PROF. DR. ERIKA RÓTH, EGYETEMI TANÁR
University of Miskolc | DOI: 10.32041/9788367149761/7

Chapter 7. Application of Coercive Measures in Cybercrime Cases

7.1. Introduction

A delicate balance must prevail in criminal proceedings. On one side of the scale is the interest in the effectiveness of criminal proceedings, while on the other are the rights of the participants of the procedure. These rights may be limited in order to ensure the effectiveness of the proceedings, but only if the conditions prescribed by law are met.

The fundamental rights of the suspect/accused can be restricted in several forms in order to ensure the effective completion of investigation and if neccessary that of the court procedure. The most serious limitations are coercive measures, in particular measures restricting personal liberty. A common feature of coercive measures that can be used in criminal proceedings is that they restrict fundamental civil rights, the exercise of rights that are guaranteed by international human rights conventions and the constitutions of individual states. While coercive measures affecting personal liberty may only restrict the rights of the suspect/accused, coercive measures affecting assets may be imposed not only against the suspect, other participants of the proceedings may also be affected.

The rules of coercive measures in the Act XC of 2017 on Code of Criminal Procedure (hereinafter: HCCP) have no difference according to whether they are applied in cases of cybercrime and other criminal cases. The Code distinguishes between coercive

measures affecting personal liberty and assets (property). While in the case of coercive measures affecting personal liberty there are no or only few peculiarities in the area of cybercrime, several specific features can be identified in the case of coercive measures affecting assets. The author of the chapter intends to deal with the latter in detail, especially with the search, seizure and rendering of electronic data temporarily inaccessible. It should be noted here, that in some countries search, seizure and other measures are not part of coercive measures but regulated as security measures or measures connected with evidence.[1]

However, we must also mention briefly the coercive measures affecting personal liberty, since coercive measures restricting right to liberty can play an important role in cybercrime cases as well.

When applying coercive measures, the criteria of necessity, proportionality and gradation must be taken into account. The requirement of gradation is served, for example, by the fact, that coercive measures affecting personal liberty make it possible to achieve the same procedural purpose with different restrictive measures. We can say that these measures are built on each other, since, for example, if the suspect/accused violates the relatively lenient rules of conduct imposed in the framework of criminal supervision, stricter rules of conduct can be imposed on him, or even his detention can be ordered.

According to the HCCP, in Hungarian criminal proceedings coercive measures may be ordered by the court/judge, the public prosecutor and investigating authorities to compel participants of the criminal proceeding to perform their obligations or to refrain from doing something. However, there are some coercive measures that only the court is authorised to order, e.g., pre-trial detention, criminal supervision, rendering electronic data temporarily inaccessible etc.

Coercive measures affecting personal liberty in the Hungarian Code of Criminal Procedure are:

[1] This is the case, for example, in Poland where we can find regulation of search and seizure in the Section V. (Evidence) of the Code of Criminal Procedure, while coercive measures are regulated in Section VI.

a) custody,
b) restraining order,
c) criminal supervision,
d) pre-trial detention, and
e) preliminary compulsory psychiatric treatment.

It is important to mention that custody can be ordered by the court, the public prosecutor and the investigating authority, but the ordering and maintaining of the other coercive measures listed above falls under the jurisdiction of the court, therefore these are called "coercive measures affecting personal liberty subject to judicial permission".

Coercive measures affecting assets are the following:

a) search,
b) body search,
c) seizure,
d) sequestration, and
e) rendering electronic data temporarily inaccessible.

7.2. General Rules for the Application of Coercive Measures

The common feature of coercive measures is that their application means a greater or lesser restriction of fundamental rights of citizens. Therefore, efforts should be made that the use of coercive measures result in a restriction of the fundamental rights of the person concerned only to the extent and for the period of time that is strictly necessary (HCCP 271. § (1) para.). In the case when coercive measures are applied, the principles of gradation and proportionality prevail, which means that a coercive measure with more severe restriction may be ordered, if the purpose of the coercive measure cannot be achieved by a less restrictive coercive measure or other procedural act (HCCP 271. § (2) para.). The coercive measure must be carried out with respect for the fundamental rights of the person concerned, and unnecessary damage should be avoided (HCCP 271. § (3) and (6) para.).

7.3. Coercive Measures Affecting Personal Liberty

Without discussing coercive measures affecting personal liberty in detail, it is necessary to mention their possible inclusion, importance, and role in the fight against cybercrime.

Coercive measures affecting personal liberty subject to judicial permission may be ordered:

a) to ensure the presence of the defendant (to prevent him from escaping or hiding from the authorities),
b) in order to avoid the complication and obstruction of evidence (e.g., if the defendant destroyed, falsified, or hid any physical evidence or electronic data, or there are reasonable grounds to assume that he will do so),
c) to prevent the possibility of reoffending.

In cybercrime cases, where electronic evidence can be very easily modified, deleted or hidden, it is extremely important to prevent the suspect for doing so. Another purpose of ordering a coercive measure may be to prevent reoffending. The suspect may purchase a new device and continue the criminal activity even if the device originally used to commit criminal offence has been seized.

Two coercive measures are appropriate to achieve this aim: pre-trial detention and criminal supervision. If the offence was committed by harassing the person in question on social networking sites, via email messages, SMS or by other similar ways, even the restraining order may be a suitable instrument. When a restraining order is applied, the court shall impose as a rule of conduct that the defendant may not contact, directly or indirectly, and is to stay away from, a person protected by the restraining order (HCCP 280. § (2) para.).

A restraining order may be issued to avoid the complication or obstruction of the taking of evidence, or to eliminate the possibility of reoffending with regard to the victim. Criminal supervision and pre-trial detention may be ordered for all three procedural purposes mentioned above.

7.4. Coercive Measures Affecting Assets

Coercive measures affecting assets may restrict or limit the rights of the person concerned to possess, dispose and use the property its entirety, but may only affect certain elements of the property right (ownership). Thus, if the affected thing remains in the possession of the owner or processor after the compulsory measure has been ordered, he may still be able to use it.

7.4.1. SEARCH

The search restricts the so-called right to a house, the right to inviolability of the private home. Not only the suspect could be the person affected by the search. This coercive measure means a searching of a dwelling, other premises, fenced area or vehicle in order to conduct the criminal proceeding successfully. The search may also include the inspection of an information system or data medium (HCCP 302. § (1) para.). A search may be ordered if it can be reasonable to assume that it leads to:

a) the apprehension of a perpetrator of a criminal offence,
b) the detection of traces of a criminal offence,
c) the discovery of a means of evidence,
d) the discovery of a thing that may be subject to confiscation or forfeiture of assets,
e) the examination of an information system or data medium (HCCP 302. § (1) and (2) para.).

The search may be ordered by the court, public prosecutor or investigating authority except for the case when a search is to be conducted in the offices of a notary public, or in a law office, for the purpose of gaining access to protected data related to the activities of a notary public or a lawyer. This kind of search shall be ordered by a court. In any search conducted in the offices of a notary public, or in a law office, the presence of a prosecutor is obligatory. With his presence the public prosecutor ensures that the coercive measure is lawfully carried out by the investigating authority

within the framework of the court decision (Order of the Prosecutor General No. 9/2018 (VI.29.) 28 § (1) para.).

But even in this case, the search is allowed to be carried out without the court decision if decision-making by the court would cause a delay that would significantly jeopardise the purpose of the search. In such a case the decision of the court must be obtained afterwards without delay. If the search is not ordered by the court, its result cannot be used as evidence.

Special regulations concerning the office of the lawyer are becoming more and more important. With the spread of electronic administration, a significant part of the information related to individual cases is available in electronic form (or in electronic form as well). In addition, communication with clients and other persons involved in a case is increasingly done using IT devices.

If possible, the decision ordering a search shall specify the person, means of evidence, thing that may be subject to confiscation or forfeiture of assets, information system, or data medium to be found during the search (HCCP 304. § (2) para.). The precise, prior definition of the subject of the coercive measure is a guarantee and is of fundamental importance.[2]

If the purpose of the search is to find a specific person, a means of evidence, a thing, an information system or a data medium, the owner, possessor, user of the real estate or vehicle concerned, or the person authorised by that person shall be called upon to disclose the whereabouts of the physical evidence or person sought or to make available the electronic data sought. If the request is complied with, the search may only be continued if it is reasonable to assume that any other means of evidence, thing, information system or data medium may also be found.

Since not all police stations have the necessary means to carry out coercive measures and police staff lack the necessary knowledge on a certain special issue, they often have recourse to external assistance. The external help, the expert or specialist consultant is the person

[2] E. Belovics, M. Tóth, *Büntető eljárásjog*, Budapest 2017, p. 221.

who carries out the tasks on the spot and has the tools that are essential for the successfully executed procedural act.[3]

It is difficult to separate problems of involving expert and coercive measures because in these cases even the execution of coercive measures – such as search and seizure – affecting assets may require special knowledge in the field of informatics. In the HCCP there is no special rule concerning the seizure of electronic devices. This measure can be source of many errors, and improper execution can even lead to the destruction of evidence.

The Government Order containing detailed rules of the investigation prescribes, that during the examination of the information system, it is necessary to ensure that data accessible through the information system – without bypassing or evading protection devices or IT solutions – is also known and recorded, regardless of the location of the data (Government Order No. 100/2018 (VI.8.). According to László Dornfeld, during the search:

> in the information system, examinations are carried out which may not be possible later. For example, if a data is stored in a cloud service and accessible from the system during the search, it is worthwhile to perform the analysis at that time, as later access to the internet may jeopardise the integrity of the data on the data medium.[4]

During the search of IT system, it must be ensured that data accessible through the system remain unchanged during the inspection and recording. "Crucial is the ability to prove that the content presented in court is exactly the same as the one captured during the investigation."[5]

---

[3] B. Simon, R. Gyaraki, *A kiberbűncselekmények felderítése* és *nyomozása*, [in:] T. Kiss (ed.), *Kibervédelem a bűnügyi tudományokban*, Budapest 2020, p. 134.

[4] L. Dornfeld, *A kibertérben elkövetett bűncselekményekkel* összefüggésben *alkalmazható kényszerintézkedések*, "Belügyi Szemle" 2018, No. 2, pp. 119–120.

[5] P. Lewulis, *Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law*, "Criminal Law Forum" 2022, Vol. 33, No. 1, p. 42, https://link.springer.com/article/10.1007/s10609-021-09430-4 (accessed on: 18.07.2023).

7.4.2. BODY SEARCH

Body search is the search and examination of the clothing and body of a person subject to body search for the purpose of finding a means of evidence or a thing that may be subject to confiscation or forfeiture of assets. In the course of a body search, things found on the searched person may also be inspected. A body search may be ordered against a suspect, a person reasonably suspected of having committed a criminal offence or a person who can reasonably be assumed to be in possession of a means of evidence or a thing that may be subject to confiscation or forfeiture of assets (HCCP 306. § (1)–(2) para.). Of course, the body search can also be aimed at finding cybercrime-related evidence or thing subject to confiscation or forfeiture.

Voluntary performance is also important in the body search. If the body search is aimed at finding a specific thing, the person subject to the body search must be called upon to hand over the thing sought. If the request is fulfilled, body search cannot be continued (HCCP 307. § (1) para.).

7.4.3. SEIZURE

Although the seizure of electronic data is of particular importance from the point of view of cybercrime, we must also deal with the general rules of seizure. We do so because the seizure of electronic data is a special case of seizure and thus the general rules apply even if the seizure of electronic data is necessary in the criminal proceeding.

Seizure is a coercive measure affecting assets that are regulated in very detailed form in the HCCP. This time we limit ourselves to the introduction of the most essential provisions that can be considered fundamental. We must mention that the Code also includes, for example the list of things that cannot be seized, the detailed rules of execution of the seizure, etc. It deals with the special rules of seizure of documents and electronic data and preservation of electronic data, which we will discuss in detail. Finally, the Code also stipulates what can happen to the seized item.

7.4.3.1. *General Rules of Seizure*

As is mentioned above, seizure is one of the coercive measures affecting assets. Seizure restricts the right to a property of a person who suffered it, especially the right to possession. Thus, not only the owner of the thing but also the possessor may be affected.

According to the relevant provisions of the HCCP, the purpose of seizure may be to secure evidence or a thing or asset that may be subject to confiscation or forfeiture in order to ensure the successful conduct of the criminal proceeding (HCCP 308. § (1) para.). A movable thing, money in an account, electronic money, or electronic data may be seized (HCCP 308. § (3) para.).

Although seizure can usually be ordered by the investigating authority and the public prosecutor, only the court can order the seizure of evidence held in a notary public's or lawyer's office containing protected data related to the activities of the notary public or lawyer, similar to what was written concerning the search. However, if the delay resulting from obtaining the court decision would significantly jeopardise the purpose of the seizure, the investigating authority or prosecutor may execute the seizure, but the decision of the court must be obtained without delay. If the court does not order the seizure, the seized evidence must be returned to the person concerned.

The seizure may be carried out by taking possession, by other means securing preservation, by leaving the thing in the possession of the person concerned, but in the case of electronic data, the special method of seizure is defined by the HCCP. In order to execute the seizure, the holder or the handler of the thing or electronic data shall be called upon to disclose the whereabouts of the object or make the electronic data available. If he refuses to comply with the request, the thing or the electronic data can be detected by search or body search (HCCP 312. § (1) para.).

7.4.3.2. *Seizure of Electronic Data and Ordering the Preservation of Electronic Data*

In accordance with the requirements of the Budapest Convention,[6] the Hungarian CCP regulates the seizure of electronic data as a special type of seizure and the ordering of preservation of electronic data (HCCP 315–317). It has to be mentioned that these rules are only relatively new. The seizure of electronic data and ordering to preserve them was also regulated in the former Code of Criminal procedure.[7] The new Code only refined the former rules, but these changes were important.

However, in connection with criminal offences it may be necessary to seize not only the data, but seizure of the device also (laptop, flash drive, mobile phone, etc.) may become necessary. They are seized as physical evidence according to the practise established in relation to "traditional" offences.

Let us review what special rules apply to the seizure of electronic data, in particular the method of seizure. According to the 315. § (1) para. of the HCCP, seizure of electronic data may be carried out by making a copy of the electronic data, by transferring the electronic data, by making a copy of the entire content of the information system or data medium containing it, by seizing the information system or data medium containing it or by any other means provided for by law. The above-mentioned order of methods of seizure means the order of their application:

> If the seizure of electronic data is necessary for the purposes of criminal proceedings, it is not usually necessary to seize the information system (computer, server) or data medium containing the electronic data. The reason for this is that from the point of view of evidence the data itself is relevant, which can be obtained from the information

[6] Convention on Cybercrime (2001, ETS No. 185) adopted by the Committee of Ministers of the Council of Europe at its 109th Session, 8 November 2001 (hereinafter: Convention or Budapest Convention).

[7] See 151 § (2) and 158/A § of the Act XIX of 1998.

> system or data medium containing electronic data in a number of other ways (copying, data transfer).[8]

In some cases, it is not possible to seize the complete computer system due to the nature of the computer system under investigation (e.g., bookkeeper's office) or its technical characteristic (e.g., server room of an internet service provider). In this case the aim may be to obtain targeted data extraction for a specific set of data, which usually takes place in the context of the search of a dwelling or other premises. This may require the involvement of several experts and special equipment.[9]

The special method of seizing electronic data used for payment was first defined in the HCCP currently in force. According to it, the seizure of this special electronic data can also be carried out by performing an operation on the electronic data that prevents the person concerned from disposing of material (property) value expressed by the electronic data (HCCP 315. § (2) para.).

At the beginning of the codification of the current code on Criminal Procedure, Zoltán Szathmáry suggested that a procedural code could be developed that could provide flexible responses to the challenges of the future. To this end, "for the time being, it would be sufficient to lay down basic rules in the Act which could provide basis for regulation adapted to future needs".[10] As we can see, the legislator accepted this solution, and the Code contains only a short, one-sentence provision that does not deal with technical details.

In the case of Bitcoin – as one of the most widespread cryptocurrencies – no other measure than seizure makes sense, because there is no body to enforce the decision of the authorities. The only way to suspend the right to dispose of Bitcoin is to take a coercive measure applied directly against the owner by means of a forced transaction, whereby the Bitcoin to be seized is transferred from the owner's

---

[8] P. Polt (ed.), *Nagykommentár a büntetőeljárásról szóló 2017*, évi XC. törvényhez, Budapest 2018.

[9] See I.Zs. Máté, *A bizonyítékok kezelése. Az igazságügyi informatikai szakértő a büntetőeljárásban,* "Magyar Rendészet" 2014, No. 2, p. 33.

[10] Z. Szathmáry, *Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban*, "Magyar Jog" 2015, No. 11, p. 645.

address to the address of the authority.[11] This solution has been introduced in the current rules of criminal procedure. Regarding the seizure of Bitcoin, Viktor Halász notes that to appropriate storage of Bitcoin requires a centralised action by the investigating authority, specifically, the creation of a properly configured official wallet. Thus, the Bitcoin seized during the investigation would be placed is this central wallet.[12]

> In the case of electronic data used for payment, it may be sufficient to prevent the person subject to seizure from using this data for payment. Therefore, in such cases, it is also possible to block the use of electronic data used for payment (either by locking it by entering wrong codes, or by transferring the content of the data to a third-party account, etc.).[13]

Seizure of the information system or data medium containing electronic data may be carried out if:

a) it may be subject to confiscation or forfeiture of assets,
b) it is significant as a means of physical evidence, or
c) it contains a significant volume of electronic data that needs to be examined for the purpose of taking evidence, or the volume of such data cannot be determined in advance (HCCP 315. § (5) para.).

> It is also possible, that there is a suspicion that the data medium also contains data (for example data that has already been deleted) that cannot be seized by simple copying. In such cases the information system (data medium) containing the electronic data may

[11] V. Halász, *A bitcoin mûködése* és *lefoglalása a büntetõeljárásban,* "Belügyi Szemle" 2018, No. 7–8, p. 128.
[12] Ibidem, p. 128.
[13] P. Polt (ed.), *Nagykommentár…*, *op. cit.*

> be seized, as the expert can also extract these deleted (possible encrypted) data from the original device.[14]

The seizure of electronic data shall be carried out in a manner ensuring, if possible, that the electronic data not necessary for the criminal proceeding are not affected by it, or such data are only affected by the seizure for the shortest period possible (HCCP 315. § (4) para.). This rule meets the general requirement of ordering and implementing coercive measures, which means that efforts shall be made to ensure that the application of the coercive measures results in restriction of the fundamental rights of the person concerned only to the extent and for the time strictly necessary (HCCP 271. § (1) para.).

The electronic devices are seized in increasing number and their content is examined by an IT expert. It cannot be said that the seizure of such devices is only recommended for certain types of offence, for example, consider that a mobile phone may contain recordings of relevant events in the form of video or photographs.[15] When electronic devices are seized, their careful packaging and transport are also important from the point of view of the subsequent examination of data, and consequently, the effectiveness of the evidence.[16] When found, if the computer is on, files must not be opened, and the computer must not be turned off without the help of an expert. If the computer is on and the screen is also on, a picture of it must be taken. If it is detected that a deletion program is running, the power must be disconnected immediately.[17] Devices containing digital data must be protected from physical impact and from electric and magnetic fields.[18] The involvement of an expert during a search is not mandatory, the HCCP only makes provision for it. However,

---

[14] Ibidem.

[15] Z. Benedek, *Digitális adatok a helyszínen*, "Belügyi Szemle" 2018, No. 7–8, p. 147.

[16] See Z. Benedek, *Digitális…*, *op. cit*., pp. 149–150. T. Gaál and I.Zs. Máté also draw attention to the importance of packaging. T. Gaál, *A digitális bizonyítékok jelentőségének növekedése a büntetőeljárásokban*, "Belügyi Szemle" 2018, No. 7–8, p. 30, I.Zs. Máté, *A bizonyítékok…*, *op. cit*., pp. 34–35.

[17] Z. Benedek, *Digitális…*, *op. cit.*, p. 149.

[18] Ibidem, p. 150.

it is useful if an expert is present, as the expert can examine the data medium and electronic devices on the spot. He can also help to decide whether something needs to be seized or not.[19]

7.4.3.3. *Ordering the Preservation of Electronic Data*

The predecessor of the current coercive measure can be found in the Hungarian Code of Criminal Procedure since 1 January 2003. It was incorporated into provisions of the Act XIX of 1998 (the old code of criminal procedure) by the Act I of 2002. Its name was the obligation to preserve data recorded by means of a computer system. It transposed the requirements set out by the Article 16 of the Budapest Convention into domestic legislation. Later the name of the measure was modified (data stored in the information system which means a broader category), but the substance remained unchanged.

The Budapest Convention expressly requires appropriate measures to be taken in order to preserve computer data. In Article 16 it obliges parties to the Convention to adopt measures (legislative or other) to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification (Article 16 para 1. of the Convention). "The measures described in the articles operate only where computer data already exists and is currently being stored."[20]

The preservation of electronic data could be the part of seizure of electronic data. In order to detect or prove a criminal offence, an obligation to preserve electronic data may be ordered. It limits the right of disposal of the electronic data owner, processor and operator. (HCCP 316. § (1) para.):

---

[19] Ibidem, p. 151.

[20] Explanatory Report to the Convention on Cybercrime, point 150.

> Obligation to preserve data can be beneficial to the investigating authority because it does not have to seize information and data medium that are not of interest to it, and also to the subject of the coercive measure, because he can continue to use the data medium and programs (with the exception of the data concerned).[21]

The investigating authority, the public prosecutor or the court may order the preservation of electronic data if it is necessary to:

a) detect a means of evidence,
b) secure a means of evidence, or
c) determine the identity or actual place of residence of a suspect (HCCP 316. § (3) para.).

The person obliged to preserve electronic data is obliged to keep the electronic data specified in the decision unchanged and provide secure storage for these data separately from other data files if necessary; to prevent the modification, deletion, destruction, transfer, unauthorised copying of electronic data and unauthorised access to it. In other words, it means, that after the decision has been delivered, the person obliged to preserve the data must ensure that neither he nor anyone else changes the data (HCCP 316. § (4) para.).

The preservation of electronic data in the original location can significantly hinder the data subject's activities related to the possessing, handling, storage or transmission of electronic data. In this case the HCCP 316. § (6) para. provides another possibility:

> At the request of the person obliged to preserve data, it can also be ordered that he does not have to physically store the given electronic data where the authority found it, but to make a copy of the electronic data and keep it. In such cases the person obliged to preserve the electronic data can even change the original data (if the decision so allows).[22]

[21] F. Tóth, *Az informatikai bűnözéshez kapcsolódó kényszerintézkedések*, "Büntetőjogi Szemle" 2017, No. 1, p. 79.
[22] P. Polt (ed.), *Nagykommentár…*, *op. cit.*

If, despite the best efforts of the person obliged to preserve electronic data, the data are assessed (modified, deleted, destroyed, transferred, copied, accessed without authorisation, or any attempt to do so is detected), he must immediately inform the authority ordering the preservation of electronic data (HCCP 316. § (8) para.).

Since the purpose of the ordering this measure is to preserve data that may be important from the point of view of the detection or evidence in an unchanged state, after the order is issued, the authority that ordered it shall start the examination of electronic data. As the result of such examination, the authority shall decide whether to order the seizure to be enforced in another way or terminates the preservation.

The fundamental difference between a seizure and the obligation to preserve electronic data is correctly summarised by Fanni Tóth: While in the case of the preservation order the investigating authority can only examine the data, the seizure is used to secure the evidence.[23]

The preservation obligation lasts for a maximum of three months.

7.4.4. SEQUESTRATION

On the one hand, the sequestration serves the interest of the state, which manifests itself in the confiscation of assets, and on the other hand serves the private party's claims for the compensation.[24] While seizure limits the right to possession, the sequestration restricts the right to dispose of the property.

Sequestration means the suspension of a right of disposal over the sequestrated thing for the purpose of securing the confiscation of assets or a civil claim (HCCP 324. § (1) para.).

In general, we can say that in the field of cybercrime, seizures ordered for the purpose of finding and preserving evidence are much more important and much more frequent. There are two cases

[23] F. Tóth, *Az informatikai…*, *op. cit.,* p. 78.
[24] E. Belovics, M. Tóth, *Büntető…*, *op. cit*., p. 230.

when the legislator allows the sequestration to be ordered: when it is necessary for the forfeiture of property or to satisfy a civil claim.

The Code allows ordering sequestration regarding assets, providing a detailed list of items of property concerned, e.g., thing, money in an account, electronic money, right of pecuniary nature, claim of pecuniary nature, etc. (HCCP 324. § (2) para.).

Sequestration may be ordered if:

a) a proceeding is conducted because of a criminal offence with regard to which the forfeiture of assets may be ordered, or
b) its purpose is to secure a civil claim,

and it is reasonable to assume that enforcing the forfeiture of assets, or satisfying the civil claim, would be frustrated (HCCP 324. § (3) para.).

Sequestration may be ordered by the court, the prosecution service, or the investigating authority, but in some cases defined by the Code only the court is authorised to order it even before the indictment (HCCP 327. § (1)–(2) para.). If the obtaining the decision of the court would significantly jeopardise the purpose of sequestration, the prosecution service or an investigating authority may order the sequestration until the court decision is adopted. In such a situation, the permission of the court shall be obtained ex-post without delay (HCCP 327. § (5) para.).

7.4.5. RENDERING ELECTRONIC DATA TEMPORARILY INACCESSIBLE

The introduction of the measure called "rendering electronic data irreversibly inaccessible" into the Criminal Code and the insertion of coercive measure enabling the temporarily inaccessibility of electronic data into the Code of Criminal Procedure – as it was already analysed by several authors[25] dealing with the topic and

[25] See, for example, F. Tóth, *Az informatikai…*, *op. cit*., pp. 80–81.; T. Gaiderné Hartmann, *Elektronikus adatok ideiglenes* és *végleges hozzáférhetetlenné tétele – egy* új *intézmény első* évei, "Magyar Jog" 2015, No. 2, pp. 106–107; L. Dornfeld, *A kibertérben…*, *op. cit*., pp. 129–130.

as it is written in the reasoning of the given acts – was primarily required by the obligation stemming from the Directive 2011/93/EU.

The coercive measure was introduced in the Code of Criminal Procedure in connection with the entry into force of the Criminal Code. It was a logical legislative step to have a procedural counterpart of the criminal measure to prevent access to illegal content. At the same time, it raised a number of problems in practice, which were also pointed out by László Dornfeld in his study.[26]

In order to understand the purpose of this coercive measure, we need to have a look at the parallel measure of the Criminal Code. According to the 77. § (1) para. of the Criminal Code, data disclosed through an electronic communications network shall be rendered irreversibly inaccessible:

a) if the publication or disclosure of which constitutes a criminal offence,
b) if said data are actually used as an instrument for the commission of a criminal act, or
c) if said data are created by way of a criminal act.

The conditions for the application of the given coercive measure in the HCCP are thus aligned with the applicability of the measure prescribed in the Criminal Code. In addition, however, two further criteria can be derived from the provision of the HCCP. Rendering electronic data temporarily inaccessible may be ordered where a proceeding is conducted regarding a criminal offence subject to public prosecution, in connection with which rendering electronic data permanently inaccessible may be ordered, and doing so is necessary to interrupt the criminal offence.

Rendering electronic data temporarily inaccessible restricts the right to dispose of data published via an electronic communications network.

It may be ordered in the form of:

a) temporarily removing the electronic data concerned, or
b) temporarily preventing access to the electronic data concerned.

[26] See L. Dornfeld, *A kibertérben…*, *op. cit.*, pp. 130–133.

Removing electronic data temporarily means that service provider that processes the electronic data concerned shall be ordered to temporarily remove the electronic data (HCCP 336. § (1) para.). In the second case (point b) the court may order an electronic communications service provider to prevent access to electronic data temporarily (HCCP 337. § (2) para.). The enforcement of this coercive measure is organized and controlled by the National Media and Communications Authority (HCCP 337. § (3) para.).

The temporarily removing the electronic data is the primary solution, in the event of its ineffectiveness, access may be temporarily blocked, provided that the procedure is in progress due to the crimes listed in the HCCP.

In addition, the legislator also created the possibility for the prosecutor or the investigating authority to call on the service provider capable of preventing access to electronic data to voluntarily remove electronic data, provided that this doesn't harm the interests of the criminal proceeding. The purpose of this provision is to ensure that the content that violates criminal law is only available for the shortest possible time.[27]

7.5. *The Lege Ferenda* Proposals

We do not wish for, and cannot formulate, proposals for specific legislative amendments, since to formulate it we would need to have a much better understanding of Polish procedural rules and law enforcement practice.

In relation to cybercrime, it can be said in general, that due to rapid technical development, substantive and procedural rules that should be timeless quickly become out-of-date. Frequent amendments of rules can cause a breakdown in coherence.

The task of the legislator is to remedy the problems arising in the application of the law if the applicability of the rules is called into question. In doing so it is necessary to cooperate with practitioners, and where appropriate, not only with lawyers.

[27] I. Lajtár, *A kíberbűnözésről*, "Ügyészek Lapja" 2019, No. 1, p. 50.

The full implementation of EU legislation is extremely important in the fight against cybercrime.

The legislator must also be open to adopting solutions and good practices already tried and tested in other countries.

7.6. Conclusion

Rules of criminal procedural codes and law enforcement practice must meet double requirement: to ensure effectiveness of criminal justice and to protect and respect human rights of participants, among others fundamental rights of the suspect/accused.

In the proceedings due to cybercrimes, law enforcement authorities, in particular the investigating authorities, have to deal with particular difficulties. The easy alteration of data, the possibility of encryption and the difficulty of identifying the perpetrator can easily encourage the authorities to circumvent the legal rules to a certain extent and try to obtain evidence. Thus, the requirement of efficiency could precede the respect for fundamental rights. However, this should not be allowed to happen.

Successful execution of search or seizure in the case of cybercrimes requires special expertise. Therefore, it is very important to involve IT experts in the performance of these procedural acts. It is almost impossible to correct errors or shortcomings in this area at a later stage. "(…) even the best legislation on coercive measures is not enough if the investigatory authorities lack the competence, tool, methods, and resources needed to investigate cybercrime and to collect relevant evidence."[28]

Although certain coercive measures affecting assets (e.g., search, seizure) are of paramount importance in the case of cybercrimes, it should not be forgotten that other coercive measures can also play a role in ensuring the effectiveness of evidence or preventing reoffending (e.g., pre-trial detention, criminal supervision or restraining order).

[28] J. Riekkinen, *Evidence of cybercrime and coercive measures in Finland*, p. 16, https://journals.sas.ac.uk/deeslr/article/view/2296/2249 (accessed on: 12.07.2023).

REFERENCES

Belovics, E., Tóth, M., *Büntető eljárásjog*, Budapest 2017.

Benedek, Z., *Digitális adatok a helyszínen*, "Belügyi Szemle" 2018, No. 7–8.

Dornfeld, L., *A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések*, "Belügyi Szemle" 2018, No. 2.

Gaál, T., *A digitális bizonyítékok jelentőségének növekedése a büntetőeljárásokban*, "Belügyi Szemle" 2018, No. 7–8.

Gaiderné Hartmann, T., *Elektronikus adatok ideiglenes és végleges hozzáférhetetlenné tétele – egy új intézmény első évei*, "Magyar Jog" 2015, No. 2.

Halász, V., *A bitcoin mûködése és lefoglalása a büntetõeljárásban*, "Belügyi Szemle" 2018, No. 7–8.

Lajtár, I., *A kíberbűnözésről*, "Ügyészek Lapja" 2019, No. 1.

Lewulis, P., *Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law*, "Criminal Law Forum" 2022, Vol. 33, No. 1, https://link.springer.com/article/10.1007/s10609-021-09430-4 (accessed on: 18.07.2023).

Máté, I.Zs., *A bizonyítékok kezelése. Az igazságügyi informatikai szakértő a büntetőeljárásban*, "Magyar Rendészet" 2014, No. 2.

Polt, P. (ed.), *Nagykommentár a büntetőeljárásról szóló 2017. évi XC. törvényhez*, Budapest 2018.

Riekkinen, J., *Evidence of cybercrime and coercive measures in Finland*, https://journals.sas.ac.uk/deeslr/article/view/2296/2249 (accessed on: 12.07.2023).

Simon, B., Gyaraki, R., *A kiberbűncselekmények felderítése és nyomozása*, [in]: Kiss, T. (ed.), *Kibervédelem a bűnügyi tudományokban*, Budapest 2020.

Szathmáry, Z., *Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban*, "Magyar Jog" 2015, No. 11.

Tóth, F., *Az informatikai bűnözéshez kapcsolódó kényszerintézkedések*, "Büntetőjogi Szemle" 2017, No. 1.

Basic Hungarian legal sources

1998. évi XIX. törvény a büntetőeljárásról (the old Code of Criminal Procedure).

2017. évi XC. törvény a büntetőeljárásról.

9/2018. (VI. 29.) LÜ utasítás az előkészítő eljárással, a nyomozás felügyeletével és irányításával, valamint a befejező intézkedésekkel kapcsolatos ügyészi feladatokról.

100/2018. (VI. 8.) Korm. rendelet – a nyomozás és az előkészítő eljárás részletes szabályairól.