SIMILARITY AND COMPETITION BETWEEN CYBERCRIMES RELATED TO COMPUTER DATA IN THE COUNCIL OF EUROPE'S CONVENTION ON CYBERCRIME

by

PEDRO DIAS VENÂNCIO*

The Council of Europe's Convention on Cybercrime provides four types of cybercrime for very similar acts on computer data: data interference, system interference, computer-related forgery and computer-related fraud. All these crimes criminalize acts that are in their objective factors materially identical, essentially: input, delete, damage or alteration of computer data. What really distinguish these cybercrimes are the protected legal interests, and therefore the damage potentially affected by them. Thus, integration of an identical behavior on one of these types of cybercrimes requires the evaluation of the technical effect produced. Since the difference in some cases may prove to be only in the intensity/extent of damage, the distinction is not always easy. On the other hand, this similarity makes it possible for one behavior to integrate the requirements of more than one cybercrime, which brings us to the question of potential competition or cumulating between them. Our communication will focus on the differentiation and possible cumulating of these cybercrimes under this Convention.

KEYWORDS

Cybercrime Convention; Computer-data related crimes; data interference; system interference, computer-related forgery; computer-related fraud

*Lecturer at Instituto Politécnico Cavado e do Ave, Barcelos, Portugal; pvenancio@ipca.pt

1 INTRODUCTION

This article is based on our communication at the 10th International Conference "Cyberspace 2012", Brno, Czech Republic, 30 November to 1 December, with some short adaptation. This study, more than solutions, intended to bring to this international colloquium a motto of discussion about the specifics that the Information Society brings to the Law and, in this case, crimes related to computer data. It is therefore an empirical analysis without pretensions of doctrinal depth, which explains the absence of citation of the authors of reference in this regard.

Our purpose in this communication is to discuss The Council of Europe's Convention on Cybercrime[1] measures for substantives crimes related to computer data, in particular the difficulties of interpretation raised by the similarity of the acts mentioned in the four types of cybercrime that are specifically related to computer data: *data interference* (article 4.), *system interference* (article 5.), *computer-related* forgery(article 7.) and *computer-related fraud* (article 8.).

All these crimes criminalize acts that are in their objective factors materially identical, essentially: input, delete, damage or alteration of computer data. As we will see on our communication, the protected legal interests and the damage potentially affected by them is what really distinguishes these cybercrimes. Or, in other words, the effects of the predicted acts. Thus, integration of an identical behavior on one of these types of cybercrimes requires the evaluation of the technical effect produced by them.

Since the difference in some cases may prove to be only in the intensity or extent of damage, the distinction is not always an easy one. On the other hand, this similarity also raises the question of potential competition or cumulating between them.

2. COMPUTER DATA

The Article 1. of the Convention on Cybercrime defines "computer data" as «*any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function*». This means that, under this statute the concept of computer data covers any type of data recorded in digital format, regardless of their intelligible content, including computer programs. Therefore,

[1] The Council of Europe's Convention on Cybercrime, Budapest, 23.XI.2001, Treaty Office on http://conventions.coe.int.

acts related to computer programs, when in digital form, also fall within the scope of crimes related to computer data.

Related to this definition, the same article gives also the definition of "computer system" as «*any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data*». This definition helps us to integrate were the damage potentially caused by acts that interfere in computer data produce their effects.

3. FOUR CRIMES RELATED TO COMPUTER-DATA

The Section 1 of the Convention on Cybercrime provides measures to be taken at the national level concerning substantive criminal law. In Title 1 and 2 of this section, the Convention of Cybercrime defines four types of crimes that are related to computer data. On Title 1, as crimes that constitute offences against the confidentiality, integrity and availability of computer data and systems, we have the crime of *data interference* (article 4.) and the crime of s*ystem interference* (article 5.). The first is similar to the crime of "damage"[2] over tangible goods and the second to the crime of "sabotage"[3] under ordinary criminal law. On Title 2 of this section, as computer-related offences, we have the crime of *computer-related forgery* (article 7.) and the crime of *computer-related fraud* (article 8.), that are similar the first to the crime of "forgery"[4] of tangible goods as authentic documents, and the second to the crime of "fraud" under ordinary criminal law.

---

[2] In portuguese law, the crime of data interference also resembles the "*crime of tampering or destruction of personal data*" of article 45.º of theLaw of Personal Data Protection (Lei n.º 67/98, 26/10), with some room for overlap [BENJAMIM SILVA RODRIGUES, *Direito Penal - Parte Especial*, Tomo I - Direito Penal Informático-Digital, Coimbra Editora, Coimbra, 2009p. 453; and PEDRO DIAS VENÂNCIO, "O Crime de Dano Relativo a Programas ou outros Dados Informáticos" (JusNet 121/2010), *JusJornal*, 1177, 2011p. 3].

[3] We defended the same in annotation to the article 5. of the Portuguese Cybercrime Law (Lei n.º 109/2009, 15/09) in comparison to the article 329.º of de Portuguese Penal Code.Being questionable whether, in certain situations, the crime of system Interference will not be consumed in the crime of sabotage of the Penal Code. The crime of system interference seeks protection of any «*computer system or data communication at a distance*», regardless of their public or private nature, greater or smaller, more or less economic importance. The crime of sabotage of Article 329.of the Portuguese Penal Code aims to protect «*media or roads, public services or facilities for the supply and satisfaction of the vital needs of the population, infrastructures relevant value to the economy, security or national defense*». Thus, if we think of an attack affecting the computer system that controls a public services or facilities like communications, so that it could jeopardize the functioning of the national telecommunications network, it would integrate not only the legal type of the crime of system interference but also the crime of sabotage from the crime Article 329. from the Portuguese Penal Code, in particular, in that it punishes acts against «*facilities (...) for the supply and satisfaction of the vital needs of the population" or "infrastructure of relevant value to the economy*» [PEDRO DIAS VENÂNCIO, *Lei do Cibercrime - Anotada e Comentada*, 1.ª ed., Coimbra Editora - Grupo Wolters Kluwer, 2011p. 54].

3.1 SIMILARITIES

Observing these articles it is easy to denote three essential similarities between these four substantive crimes: first, they all demand that the agent should act "without right"; second, the acts must be committed "intentionally"; and third all these crimes originate from the practice of the same material acts. This last element of similarity raises the study of this short communication.

The crime of data interference punishes the acts of «*damaging, deletion, deterioration, alteration or suppression of computer data*» (article 4.), the crime of system interference the acts of«*inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data*» (article 5.), the crime of computer –related forgery the acts of «*the input, alteration, deletion, or suppression of computer data*» (article 7.), and the crime of computer-related fraud the acts of «*any input, alteration, deletion or suppression of computer data*» (article 8). Despite the slight variations of the text, apparently all crimes originate from the practice of the same material acts, essentially: *input, delete, damage or alteration of computer data*.

Slight differences like the fact that the crime of data interference does not predict «*input of data*» or that the crime of system interference predict «*transmitting*» that is not predicted by the other crimes, do not seem relevant. The majority of the material acts which fall within the legal forecast of these crimes are the same.

This brings us to the central question of our communication. What are the differences between these four crimes, and how to solve the two problems that result of these similarity:- 1st - how to make a distinction between these crimes?; and - 2nd - are these crime "cumulative"?

3.2 WHAT IS THE DIFFERENCE?

First we will address the possible elements for distinguishing between these crimes. There are two elements were we can find those differences: in a fourth element of characterization of the criminal legal type, and in the legal interest that they protect.

---

[4] In the portuguese case it resembles the crime of forgery of documents of the article 256.º of the Portuguese Penal Code [PEDRO DIAS VENÂNCIO, "O Crime de Falsidade Informática" (JusNet 120/2010), *JusJornal*, 1176, 2011p. 2] and the "*crime of tampering or destruction of personal data*" of article 45.º of the Law of personal Data Protection (Lei n.º 67/98, 26/10), with some room for overlap [BENJAMIM SILVA RODRIGUES, Direito Penal - Parte Especial, Tomo I - Direito Penal Informático-Digital, Coimbra Editora, Coimbra, 2009p. 453].

As for this fourth element of the legal type, the Convention on Cybercrime those not demand any other mandatory element for the crime of data interference but it gives the parts the option to «*require that the conduct result in serious harm*» (article 4.). This means that the crime of data interference is the most simple or elementary crime of the pack. In the crime of system interference the Convention on Cybercrime establishes as fourth mandatory element that that act should cause a «*serious hindering of the functioning of computer system*» (article 5.). In the crime of computer–related forgery the Convention on Cybercrime establishes as fourth mandatory element that the act should «*resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic*» (article 7.). Finally in the crime of computer-related fraud the Convention on Cybercrime establishes as fourth mandatory element «*the causing of a loss of property to another person by … with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person*» (article 8.). In fact, this fourth element relates with the legal interest that these crimes protect.

As for the legal interest that these four crimes protect, we will base ourselves on the Explanatory Report to the Convention on Cybercrime.[5]

In the crime of data interference «*the protected legal interest here is the integrity and the proper functioning or use of stored computer data or computer programs*».[6] In the crime of system interference «*the protected legal interest is the interest of operators and users of computer or telecommunication systems being able to have them function properly*».[7] In the crime of computer–related forgery «*the protected legal interest is the security and reliability of electronic data which may have consequences for legal relations*».[8] In the crime of computer-related fraud «*the aim of this article is to criminalise any undue manipulation in the course of data processing with the intention to effect an illegal transfer of property*».[9] As for this last crime, although the Explanatory Report doesn't said so, it seems to us that the legal interest protected is also the safety and confidence in the computer systems, especially in the context of electronic commerce and electronic transactions of money.

---

[5] VV, Explanatory Report to the Convention on Cybercrime, Council of Europe, Budapest, 2001, available at http://conventions.coe.int./Treaty/en/Reports/Html/185.htm.

[6] Idem, (paragraph 60).

[7] Idem, (paragraph 65).

[8] Idem, (paragraph 81).

[9] Idem, (paragraph 86).

It is relevant for our study to notice that the legal interest predicted in the crime of data interference «*the integrity and the proper functioning or use*» of computer data seems implicit in the legal interests protected by all the other three crimes. To have the computer system «*function properly*», the «*the security and reliability of electronic data*» or to «*criminalise any undue manipulation in the course of data processing*», it all comes to a certain form of maintaining the «*the integrity and the proper functioning or use*» of computer data. Therefore we think that the legal interest protected by the crime of data interference is absorbed by the legal interests protected by the others three cybercrimes related to computer data.

At this point we are ready to give a first answer to the two questions that we made above: (1st) how to make a distinction between these crimes? And (2nd) are these crimes "cumulative"?

4. HOW TO MAKE A DISTINCTION BETWEEN THESE CRIMES?

The first question that might be put is distinguishing the crime of data interference from others because, in its simple form, it just needs the occurrence of the first three elements mentioned above as similar: acting "without right"; "intentionally"; and the acts of delete, damage or alteration of computer data. In the presence of any of the three other crimes these elements also appear. However, in this case the issue is not distinguishing them but if they are "cumulative". We will answer that question later.

The crimes of *computer-related forgery* and of *computer-related fraud* are easier to distinguish from the rest because they must result in a specific effect easy to determine from a legal point of view. The crime of *computer–related forgery* must result in the producing of «*inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic*» (article 7.) and the crime of *computer-related fraud* must result in «*the causing of a loss of property to another person by (…) with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person*» (article 8.). These two legal requirements are very specific results with defined legal meaning and therefore more easy to identify in a legal point of view.

The crimes of *data interference* and *system interference* may be more difficult to distinguish. Despite the fact that the crime of data interference does not require other mandatory elements, the Convention on Cybercrime al-

lows the parts to «*require that the conduct result in serious harm*» (article 4 n.º 2). If they do so, then we might have some problems distinguishing this crime from the crime of system interference. The crime of system interference (article 5) requires that the act must result in «*serious hindering of the functioning of a computer system*». The issue is what is the difference between "serious harm" and "serious hindering"? Or "serious hindering" can be also considered a "serious harm"?

The Explanatory Report says that «*the interpretation of what constitutes such serious harm is left to domestic legislation*»[10] and the same goes for the meaning of "serious hindering" according to the same report, for according to it «*each part shall determine for itself what criteria must be fulfilled in order for the hindering to be considered as "serious"*».[11] This means that in both situations the Convention on Cybercrime does not give a legal meaning to requirements. And even if it did, "serious hindering" or "serious harm" would never be an exclusive legal concept (as it is the concept of authentic document) they must relate to the technical operations of the computer system and the economic, social or technical damages that such interference produces. Therefore, this evaluation must require specialized knowledge about the functioning of the computer system (i.e. expert evidence).Who is, as we know, a strong element of uncertainty. This is, therefore, an issue to take in account in the transposition of this convention to the national level.[12]

5. ARE THESE CRIMES 'CUMULATIVE'?

In the Convention on Cybercrime these crimes seem laid in a hierarchy of gravity where the crime of data interference (article 4) is presented as the least serious. As we said before is mandatory elements - acting "without right"; "intentionally"; and the acts of delete, damage or alteration of com-

---

[10] Idem, (paragraph 64).

[11] Idem, (paragraph 67).

[12] For example, the article 4.of the Portuguese Cybercrime Law (Lei n.º 109/2009, 15/09) predicts the crime of data interference in his simple form, with only the three mandatory elements, and in an aggravated form when «*the conduct result in serious harm*», in this case the Portuguese law assesses the «serious harm» solely by monetary value of the damage. [VENÂNCIO, *Lei do Cibercrime - Anotada e Comentada*, pp. 45 ss.]. As for the crime of system interference the Portuguese Cybercrime Law predicts it in his simple form without demanding a serious hindering, any type of hindering a computer system is punish by law. Only in his aggravated form it requires a certain form of serious hindering, and here the Portuguese law takes two alternatives options: it is aggravated the act of system interference that causes damage with high monetary value; or the act of system interference «that affect severe or enduring a computer system that supports an activity designed to ensure social functions critical» [PEDRO DIAS VENÂNCIO, "O Crime de Sabotagem Informática" (JusNet 122/2010), *JusJornal*, 1178, 2011p. 2]

puter data - are also present in the other three crimes. And even the legally protected interest - «*the integrity and the proper functioning or use of stored computer data or computer programs*»[13] - seems absorbed by the interests protected by the other crimes, like we explained above. Therefore we believe that the crime of data interference can not be accumulated with the others three crimes.

As for the crimes of system interference, computer–related forgery and computer-related fraud, it seems to us, from the explanation we made above, that not only their forth mandatory element are not inherent or complementary to each other, but also their protected legal interest are independent to each other.

In conclusion we believe that these crimes can be cumulated when their mandatory elements occur in the same situation.

6. CONCLUSION

The complexity of the computer systems and is universal use to all kind of purposes makes it an essential part of the good behavior of the modern Information Society. This increasing importance has made States recognize it's dignity to obtain criminal protection.

The problem is that due to multiple use made by the same technology, in reality similar material acts related to computer data are able to produce different effects and thus affect different legal interests.

The Council of Europe's Convention on Cybercrime provides four types of cybercrime for very similar acts on computer data, the crimes of data interference, system interference, computer-related forgery and computer-related fraud. All these crimes criminalize acts that are in their objective factors materially identical but, with the exclusion of the crime of data interference, all the other three crimes predict the producing of different effects and therefore protect different legal interest.

On this basis, we concluded that this different effects and interest would in most cases be sufficient to distinguishing the four crimes from each other, although with some difficulties in the case of crime of data interference that demand a "serious harm" who may not be easy to distinguish from the "serious hindering" predicted in the crime of system interference.

As for the possibility of cumulating this four crimes, we conclude that the crime of data interference, been the base form of all the others and pro-

[13] VV, Explanatory Report to the Convention on Cybercrime, (paragraph 60)

tecting a legal interest absorbed by the legal interest protected by the others, should not be cumulated with any of the other three crimes.

But, as for the crimes of *system interference*, *computer–related forgery* and *computer-related fraud*, we concluded that their predicted effects and their protected legal interest are independent to each other, and therefore they can be cumulated when their mandatory elements occur in the same situation.

BIBLIOGRAPHY

RODRIGUES, BENJAMIM SILVA, Direito Penal - Parte Especial, Tomo I - Direito Penal Informático-Digital, Coimbra Editora, Coimbra, 2009.

VENÂNCIO, PEDRO DIAS, Lei do Cibercrime - Anotada e Comentada, 1.ª ed., Coimbra Editora - Grupo Wolters Kluwer, 2011.

VENÂNCIO, PEDRO DIAS, "O Crime de Dano Relativo a Programas ou outros Dados Informáticos" (JusNet 121/2010), JusJornal, 1177, 2011 (http://www.jusjornal.pt/)

VENÂNCIO, PEDRO DIAS, "O Crime de Falsidade Informática" (JusNet 120/2010), JusJornal, 1176, 2011 (http://www.jusjornal.pt/)

VENÂNCIO, PEDRO DIAS, "O Crime de Sabotagem Informática" (JusNet 122/2010), JusJornal, 1178, 2011 (http://www.jusjornal.pt/)

VV, Explanatory Report to the Convention on Cybercrime, Council of Europe, Budapest, 2001