dr. Réka Gyaraki (University of Pécs Doctoral School of the Faculty of Law)

gyarakireka@gmail.com

THE LEGAL REGULATION OF RENDERING ELECTRONIC DATA INACCESSIBLE

As a consequence of the growing number of information technology crimes it has become necessary to enact legal regulations that prevent further access to illegal contents in the course of the criminal proceeding as well as subsequently to its conclusion, and at the same time does not obstruct the complete conducting of the proceeding.
Not only the general portion of Section 77 of the Criminal Code regulates rendering inaccessible, but this new regulation has also been included in the Act on Criminal Procedure in relation to enforcement measures. Besides presenting the text of the Act, I will also perform the comparison of law enforcement intent and its operation in practice, while listing those criminal act types in the case of which rendering illegal data inaccessible is applicable.
The question is, whether the procedure for rendering inaccessible meets the requirements, or not.

Introduction

In recent years, legislators, courts of law, the prosecutor general's office and investigative authorities have had little chance of controlling/preventing information technology crimes. Criminal substantive law not at all, while criminal procedural law only attempted in general terms to prevent criminal acts committed by means of information technology.
The development of information technology and the spread of information technology systems have entailed not only the faster dissemination of information, but also the proliferation of criminal acts committed by their means (devices), as well as against them (e.g. data). Types of information technology crimes have emerged, which to the grievance of private individuals, legal entities, organizations as well as state institutions affected by the offence, are a threat to property, moral, possibly information security, and at the same time also cause (financial) damage. Until now, there has not been much chance for the management, follow-up, prevention of such offences by legal means, while the existing legal means have been easily circumvented by the offenders. The contents affected by the offence were accessible in the course of the criminal proceeding, at the same time there was no sufficient method for rendering them inaccessible after its conclusion.

With Act C of 2012, a new legal institution appeared during the reconsideration of the Criminal Code: *Rendering electronic data inaccessible.* At the same time, the procedural law regulation of this also emerged, which was included among the enforcement measures: „The permanent rendering of electronic data inaccessible", and „The temporary rendering of electronic data inaccessible".
Otherwise, this new regulation also satisfies an EU obligation – the contents of Section 25 of Directive 2011/93/EC -, according to which, member states shall take the necessary measures to render websites removable that contain or disseminate child pornography, operated on their territories.

Electronic data and rendering it inaccessible

First, it is the most important to get to know what electronic data is. Why is rendering electronic data inaccessible necessary, and in what cases and by what method this can be ordered?

Electronic data: „the materialization of facts, information, or concepts stored, managed, processed or transmitted in an information technology system, in all such forms that are suitable for processing by an information technology system, including the program that provides for the execution of any function by the information technology system.[1] According to the execution related to the procedure, on the homepage of the National Media and Infocommunications Authority (NMHH), in the case of a rendering inaccessible procedure, electronic data is such data published by means of an electronic communication network, by access providing electronic communication service providers, which is identifiable by an IP and URL address, as well as port number[2].

The permanent rendering of electronic data inaccessible

According to the Ministerial Reasons, prior to the taking effect of the new Criminal Code, in the case of criminal acts committed through the information technology network there was no measure for rendering illegal content inaccessible. The options of the authority were indeed limited against information technology criminals. In the case of illegal content, for the investigation and arrest of the offender(s), the options of criminal procedural law and other open or secret investigations (among others police investigation), enforcement measures, specified by law were relatively limited.

The General Portion of Section 77 of the Criminal Code provides an option for the removal of content from the electronic communication network, the providing access to which, or publications of which is a felony, or which content is used as an instrument in the commission of a criminal act. It also provides an option for the permanent removal of content that was used as an instrument in the commission of a criminal act.

Therefore, rendering inaccessible is justified in the following cases:

- Terrorist acts,
- Child pornography,
- Racist acts,
- Fraud,
- Copyright infringement,
- Consumer deception,
- Abuse of personal data,

---

1 Section 423 Paragraph (4) of Act C of 2012 on the new Criminal Code

2 http://nmhh_muszaki_ajanlas_20131008.pdf (downloaded: 18.10.2014)

- In certain cases of cyberbullying or internet harassment

In these cases the temporary or permanent rendering of electronic data inaccessible may be ordered.
Likewise, electronic data shall also be rendered inaccessible, if the illegal content thereof is connectible to a person who is unpunishable because of being a minor, or mentally incapable.

The temporary rendering of electronic data inaccessible

Act XIX of 1998, discusses it among procedural law enforcement measures. The purpose of rendering inaccessible is for the technical methods for rendering electronic data inaccessible implemented by the electronic communication service provider *to display a text regarding the fact and reason for the prohibition instead of the accessible electronic data to the internet user, based on characteristics specified in a prohibition ruling by a court of law, or authorities specified in a separate statute (National Tax and Customs Administration of Hungary, police)*[3].

In the case of so-called content criminal acts – such as child pornography or copyright infringement offences – the illegal act is committed instantly, therefore the insulation of electronic data may become necessary.

According to the wording of this statute, temporary rendering of electronic data inaccessible is the temporary restriction of the right to dispose over the data published on the electronic communication network (for the purposes of this article hereinafter: electronic data), and the temporary prevention of access to the data. In the case of any content created by a criminal act liable to be prosecuted under public prosecution, if the (permanent) rendering of electronic data inaccessible and preventing the continual commission of the criminal act is justified, temporary rendering inaccessible may be ordered. Meaning that in the case of websites the content of which is illegal, temporary rendering inaccessible becomes possible that can be applied during the criminal proceeding. According to the Act on Criminal Procedure, on the one hand the proceeding is of preventive nature, meaning that further access to the specific content shall be prevented, on the other hand it may prevent the escalation of such criminal acts.

The obligor so ordered shall be mandated to temporarily remove the electronic data, from the time of notification regarding the ruling. In the case of failure to comply, the court may impose a fine of HUF one hundred thousand to HUF one million on it, possibly repeatedly. (The storage space provider is also the obligor of the restoration of the electronic data, however in this case the Act does not stipulate a fine). The storage space provider is mandated to take measures within 12 hours regarding the removal of the electronically published illegal data in a restorable manner, at the same time to inform the users regarding the legal basis for the content's removal or prevention of access to the content. (In the case of the cessation of the measure, the storage space provider also has 12 hours to make the electronic data accessible again.)

---

[3] http://nmhh_muszaki_ajanlas_20131008.pdf (downloaded: 18.10.2014)

According to my assumption, beyond prevention, temporary rendering inaccessible may create such a transitional condition, which if the commission of the criminal act is possibly unprovable, then by means of temporary blocking, subsequently to the conclusion of the proceeding the original condition is restorable.
In the proceeding, the court, more precisely the investigating magistrate is authorized to proceed.
The Act differentiates between two forms of the measure:

a.) Dependent of the court's deliberation:
If the proceeding is initiated because of a criminal act liable to be prosecuted under public prosecution, in relation to which permanent rendering inaccessible is justified, and thereby the continuation of the criminal act can be prevented.

b.) Ordering of mandatory rendering inaccessible:
a) the storage space provider failed to comply with its obligation related to temporary rendering inaccessible, or in relation to the temporary rendering of the electronic data inaccessible petitioning a foreign authority for legal assistance is unsuccessful within thirty days calculated from the issuance of the petition, and
b) the criminal proceeding was initiated for child pornography (Section 204 of the Criminal Code) or a criminal act against the state (Chapter XXIV of the Criminal Code) or a terrorist act (Sections 314-316 of the Criminal Code), and the electronic data is related to the criminal act.[4]

Subsequently to this the judge (as the above mentioned investigating magistrate) makes a ruling, which it forwards to the National Media and Infocommunications Authority, who notifies the storage space provider regarding the proceeding and the case file number.

In the course of the proceeding to render inaccessible in reality two processes can be differentiated. In one case we can speak of the removal of electronic data. The court is authorized to order this in a ruling. The obligor is the storage space provider. In this case the National Media and Infocommunications Authority does not participate in the organization of the proceeding.
In the other case, the prevention of access to electronic data occurs, in which a court is authorized to proceed as well. The obligors of the proceeding are internet-service providers, browser service providers and the cache service provider. In this case the National Media and Infocommunications Authority plays a role!

Rendering electronic data inaccessible can be ordered temporarily, by the temporary removal of the data or the temporary prevention of access to the data.

Thus, the subjects of the proceeding are the internet-service provider, the browser service provider and the cache service provider, the investigative authority, the prosecutor general's

---

[4] Section 158/D Paragraph (1) Items a) and b) of Act XIX of 1998

office, the investigating magistrate, the National Media and Infocommunications Authority, and of course the victim(s), the offender(s), possibly experts, etc.
In reality this enforcement measure occurs if the storage space provider fails to remove the illegal data despite the order, or the petitioning a foreign authority for legal assistance is unsuccessful within thirty days calculated from the issuance of the petition, or the electronic data is related to a criminal proceeding initiated for child pornography, a criminal act against the state, or a terrorist act.
The court notifies the National Media and Infocommunications Authority regarding temporary rendering inaccessible, who verify the execution thereof, as well as register the fact thereof into the Central Database of Rulings to Render Inaccessible.

What is the Central Database of Rulings to Render Inaccessible?

KEHTA, is the abbreviation of the Central Database of Rulings to Render Inaccessible. KEHTA is operated by the National Media and Infocommunications Authority by processing the data entered by the court or other authority specified in a separate statute. The data of KEHTA are not public, only the court, the prosecutor general's office, the authority specified in a separate statute, the investigative authority, or the members of the competent committee of Parliament and the National Media and Infocommunications Authority may access it.
The court and the authority specified in a separate statute record the following in the Central Database of Rulings to Render Inaccessible:

- *The designation of the proceeding court or the authority specified in a separate statute, and the file number of the ruling,*
- *The order related to preventing access to the electronic data or to the cessation of blocking,*
- *Data related to the identification and accessibility of the data*[5].

In the case of failure to temporarily remove the electronic data, a fine of HUF one hundred thousand to HUF one million may be imposed, which may be imposed repeatedly, once every three months.
Thus, the task of the authorities, in the case of illegal contents, is to block access thereto, meaning to render them inaccessible to users. At the same time, let's not forget that the website itself is a piece of investigative material, meaning that it constitutes evidence during the proceeding.
Further tasks of the proceeding court in the interest of the success of the ruling regarding rendering inaccessible:

1. In the operative part of the ruling the electronic data affected by the ruling must be exactly specified (exactly specify the URL address, IP address, domain name, etc.).

---

5 http://nmhh.hu/cikk/160577/Kozponti_elektronikus_hozzaferhetetlenne_teteli_hatarozatok_adatbazisa_KEHTA#sthash.zzEljjPg.dpuf

2. It must be exactly specified, on what basis the court orders the temporary or permanent rendering inaccessible, meaning that specifying the fact of the offence by itself is insufficient.
3. The ruling regarding the temporary or permanent rendering inaccessible must be immediately forwarded to the National Media and Infocommunications Authority.
4. The court must specify the text it wishes to be displayed on the website affected by the ruling.

The cases of cessation of rendering inaccessible

The court orders the cessation of rendering inaccessible, if:

- The reason for rendering inaccessible has ceased,
- The investigation has been ceased, except in the case specified in Section 77 of the Criminal Code, when the permanent rendering inaccessible shall be ordered even if the offender is unpunishable because of being a minor, mentally incapable, or other reasons exempting from punishability,
- The storage space provider has complied with its obligation related to the temporary removal of electronic data,
- The reason for the enforcement measure has ceased.

Misgivings related to rendering electronic data inaccessible

According to the stance of the Hungarian Civil Liberties Union (TASZ), until such time that an effective court decision states regarding the data – for instance a blog comment – that it is illegal and liable to be prosecuted under public prosecution, a restriction of this characteristic may only be proportional in the case of the suspicion of such crimes, when the interest related to the removal or restriction of access is of greater importance than grievance caused by the possible commission of the criminal act.
However, the Hungarian Civil Liberties Union has also acknowledged in relation to the procedure that in the case of child pornography the introduction of the new form of measure is justified and proportional, since this offence is not protected by freedom of speech, they furthermore explained that in certain cases it is also justified that criminal acts against the state and terrorist acts may serve as the basis for temporary removal, however expanding it to all criminal acts liable to be prosecuted under public prosecution is a disproportionate measure. At the same time the Hungarian Civil Liberties Union made a proposal that the legislature should also make the measure applicable to cases of incitement against the community, preparation for violence against members of the community (Section 216 Paragraph (4) of the new Criminal Code).
The Hungarian Civil Liberties Union considers the 12 hour removal deadline specified in the rendering inaccessible procedure excessively short and the HUF 1 million fine excessively high in relation to storage space providers who are unaware of the illegal content.

Conclusion

On the one hand rendering electronic data inaccessible is a positive innovation in relation to combating offences committed in the information technology environment. In my opinion, the creation of such procedural law regulations that deal with the blocking of illegal content has already become necessary.

At the same time the procedure itself is excessively complex, and it passes through many authorities and many persons until reaching its goal, which may possiblly lead to the failure of the investigation. In reality, one of the principles of procedural law is also violated, the principle of proportionality.

It is rather simple to judge how applicable rendering inaccessible is.

It is problematic that the storage space provider is not necessarily aware of what kind of data has been placed on the storage space provided by it, and removal as well as blocking may be difficult, since in certain cases it must inspect an immense quantity of data.

According to my view the procedural system described in the Act is slow and it does not clarify the roles. It arises as a question that knowing the characteristics of internet criminal acts, such as rapidity, anonymity, and criminal activity reaching across borders, how flexible the procedure is. If it is rigid, in my opinion it will not necessarily be sufficiently applicable in every case.