available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

The definition of ICT Crime

Pieter Kleve, Richard De Mulder, Kees van Noortwijk

Erasmus University Rotterdam, The Netherlands

Keywords:
ICT Crime
Computer crime
Cybercrime
High tech crime

ABSTRACT

In the last few years, a lot of attention has been paid to what is usually called 'ICT Crime'. In this contribution, the term ICT Crime is analysed from both a practical and theoretical legal perspective. It will be argued that it is very difficult if not impossible to define ICT Crime unequivocally. Furthermore, there seems to be insufficient grounds to see ICT criminality as an autonomous legal discipline, as an independent functional discipline or as a specialisation. An important reason for dealing with ICT Crime as if it is a problem area seems to be fear in governmental organisations that new technology could lead to forms of criminality that are outside their reach of control. Furthermore, the application of ICT has led to a reorientation of legal powers with respect to investigation and prosecution. However, these subjects should be dealt with at an international level.

1. Introduction - definition problems

'ICT Crime', also indicated as 'Computer Crime', 'Cybercrime' or 'High Tech Crime', is a term used for a concept that is rather difficult to define. In legal science, legal literature and in legislative processes, however, the term is used regularly, usually in a way that suggests a common, well-defined frame of reference. It is of course a term that sounds uncomplicated. It seems to be a new legal discipline connected with criminal law as well as with computers. However, if a closer look is taken, it soon becomes apparent that this discipline might in fact not be that new at all. In fact, it could be argued that it is not even a functional legal discipline. That ICT Crime is related to criminal law and to computers is a conclusion that can be drawn, but not much more than that.

Legal practitioners with only a limited interest in the scientific approach of legal phenomena might shrug their shoulders at the fact that this field lacks a clear definition and, therefore, has unclear boundaries. However, for legal scientists, such a situation is definitely undesirable. What contribution could research make to the increase of knowledge about a certain object of studies, if that object of studies has no clear boundaries? What should be the researcher's scientific basis? Can he or she develop a theoretical framework under these circumstances? And how can the methods that are used be justified? We do not intend to imply that research regarding 'ICT Crime' has not made a contribution to the increase of scientific knowledge. This research, however, has mainly had an impact within the traditional legal areas, with a primary focus on the area of criminal law.

If ICT Crime can neither be characterised as an independent legal discipline, nor as a functional discipline, could it then perhaps be a legal 'specialisation'? Describing ICT criminality as a specialisation could quickly be seized upon by 'traditional' lawyers or lawyers specialising in criminal law as a justification not to study it. For the specialist, that is usually a desirable situation, because there are practically no limitations to what he can do.

2. ICT Crime: the object of an autonomous legal discipline?

A characteristic of autonomous legal disciplines is that within these disciplines, theory is formed autonomously (Elias, 1970). With respect to ICT Crime, that is still hardly the case, although some subjects that are dealt with within this field have had an

0267-3649/$ – see front matter
doi:10.1016/j.clsr.2011.01.004

impact on the development of legal doctrine, terminology and definition; one example is the discussion on the legal nature of software that will be described below. ICT Crime is not characterised by the development of theories that deviate from the theories that are common in criminal law. Neither do terms that are associated with ICT Crime get a different meaning in a criminal law context, nor do these terms lead to a different understanding when used in, for instance, a *civil* law context.

An example of theory development might be the discussion on the legal nature of software: the special treatment of computer data within the field of criminal law[1]. In The Netherlands, a definition of 'data' has been added to the definition part of the Dutch Criminal Code by the Computer Crime Act (I)[2]. The 'taking over', 'wiretapping' or 'recording' of data have been characterised as aggravating circumstances to article 138a on 'trespassing in a computer' which was also recently introduced. Although computers of course were the incentive for the introduction of the Computer Crime Act, the definition of 'data' used in this Act is wider than just 'computer data' or 'computer files'; data that are suitable for 'transferral', 'interpretation' or 'processing' by human actors are also included in the definition.

The specific regime for data in the Criminal Code seems to have been introduced not so much because of a deficiency in criminal theory or criminal legislation, but rather because of the unfamiliarity of many lawyers in dealing with information technology. In the new article on 'trespassing in a computer' the term 'taking away' is meticulously avoided, but this does not result in anything new or different that was not possible under the existing definition of the criminal offence of 'theft'. Furthermore, this new article – which specifies that the 'copying' of data is an aggravating circumstance for the crime of 'hacking' – means that the article on 'theft' will be no longer applicable when computer data are involved. This is undesirable, for instance because it is certainly possible to take away computer data without any previous 'hacking'. Several case decisions in The Netherlands would seem to indicate that even the theft of 'virtual objects' is possible[3]. Although in these particular cases a criminal offence had indeed been committed, it seems that in the decisions, no clear distinction was made between the computer game and reality[4].

[1] This data regime is not only the most remarkable, but with this choice of regulation for computer data, The Netherlands has taken an exceptional position in the international context.

[2] Article 80 quinquies: data includes every reproduction of facts, concepts or instruction suitable for transfer, interpretation or processing by persons or automated systems.

[3] District Court of Leeuwarden 21 October 2008 (*Virtual amulet*), LJN BG0939 en Rechtbank Amsterdam 2 April 2009 (*Habbo Hotel*), LJN BH9791. 'Virtual goods' here are objects represented in the computer game, such as an amulet or a piece of furniture.

[4] That an element *in* a computer game represents an object, for example an amulet, does not make that representation a good *outside* the game, according to Article 310. The taking away of data, which in principle would have been possible, would appear not to be possible now that the data have not been taken away. The data are still available to the controller of the game, or the host provider. There is only a difference with respect to access to the data. With respect to access to the game elements concerned, the legal relation is determined by the agreement between the controller of the game and its subscribers. There are criminal offences in this case as well, but those are of the nature of hacking, extortion and abuse.

3. ICT Crime: the object of a functional discipline?

If we try to see ICT Crime as a functional discipline, to which 'function' are we referring when using this term? The answer to this question appears to be more concerned with the ICT component than the crime component. Crime can be defined as 'unlawful behaviour that may be prosecuted'[5]. We could extend this definition of criminality by including behaviour that at present cannot be the subject of a criminal prosecution, but for which it would be *desirable* to be able to prosecute such behaviour in the future. In other words, we could include future law as well as current law. Criminology is an interdisciplinary, scientific field concerned with criminality in a social context. However, it is not a functional discipline, like, for instance, 'security' or 'fraud prevention'.

'ICT' is part of the domain of technology. In fact the name 'Information and Communication Technology' is redundant, as communication technology by definition is part of information technology. The term 'ICT' can also be used to indicate a functional discipline – such as 'Finance', 'Marketing' or 'Human Resource Management' – related to the ICT resources within an organisation. As a functional discipline, ICT can refer to the information infrastructure, but can also be understood as information science, the automation of business processes or automatic data exchange. Guarding the integrity of information resources is an important subject here, of which the prevention and combating of criminal behaviour could also be a part. However, that would not be a sufficient reason to see ICT criminality as a functional subdiscipline of the functional discipline of ICT.

If, in a similar way, we would like to consider ICT Crime as a sub-functional discipline within the criminal law system, then the area covered by ICT would appear to be too diverse. Under the label of ICT Crime, one could encounter issues regarding software piracy, child pornography and crimes of expression (such as libel, hate speech, incitation to terrorism), as well as, for instance, 'spam' and identity theft (van der Meulen, 2009; Brasem and Schermer, 2008; Schermer, 2008; Online Identity Theft, 2009).

4. ICT Crime: a specialisation?

If ICT Crime is neither an autonomous legal discipline, nor a functional discipline, it is in fact difficult to imagine that it *is* a specialisation. When we look at it from the *perspective* of a specialisation, this specialization would imply knowledge about ICT. This could be applied to criminality in general, or to criminal behaviour in general, when certain ICT aspects would prevent a full understanding of these activities. With a little scepticism, we could say this is about criminality in the information age, but this information age we live in is not fully understood by most people.

When we look at it from this perspective, ICT Crime is rather similar to the fourth category of the classification

[5] The term 'criminality' is defined in many different ways. It is clear that we are using a positive law definition of criminality.