Criminalizing attacks against information systems in the EU and the impact of the European legal instruments on the Greek legal order*

Maria Kaiafa-Gbandi#

1. Introduction

Admittedly, information technology has radically and irrevocably changed modern societies. In technologically advanced countries, information systems have infiltrated virtually every sector of social life to such an extent as to redefine both State and individual activities. Government, national defense, communications, transportation, health systems, education, and entertainment are but a few among many fields administered by the so-called "information society".[1] Personal computers on their part have affected the everyday lives of all citizens, as evidenced for instance in the widespread use of e-mail and the dissemination of information on the worldwide web.

The unprecedented economic and social changes brought about by these developments have rendered information systems –as well as the data circulated therein- fundamental interests worthy of protection. This only makes sense, given the implications of the potential abuse of an information system: a mere click of the mouse can cause massive power outages, cancel out copious scientific efforts, and even bring about nuclear holocaust through the breach of information systems running nuclear reactors.

---

* The present article is a redacted and updated version of a paper published in the European Journal of Crime, Criminal Law and Criminal Justice 2011/1.

Prof. Dr. Maria Kaiafa-Gbandi, Law Faculty, Aristotle University Thessaloniki.

1 See indicatively *St. Furnell* (2012), Cybercrime – Vandalizing the information society, 1 ff., *M. Gercke,* Herausforderungen bei der Bekämpfung der Internetkriminalität, in *M. Gercke*, and *Ph. Brunst* (2017), Praxishandbuch Internetstrafrecht, 7-9; *cf*. the Explanatory Report to the Cybercrime Convention by the Council of Europe, paras. 1-6.

Without a doubt, this dark side of the use of information systems might be the single most important challenge information society has to face.[2]

It soon became clear that the applications of information technology had to be accompanied by pertinent regulation.[3] As far back as the '80 s, a number of legal orders recognized information systems as fundamental interests worthy of protection, and adopted criminal law rules to proscribe their breach.[4]

The rapid growth of the worldwide web has made it palpable that the impact of criminal conduct against information systems is unrestrained by national or geographic boundaries, hence ringing an alarm for the international community.[5] Considering that malicious viruses can be unleashed from anywhere in the world, no viable solution can be achieved in the absence of international cooperation[6]. This is especially true of a supranational organization like the E.U., which aspires to establish a common area of freedom, security and justice (articles 67 and 82 *et seq*. TFEU) also by addressing serious crime with a cross-border dimension (article 83, par. 1

---

2 *Cf*. the analysis of *M. Sieber*, Computer crimes, cyber-terrorism, child pornography and financial crimes, in Spinellis D. (ed.) (2004), Computer crimes, cyber-terrorism, child pornography and financial crimes, 14 ff.; *P. Jougleux, L. Mitrou,* and *T. Synodinou*, Criminalization of attacks against information systems, in I. Iglezakis (ed.) (2016), The Legal Regulation of Cyber Attacks, 34; *T. Politis, Ph. Kozyris,* and *I. Iglezakis* (eds.) (2009), Socioeconomic and Legal Implications of Electronic Intrusion; *J. Martin-Ramirez* (2017), Cyberspace, 141ff. On the socioeconomic background of cybercrime see indicatively *M. Karyda*, The socioeconomic background of cybercrime, in D. Politis, Ph. Kozyris and I. Igrlezakis (eds.) (2009), Socioeconomic and Legal Implications of Electronic Intrusion, 1ff.

3 For a survey of pertinent developments through time see, inter alia, *M. Kaiafa-Gbandi* (2007), Criminal law and abuses of information technologies [in Greek], Arm, 1059, with further citations.

4 Articles 370ter and 370^{quater} were introduced into the Greek Criminal Code in 1988, while German law had incorporated similar provisions by virtue of a statute dated 15.5.1986 (Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität – 2. WiKG). For an interesting recent comparative study on criminalizing cyber aiding see *T. Zhang* (2017), A comparative study on sanction system of cyber aider from perspectives of German and Chinese criminal law, Computer Law and Security Review 33, 98ff.

5 See the Explanatory Report to the Cybercrime Convention, paras. 5-6, and *M. Gercke* (2010), Impact of the Lisbon Treaty on Fighting Cybercrime in the EU, CRi, 75.

6 *K.-L. Hui, S.-H. Kim,* and *Q.–H. Wang* (2017), Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks, MIS Quarterly (41:2), 497ff.

TFEU),[7] including cybercrime. Besides, the approximation of domestic criminal law in this field is the first step towards achieving harmonized approaches in the field of procedural law, as well as facilitating judicial cooperation.

It becomes evident that, when it comes to the criminal law protection of information systems, European and international initiatives become central, as they largely determine the position of national legislatures.

2. The European and international institutional framework concerning attacks against information systems

2.1. A comparative survey of a complex framework

The Council of Europe Convention on Cybercrime holds a central position on the international plane.[8] The said convention requires State-parties to proscribe not only *stricto sensu* computer crimes[9] –i.e. those posing a direct threat to information systems and digital data- but also other types of crime perpetrated by means of a computer (such as computer fraud), including content-related crime (such as child pornography). Despite its flaws,[10] the Convention on Cybercrime has thus emerged as the most com-

---

7 On the pertinent competence of the E.U. see indicatively *M. Kaiafa-Gbandi* (2011), European criminal law and the Lisbon Treaty [in Greek], 29 ff.

8 See CETS No. 185, Budapest, 23.XI.2001, in force 1.7.2004.

9 On the distinction between genuine and non-genuine computer crimes see *Kaiafa-Gbandi* (2007), Arm, 1062. On the distinctions drawn in the field of computer crime in general see *D. Kioupes*, Combating computer crime in the European Union [in Greek], in Piraeus Bar Association – Hellenic Criminal Bar Association – Center of International, European and Economic Law, Contemporary developments in European Economic Criminal Law (2010), 191 ff.

10 With respect to matters pertaining to fundamental rights, personal data, and procedural rights see, inter alia, *P. Breyer* (2001), Die Cyber-Crime-Konvention des Europarats, DuD, 600, *A. Dix* (2001), Regelungsdefizite der Cyber-Crime-Konvention und der E-TKÜV, DuD, 588 ff., *D. Kugelmann* (2001), Die Cyber-Crime Konvention des Europarates, DuD, 222 ff., *id.* (2002), Völkerrechtliche Mindeststandards für die Strafverfolgung im Cyberspace-Die Cyber-crime Konvention des Europarates, TMR, 21 ff., *Br. Valerius* (2004), Der Weg zu einem sicheren Internet?, K&R, 517-518; with respect to substantive criminal law see *I. Carr*, and *K. Williams* (2002), Draft Cyber-Crime Convention, Criminalization and the Council of Europe (Draft) Convention on Cyber-Crime, Computer Law & Security Report, 83 ff.

prehensive instrument in the international fight against cybercrime,[11] owing in part to its provisions on procedure and judicial cooperation.

Although the E.U. itself is not a signatory party to the Convention, all of its member States have signed it, while most of them have already ratified it. In fact, the European Commission "actively encouraged" the member States to ratify the Convention as soon as possible,[12] despite the adoption of a framework-decision on attacks against information systems in 2005,[13] which has been replaced by a pertinent directive, owing to the novel institutional framework introduced by the Lisbon Treaty.[14]

States which happen to be members of both the Council Europe and the E.U. are therefore faced with the dual challenge of harmonizing their domestic law to the Convention on Cybercrime and the directive alike.[15] Yet the E.U. might not realistically dispense with the need of proposing a legal instrument of its own by merely becoming a party to the Council of Europe Convention. This is because a supranational organization such as the E.U. is in a much better position to bind its member States to follow its decisions; in addition, it can expand the proscribed types of conduct, ad-

---

11 See, e.g., *P. Csonka* (2000), The draft Council of Europe Convention on Cyber-Crime: A Response to the Challenge of Crime in the Age of the Internet?, Computer Law & Security Report, 329, *M. Gercke* (2004), Die Cybercrime-Konvention des Europarates, CR, 782 ff., esp. at 786, *id.* (2004), Analyse des Umsetzungsbedarfs der Cybercrime-Konvention, MMR, 728, *id.* (2006), The Slow Wake of A Global Approach Against Cybercrime – The potential of the Council of Europe Convention on Cybercrime as international model law, CRi, 144-145, *H. Kaspersen* (2001), Council of Europe's Cybercrime Convention, in ERA, Cybercrime: Developing the legal Framework in Europe-Documentation, London, 11-12.11.2010.

12 See Directive 2013/40/EU preamble sect. 15.

13 2005/222/JHA, 24.2.2005, OJ L 69 of 16.3.2005, 68.

14 See Proposal for a Directive of the European Parliament and of the Council on Attacks against Information Systems, replacing Council Framework Decision 2005/222/JHA in COM (2010) 517 final, of 30.9.2010; *cf.* the Presidency's proposal to the Council 8795/11, DROIPEN 27-TELECOM 43- CODEC 609, of 8.4.2011 and Directive 2013/40/EU; also see *D. Brodowski* (2010), Strafrechtsrelevante Entwicklungen in der Europäischen Union-ein Überblick, ZIS, 753-754 and *Ph. Jougleux, L. Mitrou and T. Synodinou*, Criminalization of Attacks against Information Systems, in I. Iglezakis (ed.) (2016), The Legal Regulation of Cyber Attacks, 25ff..

15 *Cf. F. Sanchez-Hermosilla* (2003), Neues Strafrecht für den Kampf gegen Computerkriminalität- Konvention des Europarates und neuer Rahmenbeschluss der Europäischen Union im Vergleich mit dem deutschen Strafrecht, CR, 774 ff.

just the applicable rules to correspond to ever-evolving needs, and determine not only "what" will be punished but also "how" it will be punished.[16] In doing so, it is to keep an eye open for initiatives by the Council of Europe affecting its member States, so that it may align its actions accordingly.

It follows that States like Greece or Germany, i.e. EU Member States, had better subscribe to a comparative approach, starting from the E.U. directive, while keeping in mind the Council of Europe Convention on Cybercrime.

2.2. The reasons for the E.U. directive and the core questions arising in a comparative context

On September 30, 2010, the Commission came up with a proposed directive on attacks against information systems, aiming at replacing the existing framework-decision 2005/222/JHA.[17] Less than one year before, the Lisbon Treaty had come into effect, by virtue of which the E.U. was granted the authority to establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension based on the principle of majority (article 83, par. 1 TFEU).[18]

The declared reason for this initiative was "emerging threats highlighted by recent attacks across Europe since the adoption of the framework decision, in particular the emergence of large-scale simultaneous attacks against information systems and the increased criminal use of the so-

16 On the competence of the E.U. in the field of substantive criminal law after the Lisbon Treaty see *Kaiafa-Gbandi* (2011), European criminal law and the Lisbon Treaty [in Greek], 28-34.

17 See pertinently *S. Bier* (2005), Kampf gegen die Cyberkriminalität, Der Rahmenbeschluss 2005/222/JI des Rates der EU über Angriffe auf Informationssysteme, DuD, 473 ff.

18 It is noteworthy that the TFEU (article 83, par. 1) explicitly enumerates computer crime among types of crime with a cross-border dimension triggering the E.U.'s competence to establish minimum rules in the field of criminal law. In fact, the term 'computer crime' was deliberately chosen to cover a broder array of cases compared to 'cybercrime' as provided in the Council of Europe Convention: see *Gercke* (2010), CRi, 79.

called 'botnets'".[19] These factors, which emerged after the framework decision had been adopted, prompted the Commission to seek more effective ways of addressing the threat. According to the Commission, "the main cause of cybercrime is the vulnerability of information systems resulting from a variety of factors, while insufficient response by law enforcement mechanisms contributes to the prevalence of these phenomena, and exacerbates the difficulties, as certain types of offences go beyond national borders. Furthermore, variations in national criminal law and procedure may give rise to differences in investigation and prosecution, leading to differences in how these crimes are dealt with. Developments in information technology have exacerbated these problems by making it easier to produce and distribute tools ('malware' and 'botnets'), while offering offenders anonymity and dispersing responsibility across jurisdictions."[20] In this new environment, the Commission has attempted to formulate its proposal,[21] taking into account novel forms of cybercrime, including the use of botnets.[22]

The EU directive explicitly relies on the Council of Europe Convention on Cybercrime and it poses three core questions:

(i) How are criminal law provisions to be delineated to address attacks against information systems?
(ii) What is the relationship between the E.U. directive with the pertinent provisions of the Council of Europe Convention on Cybercrime?

---

19 COM (2010) 517 final, 30.9.2010, 2 and Directive 2013/40/EY preamble sect. 5.
20 *Ibid*., at 3.
21 The need for further measures to combat cybercrime has been highlighted by the Commission in the context of the Stockholm Program (and the pertinent action plan); moreover, the digital agenda drafted in the framework of the "Europe 2020" strategy features new forms of crime –and especially cybercrime- as its first item: see COM (2010) 517 final, 30.9.2010, 4. *Cf.* the opinion of Europol member *N. Dileone*, Cybercrime: Developing the legal framework in Europe, in ERA, Cybercrime: Developing the legal framework in Europe – Documentation, London, 11-12.11.2010, and Commissioner *R. Jansky*, EU legislative and non-legislative instruments against cybercrime, in ERA, Cybercrime: Developing the legal framework in Europe – Documentation, London, 11-12.11.2010.
22 On 'botnets' and the dangers inherent in their use see COM (2010) 517 final, 30.9.2010, 3-4.

(iii) Last but not least, what is the underlying foundation of the choices made in this directive, placed in the context of fundamental principles of European criminal law after the Lisbon Treaty?[23]

2.3. A comparative survey of the criminal law rules on attacks against information systems on a European and international level

2.3.1. An initial approach

As already noted, the EU proceeded to a new directive on attacks against information systems, because it deemed the existing framework decision deficient in terms of addressing the full array of cybercrime, safeguarding against large-scale attacks, and providing for adequate sanctions.[24]

Specifically, the directive requires member States to proscribe two additional types of conduct (in line with the Council of Europe Convention), namely the illegal interception of computer data (article 6) and the production, sale etc. of tools used for committing computer offenses (article 7), in addition to the ones already covered (illegal access to information systems – article 3; illegal system interference – article 4; illegal data interference – article 5). Even with regard to conduct already covered by the replaced framework decision, the directive introduces changes pertaining to incitement, aiding and abetting, attempt (article 8), and especially applicable penalties (articles 9 to 12), including aggravating circumstances (article 9 paras 3 and 4). In terms of procedural matters, the directive introduces provisions on jurisdiction (article 12), as well as exchange of information (article 13), requiring member States to ensure that they have procedures in place so that in urgent requests they can indicate within a maximum of 8 hours at least whether the request for help will be answered. At the same time, the directive requires the establishment of a system for the recording, production and provision of statistical data on the offences referred to in articles 3 to 7 (article 14).

---

23 See pertinently *European Criminal Policy Initiative* (ECPI) (2009), A Manifesto on European Criminal Policy, ZIS, 707 ff.; *cf. Chr. Mylonopoulos* (2011), European Criminal Law after the Lisbon Treaty: The legitimization of European Criminal Law and the importance of criminal law doctrine for its shaping, PChr, 86-87.

24 See COM (2010) 517 final, 30.9.2010, 4.

2.3.2. Proscribed types of conduct

Starting with the types of conduct already provided for in the replaced framework decision, it is to be noted that the directive does not expand the ambit of *illegal access to information systems*, as contrary to the relevant Commission's proposal it recognizes each member State's discretion to confine the proscribed conduct to situations where the offense is committed by infringing a security measure.

The directive goes even further than the Council of Europe Convention, which allowed some margin of discretion to member States under article 2, just like the framework decision. In fact, the Convention not only allows States to exclude offenses not committed by infringing security measures or are unrelated to a computer system that is connected to another computer system, but also permits them to narrow criminal liability through the introduction of subjective elements, such as requiring 'dishonest intent'. In reality, the Council of Europe was attempting to exclude conduct which does not pose any threat whatsoever to information systems, especially when it might reveal some of their weaknesses.[25] Hence, it left State parties the choice of determining for themselves whether to subscribe to a broad or narrow version of criminalization of cybercrime.

One might counter argue that the same discretion is reserved for member States under the directive, which requires criminalization in "cases which are not minor".[26] However, this would be an erroneous assumption. Indeed, the same clause is to be found in the replaced framework decision 2005/222/JHA *alongside* a provision permitting member States to only criminalize conduct infringing a security measure, indicating that these are two distinct limitations. Notwithstanding the inherent ambiguity of the notion of "minor cases", it cannot be argued that every conduct not infringing a security measure is a minor one. Therefore, the possible exclusion of minor cases under the proposed directive cannot be said to fully coincide with the ambit of either the Council of Europe Convention or the replaced framework decision.

Besides, allowing States to introduce certain limitations is also in line with the requirement that criminal law be used as a last resort (*ultima ratio*

25 See the Explanatory Report by the Council of Europe, para. 49.
26 See, along these lines, *Brodowski* (2010), ZIS, 753.

principle),[27] particularly in view of the fact that efficient security measures could protect information systems much more efficiently than unrestrained criminalization.[28] In that sense, one can only applaud the directive having introduced the infringement of security measures as a requirement for the affirmation of illegal access to information systems.[29]

On the other hand, the provisions concerning illegal system interference (article 4) and illegal data interference (article 5) remain unchanged compared to the replaced framework decision. In addition, only minor discrepancies are traceable with the Council of Europe Convention in this respect. As regards *illegal system interference*, the directive calls for its criminalization "at least for cases which are not minor". That same limitation –albeit not contained in so many words under article 5 of the Council of Europe Convention- derives from the proscribed act itself, which alludes to "serious hindering" of a computer system, thereby rendering the exclusion of minor cases redundant. As regards *illegal data interference*, article 5 of the directive is not identical with article 4 of the Council of Europe Convention. The latter explicitly recognizes that State-parties may reserve the right to require that the conduct result in *serious harm*, while the directive again allows only for the exclusion of *minor* cases. In other words, the Council of Europe Convention also allows for the exclusion of offenses of *average* gravity, thus conceding that other measures, such as administrative sanctions, might be enough to address these.[30] Such choice shows respect for the *ultima ratio* principle,[31] entrusting the pertinent decision with each State-party.

With respect to the novel provision concerning *illegal interception of non-public transmissions of computer data by technical means* (appearing for the first time in an E.U. legal instrument), the Council of Europe Convention allows States to only criminalize conduct committed with dishonest intent or in relation to a computer system that is connected to another

---

27 On the application of this principle in European Criminal Law see *ECPI* (2010), at 707.

28 *Cf.* the Explanatory Report by the Council of Europe, para. 45; also see *Carr*, and *Williams* (2002), Computer Law and Security Report, 84.

29 See Art. 3 of the Directive 2013/40/EU.

30 See pertinently the Explanatory Report by the Council of Europe, paras. 64, 69.

31 For the importance of this principle on a European level see *M. Kaiafa-Gbandi* (2010), The importance of core principles of substantive criminal law for a European criminal policy respecting fundamental rights and the rule of law [in Greek], NoV, 2186 ff.

computer system. In contrast, the E.U. has left no such leeway, the only potential limitation emanating from article's 6 possibility to exclude minor cases. Aside from this deficiency, the directive does not even attempt to delimit the notion of 'interception', thus creating some ambiguity. Likewise, the Council of Europe Convention contains no definition of 'interception' either. That being noted, it should be emphasized that the institutional framework introduced under the Lisbon Treaty authorizes the E.U. to establish *minimum* rules concerning the definition of offenses, which inherently calls for unambiguous provisions, permitting an accurate transposition into domestic law.[32] Besides, a mere look at the explanatory report to the Convention on Cybercrime suffices to demonstrate the need for a comprehensive definition, as the Council of Europe interprets it so as to include, among other things, the monitoring or surveillance of the *content* of communications.[33]

The provision of the directive which marks an overly expansive tendency in the E.U. context is however article 7, requiring member States to criminalize "the production, sale, procurement for use, import, possession, distribution or otherwise making available of *a computer program, designed or adapted primarily for the purpose of committing any of the offences referred to in articles 3 to 6 or a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed*". There are two notable differences between this provision and the corresponding article 6 of the Council of Europe Convention.

The first difference is article 6, par. 2 of the Council of Europe Convention, which provides that the provision of paragraph 1 shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to therein is for the purpose of authorized testing or protection of a computer system. One might contend that such exception is superfluous, as the requisite intent of the offense could *per se* preclude conduct carried out for an authorized testing or protection of a computer system. However, given the fact that the proscribed conduct lies distant from

32 See *Kaiafa-Gbandi* (2010), NoV, 2196 ff.

33 See the Explanatory Report by the Council of Europe, para. 53. According to Kioupes [Combating computer crime in the European Union, *op. cit*., at 195], the interception of transmitted data constitutes a breach of what he terms as the victim's "digital domestic peace".

any actual harm to computer systems or data, the above clarification can only be regarded as a positive addition. Besides, article 6, par. 1 of the Cybercrime Convention allows State-parties to require by law a minimum number of tools in order for criminal liability to attach to their possession, a circumstance that is absent from the text of the directive.

Secondly, State-parties to the Council of Europe Convention are free to exclude certain types of conduct from criminalization under article 6, par. 1, provided that their reservations do not concern the sale, distribution or otherwise making available of the said devices. Again, one discerns a judicious choice by the Council of Europe,[34] which aims at confining criminalization to the *distribution* of potentially "threatening" means, such as passwords, which can guarantee access to an information system –or parts thereof- by their very nature. None among these limitations, which serve to exclude the use of devices for legitimate purposes from the ambit of criminalization, have been adopted by the E.U. As a result, criminalization largely depends on subjective criteria, which are hard to establish.[35]

Adding to the picture, two more elements of the E.U. directive point to the broadness of its ambit: first of all, member States are required to criminalize even aiding and abetting to the offense proscribed under article 7 (article 8, par. 1). Although this requirement is also present in the Council of Europe Convention (article 11), its effect is mitigated by the discretion granted to State-parties; secondly, member States are required to criminalize attempt without exceptions (article 8, par. 2), in stark contrast to both the replaced framework decision (exempting attempted illegal access to information systems under article 5, par. 3) and the Cybercrime Convention, recognizing the right of each State-party to not apply, in whole or in part, paragraph 2 concerning attempt (article 11, par. 2 and 3). On the other hand, the exclusion of the offense of articles 6 and 7 from the ambit of attempt is a positive step (one also taken by the Council of Europe Convention).

Last but not least, it is noteworthy that every offense proscribed under the directive is only punishable when committed "without right", an element also found in the replaced framework decision and the Council of Europe Convention. Although the Council of Europe Convention leaves

---

34 *Ibid*., at 72-78.

35 Even on a European level, criminalization needs to rely on a clear-cut affirmation of a fundamental interest which incurs serious damage by the act in question: see *ECPI* (2010), at 707.

the definition of this notion –hence the decision regarding the broadness of criminalization- to State-parties, article 2(d) of the directive defines it as meaning "access […] not authorized by the owner, other right holder of the system or of part of it, or not permitted under national legislation".[36] From a purely rule-of-law standpoint, such definition appears problematic, as it effectively allows the owner –especially in the case of a contract- to even unduly restrict the free flow of information,[37] which is absolutely essential in a democratic society, thus affecting the limits of the proscribed conduct.

2.3.3. Criminal sanctions

In the exercise of the E.U.'s recognized competence to establish minimum rules concerning penalties, the directive contains specific sentences to be imposed, going further than article 13 of the Cybercrime Convention, which is confined to declaring the need for effective, proportionate and dissuasive sanctions. In addition, there are demonstrable differences even compared to the replaced framework decision, leading to an overall strengthening of criminal repression.

Under the directive, member States shall specifically ensure that every offense mentioned above (i.e. even the preparatory acts proscribed in article 7) is punishable by criminal penalties of a maximum term of imprisonment of at least two years (article 9, par. 2).[38] Aside from undermining the principle of proportionality, such provision signifies that the E.U. leans towards inflexible sentences, as it distances itself from the replaced framework decision providing maximum terms of imprisonment in a more flexible fashion (e.g. a maximum term of at least 1 to 3 years). The principle of proportionality is clearly better served by the abolished provision, in terms of both meting out penalties for each offense and delimiting each particular sentence.[39] The wider the margin of discretion, the easier it becomes for member States to align each sentence to the corresponding gravity of the offense it attaches to. Adding to the picture, the directive introduces for the first time an inflexible minimum sentence for illegal access to in-

36 See the Explanatory Report by the Council of Europe, paras. 38 and 47.
37 See *Kaiafa-Gbandi* (2007), Arm, 1084.
38 See COM (2010) 517 final, 30.9.2010, 16.
39 See pertinently *ECPI* (2009), at 709.

formation systems. Overall, it becomes evident that the trend is now to establish more stringent penalties, while reducing the margin of discretion of member States in delimiting them.

The same reasoning has been applied under article 9 paras 3 and 4 of the directive. To begin with, the said provision expands the enumeration of aggravating circumstances so as to include commission by concealing the real identity of the perpetrator and causing prejudice to the rightful identity owner (par. 5), as well as through the use of a tool designed to launch attacks affecting a significant number of information systems (para 3), or attacks causing serious damage (par. 4), or commission against a critical infrastructure information system (par. 4).

2.3.4. Assessing the E.U. policy on criminalizing attacks against information systems in a comparative context

The above analysis of the rules concerning the criminalization of attacks against information systems as adopted by the Council of Europe and the E.U., respectively, allows us to draw a conclusion relying on the following elements:

In its effort to amend its regulatory framework concerning criminal repression of attacks against information systems, the E.U. did not pay enough heed to the *ultima ratio* principle. Such principle, which directly emanates from the principle of proportionality, is well-founded in E.U. law[40] and would protect against inhibiting technological innovation or blocking the free flow of information. Taking into account the numerous possibilities for restricting criminalization as mandated under the Council of Europe Convention, one would indeed expect the E.U. to strive for more balanced solutions in repressing cybercrime, especially after the Lisbon Treaty, which enables it to bind its member States–on grounds of majority vote- to minimum rules concerning the definition of offenses and criminal sanctions,[41] i.e. impose its own choices as to the distinction between those acts that deserve punishment and those that do not.

---

40 See *Kaiafa-Gbandi* (2010), NoV, 2187, at n. 29, *Mylonopoulos* (2010), European criminal law and general principles of E.U. law, PChr, 161.

41 On this requirement as it emerges after the Lisbon Treaty see *Kaiafa-Gbandi* (2010), NoV, 2187-2190.

A close look at the preamble of the E.U. directive reveals the actual reasons behind the choices made. Prominent among the grounds for adopting the directive is the need to fight organized crime and terrorism, and sec. 3 of the preamble notes the increasing concern about the potential for terrorist or politically motivated attacks against information systems which form part of the critical infrastructure of Member States and the Union. Interestingly, however, the repression of attacks against information systems carried out in the context of organized crime or terrorism would require nothing more than *special provisions* designed to address these acts, as opposed to a blanket extension of criminal law rules.

On the other hand, the directive neither ensures respect for fundamental rights recognized under the Charter of Fundamental Rights of the European Union nor observes Union law principles, despite the preamble's reassurance to the contrary (sec. 29). Indeed, the definitions contained in the proposal do not conform to the *lex certa* requirement, which is also applicable on a European level.[42] Two pertinent examples would be the ambiguous notion of 'interception', as well as the indeterminacy surrounding 'minor cases', which are to be excluded from criminalization.[43] The principle of proportionality[44] on its part is also undermined: How is proportionality respected, when the maximum sentence is doubled on the grounds of participation in a criminal organization, despite the fact that the latter is punishable *per se*? How can proportionality possibly be served, when member States are left with virtually no margin of discretion in determining applicable sentences, thus being deprived of any competence to introduce variations based on the harm caused to different legal interests within the particular context of their own legal order?[45]

Last but not least, there is a valid concern about broadly criminalizing preparatory acts, such as the production of tools employed to commit pertinent offenses. The problem is that the directive (just like the Council of Europe Convention) also proscribes tools that are not by their very nature designed for the sole purpose of attacking information systems. Coupled with the distance between these acts (i.e. the production or possession of such tools) and the actual attack, it becomes evident that criminalization of

---

42 See *ECPI* (2009), 707 ff., as well as *Kaiafa-Gbandi* (2010), NoV, 2190 ff.

43 *Cf. Brodowski* (2010), ZIS, 753.

44 See *ECPI* (2009), 707, *Kaiafa-Gbandi* (2010), NoV, 2183-2184, at n. 29, *Mylonopoulos*, (2010), PChr, 161.

45 On the principle of coherence see *ECPI* (2009), at 709.

this conduct is not associated with a tangible threat to information systems, thus risking punishment over one's mere intent.[46] The fact that the E.U. (unlike the Council of Europe) does not leave room for limitations in this field makes things even worse.

Such elements cause serious concerns in view of the transposition required by member States. Let us now examine as an example, i.e. what have been the implications for the Greek legal order based on the directive described above.

3. The EU directive on attacks against information systems and the Greek legal order: points of convergence and some pertinent problems

The directive made necessary both the amendment of existing provisions[47] and the introduction of new ones into Greek law[48].

First of all the Greek legislator introduced a definition of "information systems" and "computer data" under article 13 grCC, based on the ones

---

46 *Ibid.*, at 707. On the criminalization of preparatory acts in connection with attacks against information systems see *Kaiafa-Gbandi* (2007), Arm, 1085, and, more extensively, *K. Chatziioannou*, The criminalization of hacking tools as a reasonable measure of protection regarding attacks against information systems and computer data, in M. Bottis, Eug. Alexandropoulou, I. Iglezakis (eds.) (2013), Values and Freedoms in Modern Information Law and Ethics (Proccedings of the 4th International Conference of Information Law and Ethics), 123ff. Cf. also Q.-H. *Wang, L.-T. Zhang* and *M.-K. Qiao*, Online Hacker Forum Censorship: Would Banning the Bad Guys Attract Good Guys?, http://hdl.hendle.net/10125/41840.

47 About the former legal framework see indicatively*:E. Vassilakis* (1993), Combating computer crime [in Greek], 74ff.; *Kaiafa-Gbandi* (2007), Arm., 1064ff.; *D. Kioupes* (1999), Criminal Law and Internet [in Greek],, 131ff.; *Chr. Mylonopoulos* (1991), Computers and criminal law [in Greek],, 39ff.; *Th. Krithara,* Criminal Law and Internet [in Greek],; *G. Lazou* (2001), Informatics and Crime [in Greek],; *Chr. Tsouramani* (2005), Elektronic criminality: the unsafe side of Internet [in Greek],; *Spinellis D.* (ed.) (2004), Computer Crimes, Cyber Terrorism, Child Pornography and Financial Crimes: Reports Presented to the Preparatory Colloquy for the Round Table II of the 17th International Congress of Penal Law (Beijing, 2004).

48 Introduced by Law 4416/2016. For a brief description of the new legal framework see *E. Vagena* (2017), The new legal framework for combating Cybercrime [in Greek], PoinDik, 31ff.

contained in the directive and the Council of Europe Convention.[49] However, he/she did not introduce a *distinct chapter* in the Criminal Code on attacks against information systems, which would include already existing provisions, like e.g. article like 370C on illegal access to computer data (in its amended form). This would highlight the confidentiality, integrity and availability of information systems and data as a distinct fundamental interest worthy of protection by criminal law.[50]

On the contrary, the Greek legislator made the choice to introduce new provisions referring to illegal system and data interference, to illegal interception as well as to their preparatory acts (Art. 292B, 292C, 381A, 381B, 370D and 370E grCC), spread in different chapters of the Criminal Code and reformed the existing provision on illegal access to computer data (Art. 370C grCC). In this way, having made the wrong choice by the non-introduction of a new chapter, the legislator multiplied at the same time the problematic provision on preparatory acts, which has been included as well in all the different amended chapters that became new or amended provisions related to the attacks against information systems. On the other hand, the provisions on the levels of the penalties to be applied are higher than the ones provided for by the EU directive (something that occurs ad-

---

49 See article 2(a) of the directive according which 'information system' is defined as "any device or group of inter-connected or related devices, one or more of which, pursuant to a program, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of their operation, use, protection and maintenance". On the other hand, article 2(b) of the directive defines 'computer data' as "any representation of facts, information or concepts in a form suitable for processing in an information system, including a program suitable for causing an information system to perform a function".

50 See *Kaiafa-Gbandi* (2007), Arm, 1077-1078, noting that both computer systems and data have indeed been elevated to the status of fundamental interests worthy of protection. To the extent that such data is stored, are accessible and can be the object of ownership rights, criminal law ought to protect both their confidentiality (namely the owner's right to restrict access thereto), and their integrity and availability (namely the owner's right to retain them in any desired form and be able to use them at will). See also *E. Symeonidou-Kastanidou*, Attacks against information systems: the EU provisions for their repression and the Greek legal order [in Greek], in Legal Tech and Data Protection (4th Panhellenic Congress) (2013), 59, 69. On information as a fundamental interest worthy of legal protection see *E. Vassilakis*, Combating computer crime, 62 ff.; also see *G. Nouskales* (2004), The criminal law protection of digital information [in Greek], in *ENOVE*, Digital Technology and the Law, 120 ff.

mittedly quite often in the Greek legal order) and at the same time no exclusion of minor cases from criminalization is foreseen. In many cases, of course, the crimes according to the provisions introduced in the Greek criminal code can be prosecuted only after a complaint has been filed by the victim. This scheme is not excluding with certainty minor cases from criminalization, as the victim may still wish their prosecution and file a complaint, while it can also exclude e.g. cases of normal gravity, which the Union has not allowed Member States to leave out of the scope of punishment.

However, the most important problem that the Greek legal order now causes, relates to the incorporation of article 7 of the directive, proscribing the preparatory acts of production, sale, procurement for use, import, possession, distribution or otherwise making available of devices employed to commit any of the above offenses. The two issues which raise concern are the extent of criminalization and the penalty to be applied. To the extent the directive retains a blanket provision covering computer programs designed or adapted primarily to facilitate the commission of any of the offenses proscribed in the directive, the problem of excessive criminalization indeed remains. However, domestic law could have narrowed down its scope by appropriately delineating the notion of acting "without right", which is a necessary element under the directive.

One way to achieve this would be to introduce an additional element, namely that the production, sale, etc. of computer programs primarily designed to attack information systems (as described in article 7 of the directive) only be carried out upon obtaining a formal permit. Aside from contributing in putting together a list of software applications that pose a genuine threat to information systems (which would enable the outlawing of some of them), such addition would help keep tabs on those producing or selling these applications, thus rendering the lack of a permit as a formal element of the proscribed conduct. Accordingly, any person producing or selling them with permission would not incur criminal liability, at least not until launching an attempt against an actual information system. On the other hand, lack of a permit would not necessarily connote that the person is acting without a right; indeed, such right might derive from other exceptional circumstances precluding wrongfulness, such as a state of necessity or even self-defense.

In addition, domestic law should follow the example of article 6, par. 2 of the Council of Europe Convention and explicitly state that every act proscribed in article 7 of the directive is justified (even absent a permit), if

carried out for the purpose of authorized testing or protection of a computer system. Such a clause would not contradict the directive, as the latter indeed requires a special intent to commit crimes which is all but absent in the situations described above.

In point of fact, one might consolidate the two limitations into a clause exempting the procurement and possession for personal use of the applications in question by the authority issuing permits, providing that such procurement shall take place for the purpose of authorized testing or protection of a computer system in the context of personal or professional use.

Finally, it must be said that article 187, par. 1 grCC (concerning participation in a criminal organization) would have to be updated so as to include the purpose of committing felonies consisting in system or data interference. Should that amendment take place, there would be no actual need to introduce the aggravating circumstance encompassed under article 9 of the directive (i.e. in case the above acts are committed within the framework of a criminal organization), as the cumulative charges for participation in a criminal organization and illegal system or data interference would ensure aggravation of the penalty anyway.

4. Instead of a conclusion

The above analysis makes it plain that the task of EU member States in adopting criminal law rules within an international context focused on the repression of cross-border crime is not an easy one. In the post-Lisbon era, the Union's ability to bind its member States has been extended so as to allow it to not only establish minimum rules concerning the definition of offenses, but also determine minimum sentences. It therefore becomes imperative for national delegations –as well as parliaments themselves- to actively engage in the European lawmaking process, so that fundamental principles of criminal law are better served, and the EU may achieve its declared goal, i.e. place the individual at the heart of its activities.[51] At the same time, it is imperative for national legislators to be bold enough, to correct -in the framework of the possibilities the Union law offers to them- the handicaps a Union legal instrument may bear. Copying the Union legislator and serving unilaterally criminalization may, of course, cause less

51 See the Preamble to the E.U. Charter of Fundamental Rights.

problems towards the EU, but this is not an attitude that serves the evolution of justice in two-tier models of criminal law like the one of the EU, where the Union and the Member States are cooperating in the legislative process, having a shared responsibility for the result to be achieved, which needs to be a balanced one, not only offering protection to legal interests but at the same time safeguarding the citizens' freedoms.