equating "the intent to damage" a system with the degree of harm caused by someone who acts with the intent to obtain an unlawful gain for himself or for others, we would be committing a violation of the principle of legality set out in Art. 1 of the SCC. When the attacker commits the offence with the intention of damaging or copying a system's data but the offender does not succeed in carrying out his criminal intent, it may give rise to doubts concerning whether the offence should be tried under Art. 143-*bis* of the SCC, as a completed offence, or under Art. 143 SCC, as a case of an attempted offence. The same Swiss doctrine considered the possibility of punishing under Art. 143 of the SCC anyone making an unauthorised access to a computer system simply in order to get an idea of its potential or its vulnerabilities, with the purpose of using this information to obtain for himself or others an unlawful gain. And also in this case there is a problem: if we apply art. 143-*bis* as a completed crime, the conduct does not turn out punished entirely. If we apply art. 143 as an attempted crime there is not the material theft of data.

In the case we are considering now, our attacker could be sentenced to arrest – certainly not for too long – if the Swiss magistracy opted to apply Art. 143-*bis* of the SCC. If the offence were deemed not to fall within the

[14] Strauffecher, *Infraction countre le patrimonie: le nuoveau droit*, cit., p. 14.

scope of application of that particular article, our attacker could take advantage of the diversity of possible punishments for the same offence under different judicial systems and would benefit from the criminal safe haven in which he had chosen to conduct his criminal activities.

If it was possible to apply Italian criminal law, it was possible to identify several different criminal activities and a concurrence of offences forming part of a single criminal act.

First of all the attacker has made an illegal access to a computer system, a conduct which is defined in Art. 615-ter of the Italian Criminal Code (ICC) and it carries a penalty from one to three years' imprisonment. In our case, the attacker in question had been granted the rights of a normal user, not those of a root user.[15] That represents, according to prevailing case law, the ius excludendi. This condition is necessary in order to enforce Art. 615-ter. According to this technical information, we can identify a second criminally punishable offence: when the attacker installed the 'rootkit', he would have been guilty of the conduct defined in Art. 617-quinquies of the ICC. The installation of the 'sniffer' programme, one of the components of the 'rootkit', allowed the attacker to capture the passwords of users connected from Italy, with the aim of ensuring the possibility of attacking more machines and extending the radius of action of the same unlawful conduct.[16] Art. 615-quater of the ICC defines the illicit possession of access codes to informatics and telematics systems as an offence, which is also applicable to the case we are studying. In order to charge the criminal responsibility of this offence it is not necessary to cause any actual damage to the system; the mere fact of having accessed some of the systems is sufficient. For cyber-crime it is not always feasible to identify the *locus commissi delicti* (the place where the offence was committed) when the offender makes use of informatics and telematic means to commit the offence.

---

[15] Cfr. Trentacapilli, L.M. 2002, *Accesso abusivo ad un sistema informatico e adeguatezza delle misure di protezione, Diritto Penale e Processo*, n. 10, p. 1280-1295; Nunziata, L.M. 1998, *La prima applicazione giurisprudenziale del delitto di accesso abusivo ad un sistema informatico – ex art. 615-ter, Nota alla sentenza del Trib. Torino, 7 febbraio 1998*, Giurisprudenza di merito, vol. II, p. 711-715; contrary Judgment of G.u.p. Trib. of Rome, 2000-04-21, www.penale.it

[16] Judgment of Corte di Cassazione penale, 2000-12-6, whit study of Galdieri, L.M. 2001, *L'introduzione contro la volontà del titolare fa scattare la responsabilità dell'hacker*, Diritto dell'informatica, vol. I, pp. 17-25.

CONCLUSIONS [5]

In conclusion it can be assumed that the CoE Convention on cyber crime does not resolve the problems concerning the jurisdiction, since it establishes the principle of territoriality. This criterion is not able to persecute and punish cases of cyber crime. The conclusion would be that many differences exist between legislation within the EU and at international level, and that this may cause a problematic situation. The intrinsic international and cross-border character of cyber crime is proof enough that actions are needed both at global international and at EU-level. Then the Commission is preparing a new general policy initiative, consisting of a Communication on the fight against cyber crime at EU level.[17] The option consisting of a coherent strategy on the fight against cyber crime has thus been chosen. The strategy will give the EU Commission a central coordinating role in Europe. With regard to its limited competence in this field, it is clear that the Commission will play this role only when a clear added value can be established. The concrete policy can be divided into four policy areas or instruments: improved European law enforcement cooperation; increased European public-private cooperation, improved international cooperation and specific legislation. In particular, in the field of international cooperation, the policy instrument aims at better coordinating EU actions against cyber crime with external and international initiatives. In fact, cyber crime in Europe is a phenomenon which may originate or have its effects far beyond the borders of the EU. A global approach is thus especially needed when it comes to the fight against this type of crime.

In conclusion, at EU level, it is necessary to see the evolution of the European Court of Justice in this specific matter. The judgment in Case C-176/03[18] Commission v. Council and the judgment in Case C-440/05[19] clarify the distribution of powers between the First and Third Pillars as regards provisions of criminal law. The Court of Justice had annulled the Council FD 2003/80/JHA on the protection of the environment through criminal law,

[17] Cfr. *Communication from the Commission to the European Parliament, the Council and the committee of the Regions, Towards a general policy on the fight against cyber crime*, of May 22, 2007, COM (2007) 267 final, http://europa.eu.

[18] Cfr. Judgment of European Court of Justice, of 2005-09-13 2005, *Commission v. Council*, C-176/03, http://www.curia.europa.eu/it/index.htm

[19] Cfr. Judgment of European Court of Justice of 2007-10-23, *Commission c. Council*, C-440/05, http://www.curia.europa.eu/it/index.htm.

which required the Member States to provide for criminal sanctions in the case of the offences against environmental law set out in the FD, on the grounds that the power to impose such an obligation on the Member States is a matter for a Community instrument and the Commission had in fact proposed the adoption of such an instrument. However, the judgment makes it clear that criminal law as such does not constitute a Community policy, since Community action in criminal matters may be based only on implicit powers associated with a specific legal basis. Hence, appropriate measures of criminal law can be adopted on a Community basis only at sectoral level and only on condition that there is a clear need to combat serious shortcomings in the implementation of the Community's objectives and to provide for criminal law measures to ensure the full effectiveness of a Community policy or the proper functioning of a freedom. From the point of view of subject matter, in addition to environmental protection the Court's reasoning can therefore be applied to all Community policies and freedoms which involve binding legislation with which criminal penalties should be associated in order to ensure their effectiveness. The Court makes no distinction according to the nature of the criminal law measures. Its approach is functional. The basis on which the Community legislature may provide for measures of criminal law is the necessity to ensure that Community rules and regulations are complied with. When for a given sector, the Commission considers that criminal law measures are required in order to ensure that Community law is fully effective, these measures may, depending on the needs of the sector in question, include the actual principle of resorting to criminal penalties, the definition of the offence – that is, the constituent element of the offence – and, where appropriate the nature and level of the criminal penalties applicable, or other aspects relating to criminal law. It is the specific requirement of the Community policy or freedom in question which constitutes the link with the legal basis of the EC Treaty which provides the justification for such measures. Again it is on a case by case basis, depending on necessity, that the Commission will determine the degree of Community involvement in the criminal field, whilst giving priority as much as possible to horizontal measures not specific to the relevant sector. Although the Community legislature may use the criminal law to

achieve its objectives, it may do so only if two conditions – necessity[20] and consistency[21] – are met. As a result of the Court's judgment any FD are entirely or partly incorrect, since all or some of their provisions were adopted on the wrong legal basis. Since the wrong legal basis of the FD could, in some cases, undermine the national implementing legislation. There are several ways in which existing law can be rectified in the light of the judgment. One approach would be to review the existing instruments with the sole purpose of bringing them into line with the distribution of powers between the First and the Third Pillar as laid down in the Court judgment. In such a case, the Commission's proposals would not contain any provisions which differed in substance from those of the acts adopted, even where the Commission felt that these acts were not satisfactory. The FD on attacks against information system can be transfused in a directive and the EU law in this matter should be in measure to give a concrete and effective answer to the cyber crime.

In conclusion it is possible to note that the Lisbon Treaty establishes the complete comunitarization of the cooperation in criminal matter. In this context, in the future, the EU institutions will have the possibility to adopt legal instruments in measure to bring the national criminal law.

---

[20] Any use of measures of criminal law must be justified by the need to make the Community policy in question effective. In principle, responsibility for the proper application of Community law lies with the Member States. In some cases, however, it is necessary to direct the action of the Member States by specifying explicitly, the type of behaviour which constitutes a criminal offence and/or the type of penalties to be applied and/or other criminal-law measures appropriate to the area concerned. Checks must be carried out to establish necessity and the observance of the principles of subsidiary and proportionality at each of these stages.

[21] The criminal-law measures adopted at sectoral level on a Community basis must respect the overall consistency of the Union's system of criminal law, whether adopted on the basis of the first or the third pillar, to ensure that criminal provisions do not become fragmented and ill-matched. If a sector seems to require specific rules in order to implement the objectives of the EC Treaty, the relationship between these specific rules and the horizontal rules should if necessary be clarified. Care must also be taken to ensure that the Member States or the persons concerned are not required to comply with conflicting obligations. When using its right of initiative, the Commission will take the utmost care to ensure that this consistency is preserved. Parliament and the Council must also take account of this requirement in their own internal organisation.