Comments on the notion of information system in the Budapest Convention on Cybercrime, the EU directive, and selected penal codes

Stephan Foldes

Comments on the notion of information system in the Budapest Convention on Cybercrime, the EU directive, and selected penal codes

*Stephan Foldes**

August 2017

1. *International instruments and national legislation*. The penal codes of a number of countries having ratified the Convention on Cybercrime signed in Budapest in 2001 (the *Convention*),[1] or bound by Directive 2013/40/EU of the European Parliament and Commission on attacks against information systems (the *Directive*),[2] now contain provisions which criminalize certain acts directed at information systems or computer data (illegal system access or interference, data interception or interference, and making available certain tools for these offences). Both the Convention and the Directive provide definitions for the relevant concepts of ″system″ and ″data″ that appear as objects or instruments of cybercrime. In their national legislation the states bound by the Convention or the Directive are free to extend these notions of system and data, but not to restrict them. The Convention presently binds 55 countries, of which 26 are members of the European Union. (Ireland and Sweden signed the Convention but did not ratify it, while Denmark is not bound by the Directive.[3]) Most of the non-EU members of the Council of Europe also signed and ratified the Convention (the Russian Federation being a significant exception), as did some non-European countries like Japan, Canada and the USA. Thus a good number of countries are bound by both the Convention and the EU Directive. Among these we shall examine certain provisions of the penal codes of France, Germany, Austria and Hungary.

2. *Relationship between systems and data*. The primary functional relationship between information systems and data is one of unavoidable instrumentality. Data is not like water, which has many uses requiring neither aqueducts nor artificial reservoirs. In order to be useful, data in any significant quantity requires information systems. But an information system typically does not only process, store or transmit data – it also requires data for its very operation. It is a fundamental thesis of computer science that programs – which contain the instructions that a machine executes when it processes data – are data themselves.[4]

---

* Jurist candidate for bar admission in Budapest. Formerly researcher at Centre National de la Recherche Scientifique (CNRS) in France and lecturer at Rutgers University, New Jersey. Adjunct professor at University of Tampere in Finland (dosentti, 2004). All views expressed are the author's personally. Email: foldes.istvan@mta.renyi.hu

[1] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[2] http://eur-lex.europa.eu/eli/dir/2013/40/oj

[3] Recitals of the Directive, (32)

[4] Viewing program as data was an idea present in Turing's mathematical model of the not-yet-built computer. See A.M. Turing, On computable numbers, Proc. London Mathematical Soc. 1937, Section 6: The universal computing machine

3. *Concern with data preceded concern with systems*. The concern of the law with data and information historically preceded its concern with systems. Among the earliest legal provisions of modern times is § 20 of the Austrian Constitution of 25 April 1848 (*Pillersdorfsche Verfassung*) that guarantees the secrecy of mail.[5] In the Convention, signed in 2001, and certainly in the Directive of 2013, the concern with data has no priority over the concern with systems. Such an evolution of priorities in French legislation since the late seventies was already noted by Chilstein.[6] The Directive's dominant concern with systems is also clear from its title.[7] The Directive requires the criminalisation of five offences (Articles 3-7), corresponding precisely to those defined in Title 1 of the Convention (Articles 2-6), containing no provisions for computer-related forgery and fraud, content-related offences or copyright infringements as in Titles 2 to 4 of the Convention. These five offences in the Directive, in the order in which they appear there, are

(i) *illegal access to a system*,
(ii) *illegal system interference*,
(iii*) illegal data interference*,
(iv) *illegal interception of data transmissions*,
(v) *making available of tools for illegal access, interference or interception*.

4. *Focus on system interference.* Undoubtedly the most direct attacks against an information system are within the ambit of the system interference provisions (Art. 5 of the Convention and Art. 4 of the Directive); this offence is also our central concern in this note. Illegal access provisions criminalise a behaviour of endangerment; the materialization of the danger may result in system (or data) interference or influencing data, or the unwanted availability of proprietory data to others. According to both the Convention and the Directive, system interference needs to be criminalised in national law only if committed by influencing data. Influencing data means " inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing" computer data, both in the Convention and the Directive. National legislation may go beyond and not require that the interference be accomplished by influencing data, but it should not restrict the modes of influencing data allowing criminal prosecution. (Although in some cases, because of the overlapping of the types of data influencing action enumerated, a less than complete enumeration of data influencing behaviours may not prevent national courts from interpreting formally narrower offences in national law in a way to give full effect to the provisions of the Convention and the Directive – as Chilstein points out in the case of

[5] Verfassungsurkunde des österreichischen Kaiserstaates vom 25. April 1848, § 20. *Das Briefgeheimnis ist unverletzlich.*
[6] D. Chilstein, Législation sur la cybercriminalité en France. Revue internationale de droit comparé. Vol. 62 No. 2,2010, pp. 553-606. See pages 554-556.
[7] See also: Recitals of the Directive, system concerns in (1)-(6) versus data concerns in (6), (9) and (14)

data influencing behaviours criminalised by the French penal code.[8] In some cases, however, the national provisons may be too narrow to allow the courts to fill the gap.[9])

5. *Systems and data int he Convention and the Directive.* The definitions of what is meant by computer system and data are not identical but fairly consistent between the Convention, the Directive, and – as we shall see below – the notions adopted by some of the penal codes of the implementing states. The Convention's terms of ″computer system″ and ″computer data″ are rendered in the equally official French text of the Convention by ″système informatique″ and ″données infomatiques″. The English term ″computer″ refers to a device, a computing machine, while the French term ″informatique″ seems to be more abstract and process-oriented. (In the academic context ″informatique″ – when used as a noun and not an adjective – is commonly translated as ″computer science″ or ″computing science″.) This minor difference seems to be resolved by the the adoption of ″information system″ and ″système d'information″ in the English and French versions of the Directive.

6. *Automatism and programmability*. Both the Convention and the Directive define systems (computer systems and information systems, respectively) in terms of devices that process data, automatically and pursuant to a program. Presumably stressing the program-determined nature of data processing was deemed necessary as the drafters of the Convention (which the Directive later recognized as ″the legal framework of reference for combating cybercrime″[10]) deemed that ″automati″ means nothing more than″ without direct human intervention″[11]. Devices processing data without direct human intervention would include non-programmable mechanical devices measuring and recording physical data, thus requiring that processing be done ″pursuant to a program″ is indeed an additional *differentia specifica* of the definition.[12] As programs are themselves data containing instructions for devices, the system definitions refer to data in two different ways: data that the systems process and data that carry the instructions for processing. Man-made programs may indeed be considered a form of *indirect* human intervention.[13]

7. *System notions in penal codes: France, Germany, Austria, Hungary.* Comparing the system interference offences in the penal codes of France, Germany, Austria and Hungary, we first note that the automatic nature of the processing that information systems perform is explicit in the term″ *système de traitement automatique de données* (STAD)″ used in the French *Code pénal.* Taking a more formal approach, the Hungarian *Büntető Törvénykönyv (Btk.)*[14] contains a separate interpretation clause[15] defining the term ″*információs rendszer*″ (information

[8] D. Chilstein, *supra* note 6. See pages 564-565.
[9] See § 126b of the Austrian *Strafgesetzbuch* criminalising system interference by inputting or transmitting data only (for the text of the law see i*nfra* note 16)
[10] Recitals of the Directive, (5)
[11] Explanatory Report to the Convention on Cybercrime, 23. https://rm.coe.int/16800cce5b
[12] Turing's notion of automatism (*in* Proc. London Math. Soc., *supra* note 4) in fact already includes the hypothesis of computations being determined by a program.
[13] Unlike the directly intervening human agent being hidden within Kempelen's chess-playing ″automaton″
[14] 2012. évi C. törvény a Büntető Törvénykönyvről (Act C. of 2012), www.njt.hu
[15] Btk. 459. § (1) 15.

system) similarly to the Convention, but using the term ”installation” instead of ″device″, requiring automatism explicitly, bypassing the notion of being driven by a program, and explicitly including data storage and transmission among the possible functions of the system. The system concepts of the Austrian and German penal codes (both referred to as *Strafgesetzbuch, StGB*) differ in that the German code uses a broader system notion. The Austrian penal code,[16] without providing a definition or using a terminology that would explain the concept, simply refers to *″Computersystem″*, which – according to its usual technical meaning – would certainly evoke the notions of automatism and being driven by programs. The German penal code[17] uses the more general term of *Datenverarbeitungsanlage* (data processing installation) – *″Anlage″* similar to the *genus proximum* of the Hungarian definition –, but without requiring automatism, thus extending the criminalisation to attacks against systems whose functioning might involve direct human intervention. It also explicitly includes passive data storage devices (*Datenträger*) that do not need to be part of the processing system, or even connected or related thereto.[18] Finally, we note that unlike the Convention and the Directive, none of the four penal codes refer explicitly to the functioning of the systems according to programs, although the national courts would probably not view rare but conceivable cases of interference with non-programmable installations as constituting system interference.

9. *System notion of Directive includes data required for purposes of the system*. To be distinguished from the data that an information system as a device or group of devices is designed to process, data necessitated by the system in order to function, more precisely ″computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance″ also come within the ambit of the definition of systems in the Directive (Article 2), which thus extends the ″device only″ system notion of the Convention. However, this extension of the system concept – not appearing explicitly in the penal codes of France, Germany, Austria or Hungary – seems to make more inclusive only the offence of illegal system access, not that of system interference, which according to the Directive can already only be committed by influencing data. (Use of the means of influencing data is also a constitutive element of the offence of system interference in the Austrian penal code[19] (Störung der Funktionsfähigkeit eines Computersystems, StGB 126b), but not required by the penal codes of Hungary [Btk. 423. § (2) *a)*], Germany [Strafgesetzbuch § 303b (1) 3.] or France (Code pénal, Article 323-2).

10. *Limited role of systems as instrumenta sceleris in the Directive*. As opposed to the Convention, the Directive is only concerned with systems as instruments of crime to the extent that data required for purposes of the system may be used as a means to commit illegal

[16] Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296
[17] https://www.gesetze-im-internet.de/stgb/StGB.pdf
[18] Only the title of § 303b (Computersabotage) suggests a link that may after all be required with the processing devices, in order that an interference with the storage devices be held to constitute the offence and sanctioned as such
[19] With a rather limited number of criminalised data influencing behaviours behaviours as we observed above (See above Comment 5. *Focus on system interference*)

system access, system and data interference, as well as interception offences (in the sense of Articles 3-6 of the Directive, in infringing security measures, in influencing data, or as a technical means used in interception, respectively). In fact, while the Directive explicitly includes data as an instument of crime for both the system and data interference offences, – which by the minimum rule principle of Article 1 need not be a constitutive element in provisions enacted by national legislation –, there is not and should not be any requirement that information systems be used as a means of committing any of the offences described in the Directive. The penal codes of EU member state parties to the Convention of course must and do also contain offences in which computer systems are an essential element of crime as *instrumenta sceleris*, but in these offences the criminal attack is not against computer systems.

11. *Telecommunication systems*. Originating in society's basic concern for privacy and the secrecy of non-public communications, criminal law first came to protect telecommunication systems, and computer systems subsequently. A much noted case in the late seventies in Canada[20], – a signatory later of the Budapest Convention –, in which students at the University of Alberta interfering with the university's computer system were prosecuted, demonstrated that such interference may not be punishable under penal provisons protecting telecommunication systems. In that case the key distinction was teleological, the Supreme Court of Canada holding that *"the function of the computer is not the channelling of information to outside recipients"*, rather, the computer is *"to permit the making of complex calculations, to process and correlate information and to store it and enable it to be retrieved"*. The Convention and the Directive do not define computer systems by their purpose, but by the technical functions that they are able to perform and do perform. On the other hand it appears that telecommunication systems relying on digital technology should be included in the information system notion of cybercrime legislation enacted in implementation of the Convention and the Directive. Hungarian legal doctrine seems to support this inclusion,[21] which would be also in accordance with European legislators' explicit concern for availability, privacy and security in the area of communications, expressed in the EU Directive.[22]

[20] R. v. McLaughlin, cited in M. Hébert, M. Pylon, Computer Crime, Library of Parliament (Canada), Parliamentary Research Branch, Background Paper BP-87E, February 1984, revised November 1991. http://publications.gc.ca/Collection-R/LoPBdP/BP/bp87-e.htm

[21] Gula József, in *Magyar Büntetőjog Különös Rész*, CompLex Wolters Kluwer, Budapest 2013. See *XLIII fejezet*, section 2.2 (p. 704)

[22] Recitals of the Directive, (6), (9), (26).