Krytska Iryna,
Yaroslav Mudryi National Law University,
Department of Criminal Procedure

POSSIBILITY FOR THE EXTENSION OF THE MATERIAL EVIDENCE REGIME TO COVER DIGITAL INFORMATIOIN

It is almost impossible to imagine the modern world without innovative information technologies. Nevertheless electronic documents and database files designed to preserve, process and transmit documentary information in digital form in space, programs for the operation of digital technology (computers, printers, smartphones, flash cards, etc.) and for solution of practical problems, which have already existed for several decades and became an integral part of our lives, have not received specific embodiment in the provisions of the Criminal Procedure Code of Ukraine. Moreover, the legislation doesn`t determine the place of these objects in the system of evidence. Thus, the necessity of implementation of the achievements of techological progress in criminal procedure and their legislative regulation determines the current importance of the topic.

First of all, based on the analysis of the special legal literature, the definition of the main notions should be given. Thus, frequently used term "computer information" refers to the actual data generated by hardware or software, and a set of programs (commands) designed to use or to operate computers and located in computer system or in network storage media. At the same time there is the term "digital information", which can be defined as information in the form of digital signals of any physical nature recorded on storage media, content and/or properties of which establish the presence or absence of circumstances to be proved in criminal proceeding.

It is important to realize that the examined information is created, transmitted, stored, etc. not only through computer technology by which is traditionally meant, for example, the system unit, monitor, keyboard, laptop and their components, but also using other equipment like recorders, cameras, smart phones, cash registers, etc.. Thus computer information should be considered as a part of the "digital information" in its totality. And it is just this category that is suggested to use for the whole array. There are also such terms as "computer evidence", "computer facilities", "digital evidence", "electronic evidence", etc. However their definitions do not differ significantly from the definition of digital information.

The category "digital information" covers programs (software), electronic documents, database files, office files which source and thus a form of existence, is the digital equipment – storage media, which include random access memory,

permanent storage devices, hard disk drives (hard drives, floppy disks), portable storage media (optical media, flash cards), NAS-system, etc.

Important issue is a status of digital information. Among scientists there is no common position on this matter. Some (e.g, N.A. Zigura) propose to consider digital information as a separate kind of evidence, based on its specific form, environment of existence, formation mechanism and method of its conversion into proof. Others (e.g, O.G. Hryhoriiev), on the contrary regards the separation of digital information into special type of evidence as inappropriate because it may exist only in the framework of the system of material evidence and documents.

Radically new approach to determination of the status of digital information offers N. A. Ivanov insisting that it should not be considered as evidence at all. In his opinion, digital information recorded on storage media, cannot be attributed to either documents or physical evidence, so he offers to isolate it as a separate and specific source of information due to its special non-material nature, natural and technical features of its creation, processing, storage, transmission, criminal proceedings procedures and technical and forensic methods of search and seizure, access to it, research and transformation into a form that can be perceived by man. Such proposals certainly deserve attention and are quite reasonable. However, they require significant changes in the criminal procedure law and "shift" in the traditional system of evidence.

At present, while these changes have not occurred yet, let us try to consider digital information in the framework of existing criminal procedure law. Some authors offer to extend the regime of the document to that kind of information. Others regard that it is correct to recognize digital information as material evidence as an information carrier is always an object, and it is exactly the content, properties of the object that have probative value; while peculiarity of obtaining, extracting this information in accordance with the recommendations of forensic science requires such acts that entail research of the information in the laboratory (expert study).

Thereby it should be clearly understood that the difference between digital information recorded on storage media as a document and digital information as material evidence is that in the latter instance information about facts relevant to the proceedings is not formed as a result of the description of facts but as a result of immediate leaving of an event or action traces on material objects. In particular, digital information will have a probative value of real evidence in the case of software with, for example, traces of commands change or unexpected issueing of commands to create conditions of self-transformation of programs, unauthorized algorithm modification, etc. However, it is still possible to use such information as material evidence, and as the document, depending on the type of information that can be received and place of its seizure or production. So if the information was obtained from the hard drive of the computer used for hacking security system of a company`s computer network, then, the hard drive with the data of the time of hacking, a person committed cracking, used computer programs, should be admitted as material evidence. If such information is granted by ISP printout, there

are no characteristics of material evidence, and provided information will be obtained from such source of evidence as a document.

Storage media of information is considered as material evidence in the cases where the relevant information on their external appearances, features, location and other characteristics (other than content recorded on their digital information) is important. It is important that as material evidence digital information should be considered in unity of information and the media, if any of its elements was an instrument of a crime, or preserved its traces, or contains other information that may be used as evidence of facts or circumstances, or was an object of criminal unlawful actions.

Thus, digital information is an immaterial object that has a peculiarity – encoding and decoding requires not only specific hardware, but software and in some cases special methods of access. This requires using of tactics that are radically different than those used in the case of traditional evidence. There is no legislative regulation of criminal procedure of collecting, recording, preserving and initiation of digital information. This causes uncertainty of its procedural status as evidence that requires legislative regulation.