Crossborder criminality - crossborder fight through digital borders - principles practices and concerns of gathering covert information and data by the perspective of the case-law of the EctHR and the CVRIA

Semi-final presentation of the Team of HUNGARY
Hungarian Judicial Academy
Budapest
HUNGARY

18th of March
2014
'Let us imagine a case of an EU citizen committing a criminal offence listed in the Corpus Juris Europae rendered an EU-wide recognised sentence even depriving liberty and executed in an EU penitentiary upon EU rules and having been sentenced with the hope to be relocated into one of the National Societies of an entirely unified Europe.......'

I. Introduction

First and foremost, we would like to analyse the two most significant phenomena concerned in the title: crossborderness and criminality.

Judicial cooperation in criminal matters gained importance in the European Union (hereinafter: EU) when the primarily economic organization of the European Economic Community (hereinafter: EEC) was stabilized and unfolded other areas of common action too. The problems associated with crossborder crime could be classified as one of the negative consequences of free movement, namely, the physical abolition of internal borders and the unrestricted free movement of persons in general resulted a security deficit in the European Union, which definitely urged legislators to act. The desire for the greatest possible effectiveness of the common market and free movement of goods and persons as well as for the protection of its economic interests led the EU slowly but also definitely to use criminal law as the apparently most effective tool for approaching those goals. The Treaty of Amsterdam added to these goals as another particularly significant aim the guarantee of a common Area of Freedom, Security and Justice where it was deemed that criminal law could contribute conclusively. However, insofar as the EU does not possess the characteristics of a state entity this aim could only be accomplished through the cooperation with the member states.

One should also bear in mind the two fundamental principles of the relation between the EU and the MSs: subsidiarity and loyalty, while comprehensively analysing what should be done in order to improve the effectiveness of the indisputably unavoidable endeavours.

Consequently, the development of criminal law within the EU frame is co-determined by this relation.\(^1\)

\(^1\) Richard Vogler – Barbara Huber: Criminal Procedure in Europe Max – Plank – Institut für auslandisches und
Cross-border criminality is mostly connected to organised crime: crimes against humanity, war crimes, crimes against extremely vulnerable groups of the society, such as racism, xenophobia, hate speech, money laundering, corruption. In our everyday communication and commercial activity now taking place via the Internet, the threat of cybercrime is increasing, targeting citizens, businesses and governments at a rapidly growing rate. The EU in particular is a key target because of its advanced Internet infrastructure and increasingly Internet-based economies and payment systems, such as e-banking and the electronic non-banking institutions. However, these are not obvious for everyone, but no one can deny these are great concerns for the future.

The aim is to tackle the most relevant criminal threats to the EU and to ensure a systematic approach by all EU actors to fight crossborder criminality – even digitally.

Cooperation in combating crime has been and constantly is one of the priorities for the legislators in the EU. Financing terrorism, counterfeiting of goods, proceeds of these criminal offences are often basis of financing Islamic radical fundamentalism and related terrorism as a major challenge for the European Union – some experts claim.

The question has arisen: “what are those tools available for gathering information surrounding criminal actions?” There are classic and modern tools of investigations. Typical ones are: wire tapping, interception of calls and other aspects of IT related communication (e-mailing, messenger services, and voice over Internet aka. VoIP protocols [Skype, Viber, Whatsapp and so on]).

The interest in the effectiveness of law enforcement justifies the need for covert investigation in cases of serious crimes where ‘traditional’ means of investigation are not suitable for reaching the aim of these operations, especially in the field of consensual, conspirational and organized serious crime. In such cases covert investigation does not play an important role simply as a part of the ‘classic’ follow-up type police operations reacting to the criminal attempts but also displays proactive features – aiming at the exploration of elemental possibilities of committing serious crime.

In the course of the fight against this type of criminality the need for undercover operations do significantly arise, furthermore it requires both cooperation of the law enforcement agencies and criminal justice organisations of different countries and operations affecting the sovereignty of various states, the thorough regulation and execution of which is crucially important especially in
the human-rights-sensitive area of covert investigation.

In relation to the above, the topic of police cooperation taking into account the role of the European Union that is fundamentally influencing - both direct and indirect way - the domestic legislation and jurisdiction to some significant extent: - in particular with a view to the EU regulation.² Regarding the EU, it was the cornerstone to establish the Convention on Mutual Legal Assistance as a prior legal source, declaring: covert investigations may also be carried out by officers acting under covert or false identity, provided that the national law and procedures of the Member State where the investigations take place are complied with.³ According to the article, the rules of the covert investigation are flexible. Consequently, ruling this area belongs to the domestic legislation as not preempted and remained under MS control. Hence, law harmonisation was left as a preferable way, as well as approximation of Laws. What is most likely awaited from the MS is the mutual trust and confidence with the view to the preliminary investigative measures and decisions.

The starting point of the essay is the topic of covert operations concerning mainly law enforcement and covert investigation linked to criminal judicial praxis especially their role in crossborder fight through digital borders. We attempt to show some specific features of covert investigation within the frame of police operations. Then we analyse the details of the relevant Hungarian rules focusing on the territory of undercover operations under law enforcement and criminal justice.

Finally, we are trying to find the right balance between the effectiveness of law enforcement and Human Rights and the extra-values of Rule of Law appearing in procedural guarantees concentrating on domestic rules. We are looking forward also to the possible achievements present in legislation and – from our point of view – should be present in jurisdiction as well since of course this is true regarding the criminal procedure in general as well; however, it carries special relevance in this field, because of the above-mentioned issues. Taking into account that the person affected by undercover operations does not have any possibility to become aware of the fact that such tools are used (just after the operation, possibly), despite being the victim of the intrusion to privacy, thus has no opportunity to take remedy against the potential violation of one's rights, the rules themselves should be suitable for serving as obstacles to the abuse of powers. Furthermore, the organisational structure of permitting, carrying out and controlling of covert investigation should include such guarantees that exclude these abuses. As we have already referred to the above, the requirements deriving from Human Rights and Rule of Law are even more significant in the field of both legislation (including domestic and – on the basis of the European Convention on Human Rights –


Council of Europe and European legislation) and jurisdiction as well.

In the ending thoughts, we concentrate on the issues regarding jurisdiction besides *de lege ferenda* propositions, based on the main features of the scope of the EU legislation and the European Court of Human Rights.

### II. General principles of gathering covert information or data:

Human rights are fundamental civil, cultural, economic, political and social rights for which everyone is entitled to enjoy without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. This formulation takes place in Article 2 of The Universal Declaration of Human Rights.4

According to the Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedom (Rome,4.XI.1950) best known as the European Convention on Human Rights (hereinafter: ECHR) everyone has the right to be respected in his or her private and family life, home and correspondence. The second subsection of Article 8 says that: „there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”5

Within the legal framework of the European Union, the Charter of Fundamental Rights of the European Union also regulates the respect for private and family life. The regulation is similar to that of the ECHR, as Article 7 ensures the right for private and family life, home and communication.6

This general principle in different above-mentioned draftings aims to ensure the inviolability of privacy, which means privacy in family, personal relations, private habitation, right to private property, personal data, sexuality, religion and other personal attitudes. These rights are fundamental for a human being and everyone must respect them. These are not only under special and emphasized protection but ensure extremely sensitive data such as race, colour, sex, disability,
language, religion, political or other opinion, national or social origin, private property, birth or any other status. This special kind of protection can naturally also be found in the Hungarian national law.

Hungarian legal system regulates this principle in the Fundamental Law of Hungary. In the first article of Title Freedom and Responsibility we can read, that: "The inviolable and inalienable fundamental rights of MAN shall be respected. It is the primary obligation of the State to protect these rights."\(^7\) According to Article VI.: "(1) Everyone shall have the right to have his or her private and family life, home, communications and good reputation respected. (2) Everyone shall have the right to the protection of his or her personal data, as well as to access and disseminate data of public interest. (3) The application of the right to the protection of personal data and to access data of public interest shall be supervised by an independent authority established by a cardinal Act."\(^8\) The restriction of privacy is only allowed in cases provided by law, with respect to necessity and proportionality. Restrictions must be prescribed in public by law, and justifications must be corroborated by concrete circumstances.

Gathering covert information and data is an umbrella term of different manners in criminalistics. These methods infringe the fundamental human rights discussed above. The Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information defines that: "personal data may be processed only for specified and explicit purposes, where it is necessary for the exercising of certain rights and fulfilment of obligations. The purpose of processing must be satisfied in all stages of data processing operations; recording of personal data shall be done under the principle of lawfulness and fairness."\(^9\) As it states: "The personal data processed must be essential for the purpose for which it was recorded, and it must be suitable to achieve that purpose. Personal data may be processed to the extent and for the duration necessary to achieve its purpose."\(^10\) According to Section 5 subsection (1) "the personal data processed must be essential for the purpose for which it was recorded, and it must be suitable to achieve that purpose. Personal data may be processed to the extent and for the duration necessary to achieve its purpose."\(^11\)

This sort of restrictions appear in the Hungarian criminal law related to gathering covert information or data.

\(^7\) Fundamental Law of Hungary Title Freedom and Responsibility Article I. (1)  
\(^8\) Fundamental Law of Hungary Title Freedom and Responsibility Article VI. (1), (2), (3) 
\(^9\) Act CXII of 2011 on the Right of Informational Self-Determination an on Freedom of Information Section 4, subsection (1) 
\(^10\) Act CXII of 2011 on the Right of Informational Self-Determination an on Freedom of Information Section 4, subsection (2) 
\(^11\) Act CXII of 2011 on the Right of Informational Self-Determination an on Freedom of Information Section 5, (1)
Hungarian criminal law makes a strict distinction between gathering of covert information and data. The difference lies on whether the method is applied before the order of an investigation or after that. We talk about covert information gathering before the investigation is ordered. This is applied in the so-called pre stage of the investigation. Covert data gathering is possible to be applied after the investigation is already ordered until the documents thereof are presented during the trial. Hungarian criminal law disposes these two ways of gathering covert intelligence in different acts.

While covert information gathering is regulated in the Act XXXIV of 1994 on the Police, and in the Act CXXV of 1995 on the National Security Services, the Act XIX of 1998 on Criminal Procedure contains the rules of gathering covert data. Covert information gathering is performed by the police and national security services, covert data collection may be performed by the investigating authority or prosecutor.

The scope of grant is another discrepancy between the two manners. Covert intelligence gathering can be commenced under a separate legal regulation issued pursuant by the minister of justice or court but only the investigating magistrate can give the permission for gathering covert data. “Covert data gathering shall be permitted by the court at the request of the prosecutor”\(^\text{12}\). “The request shall contain the name of the prosecutorial body or investigating authority conducting the investigation, the date of the order for the investigation, the case number, if applicable, the type of covert intelligence gathering conducted prior to the order for the investigation or during the submission of the motion, the name of the organization conducting or having conducted such covert intelligence gathering and the data having been obtained thereby; the location planned to be subjected to covert data gathering, including, in the case of eavesdropping, the phone number; the name or data suitable for the identification of the person planned to be subjected to covert data gathering, as well as the description of the means and method of covert data gathering to be applied; the duration for which covert data gathering is planned to be maintained, specified in calendar days and hours; detailed description substantiating the conditions for the application as specified in Sections 201 and 202, thus especially the description of the underlying criminal offence and the data establishing suspicion that the criminal offence has been committed, the circumstances justifying that covert data gathering is indispensable, the objective thereof and facts establishing probable cause to believe that the evidence may be obtained by the means or method to be applied in the course of covert data gathering and if applicable, the reason for and the date of an exigent order”\(^\text{13}\). The court shall make the decision within seventy-two hours from the submission of the

\(^{12}\) Act XIX of 1998 Section 203 subsection (1)

\(^{13}\) Act XIX of 1998 Section 203 subsection (2)
request. When the court accepts the request whether fully or only partially it has to determine: “the subject person, the means and methods of covert intelligence gathering and the time period for which the above means and methods may be applied in respect of such subject person”\textsuperscript{14}. According to the subsection the Act rules: ”If the permission procedure caused a delay that would jeopardize the success of covert data gathering, the prosecutor may, for maximum period of seventy-two hours, order covert data gathering (exigent order). In this case, simultaneously with the order, the motion for the permit shall also be submitted. If the court has rejected the motion, a new exigent order may not be issued based upon the same facts.”\textsuperscript{15}

According to the Act on Criminal Procedure if covert intelligence gathering was commenced under a separate legal regulation issued pursuant to a judicial permit or the permit of the minister of justice prior to the ordering for an investigation, but then an investigation is ordered, then covert intelligence gathering may only be continued in compliance with the provisions of the Act as secret data gathering. In this case the Act XIX of 1998 is applicable in the later stages.

An important difference between gathering covert information and data is in the application of phase. Covert information gathering may be permitted for a maximum period of ninety days occasionally and after a new request may be extended for a further ninety days. In contrast covert data gathering may be permitted for a maximum period of ninety days and upon a repeated request the period may be extended for a further ninety days on one occasion. The emphasis is on one occasion, because this phrase implies that the never-ending extension is prohibited for covert data gathering and use as well.

However worth mentioning that Hungarian praxis on adjudication and justification of the criteria: “immediately” is still a thin ice to skate.

This warranty protects the fundamental right for private data. Nevertheless, the extension depends on the deliberation of the court, it is not mandatory. The extension is the own decision of the court which does not have to automatically meet the request. Ninety days is an objective deadline so the court is allowed to permit a shorter period of extension than ninety days. It means that the maximum period of gathering covert data is hundred and eighty days.

According to the Act XXXV of 1995 gathering covert information may be extended as many times as it is requested and permitted.

***

After the short overview of the main differences between the manners of getting covert intelligence, in the followings, we will take a look at the content of these legal institutions.

\textsuperscript{14} Act XIX of 1998 Section 203 subsection (4)
\textsuperscript{15} Act XIX of 1998 Section 203 subsection (6)
Two main aims are determined by criminal proceeding rules for which gathering covert information or data is possible: in order to establish the identity, locate or arrest the offender or to find means of evidence. It is clear to see the difference between fixity or constraint to the person and the procedural objective. Fixity to person means that the investigating authority or prosecutor needs information or data about the person concerned such as person concerned such as his or her identity to locate or arrest. Constraint to the objective is a similar term: the very criminal facts of the case determine the scope of the operation.

Covert intelligence gathering may only be conducted if obtaining evidence by other means reasonably appears to be unlikely to succeed if tried or would involve unreasonable difficulties, and there is probable cause to believe that evidence can only be obtained by covert data gathering.

“The subject of covert data gathering may primarily be the suspect, or the person who may be suspected of having committed the criminal offence based on the available data of the investigation.”\textsuperscript{16} This time the person concerned is the central point of gathering covert information or data. “Other persons may be subjected to covert data gathering, if data indicate that they have culpable communications with the person specified in subsection (1) or there is reasonable ground to suspect the same. The fact that an outsider person is unavoidably affected shall not be an obstacle to covert information or data gathering.”\textsuperscript{17}

“Covert data gathering may only be conducted in the private home and office of a lawyer acting as the defence counsel in a case, and in connection with the telephone line, other means of communication and correspondence (including electronically transmitted mail) of the lawyer, if there is reasonable ground to suspect that the lawyer has committed a criminal offence related to the case in progress against the defendant”.\textsuperscript{18} “Covert data gathering may be conducted in the visitors’ room for lawyers within a police detention room or the in a penal institution, if there is reasonable ground to suspect that the lawyer has committed a criminal offence related to the case in progress against the defendant.”\textsuperscript{19}

“Without informing the person concerned the investigating authority:

– keeps under surveillance and records the events in a private home with a technical device,
– learns and records with a technical device the contents of letters, other pieces of mail as well as communications made via telephone line or other means of communication,
– learns and uses data transmitted and stored by way of a computer system (hereinafter: covert

\textsuperscript{16} Act XIX. of 1998 Section 202 subsection (1)
\textsuperscript{17} Act XIX of 1998 Section 202 subsection (2)
\textsuperscript{18} Act XIX of 1998 Section 202 subsection (3)
\textsuperscript{19} Act XIX of 1998 Section 202 subsection (4)
We have to mention the accession of non-originally or additionally concerned persons. They are not directly under the covert intelligence gathering but necessarily suffering subjective, because their privacy also might be infringed. This situation is more than solicitous regarding the human rights safeguarding. Legal regulation contains warranty of the right for protection of personal data:

- the information and data about the uninterested and outsider person must be annihilated within eight days following the termination of covert information and data gathering. The reason of the termination has no importance in this question. The fundamental right for protection of personal data prevails with the annihilation of gathered data and information. As a warranty of the right for protection of personal data a record has to be written about the fact, circumstances and date of annihilation.

The committed or constantly being committed crime is the main point of gathering covert information and data when the aim is to find means of evidence. Covert information and data gathering are the same in the following aspect: their goal is to identify, locate or arrest the offender. The utilization of covert information or data is assigned, that means „the results of covert information or data gathering may only be used for the purpose of other criminal proceedings, and the results of covert intelligence gathering performed prior to the order for an investigation subject to a judicial permit or the permit of the minister of justice, may only be used for criminal proceedings.” That is why the investigating authority or the prosecutor has to annihilate the covert information or data gathered. For non originally concerned objects, the Hungarian legal system applies the same regulation as for the non originally concerned persons. The information and data about the uninterested and non concerned objects have to be annihilated within eight days following the termination of covert information and data gathering (prohibition of making a collection for further purpose).

“Covert information and data gathering may be applied if the proceedings are conducted upon the suspicion of a criminal offence, or an attempt of or preparations for a criminal offence which

- has been committed intentionally and punishable by five years' or more imprisonment
- is related to trans-boundary crime
- has been committed to the injury of a minor
- has been committed repeatedly or in an organised manner (including criminal offences committed for profit, in a criminal organisation and conspiracy),
- is related to narcotics or substances qualifying as such,

20 Act XIX of 1998 Section 200 subsection (1)
21 Act XIX of 1998 Section 206 subsection (3)
is related to counterfeiting of money or securities
- has been committed with a weapon."

“Covert data gathering shall be forthwith terminated by the prosecutor or the head of the investigating authority:
– in the case of an exigent order, the court has rejected the motion,
– the objective specified in the permit has been achieved
– the time period specified in the permit has lapsed
– the investigation has been terminated,
– its maintenance is unlikely to yield any result.”

If in the case of an exigent order, the Court has rejected the request: - “the data recorded so far shall be immediately annihilated.”

“A report shall be compiled on the performance of covert data gathering, detailing the process thereof, thus especially, the means and methods applied, the time period and location of the application, the natural persons, legal entities and organisation without a legal entity that had been affected by the covert data gathering, and the data obtained in the course of covert data gathering – and not annihilated – as well as the method, source, place and time of obtaining the data. The report shall allow to establish whether the provisions in the court permit have been complied with. The report shall also state whether the covert data gathering have achieved its objective, or the reason for failure.”

“The report shall be signed by the head of the prosecutorial body or investigating authority having performed the covert data gathering.”

The report may be used in the criminal proceedings as documents.

“Protection of the data produced and recorded during covert data gathering shall be the responsibility of the prosecutor or the investigating authority having performed the covert data gathering, in compliance with the provisions of the Act on State and Official Secrets.”

The fact of the covert data gathering is classified data as well as the data produced and recorded during the gathering.

“While covert data gathering in progress and thereafter until the report thereon is filed by the prosecutor with the documents, the fact of performing covert data gathering, as well as the data

22 Act XIX of 1998 Section 201 subsection (1)
23 Act XIX of 1998 Section 204 subsection (3)
24 Act XIX of 1998 Section 204 subsection (4)
25 Act XIX of 1998 Section 204 subsection (5)
26 Act XIX of 1998 Section 204 subsection (5)
27 Act XIX of 1998 Section 205 subsection (1)
produced and recorded in the course thereof may be disclosed only to the judge having issued the permit, the prosecutor and the investigating authority, further, by superior (senior officer) of the prosecutor and the investigating authority. Court documents related to the permission of covert data gathering may also be disclosed to the administrative superior of the judge having issued the permit.”28

“At the request of the judge having issued the permit, the prosecutor shall present the data obtained by covert data gathering until the time of such request. Should the judge establish that the permit has been misused, he shall, while in the event of other breach of law, he may terminate the covert data gathering. Such decision may not be appealed.”29

“If the prosecutor intends to use the result of covert data gathering as evidence in the criminal proceedings, the motion for the permit of the covert data gathering, the court decision and the report on the performance of covert data gathering shall be attached to the files of the investigation. If the documents are attached after disclosing the files of the investigation, the suspect and the defence counsel shall be notified thereof and be allowed to examine the attached documents. After being attached to the files of the investigation, the report concerning the performance of covert data gathering may be used as evidence in accordance with the rules pertaining to documents.”30

An outstanding importance has the rule that “the results of covert data gathering may only be used for the purpose of other criminal proceedings, and the results of covert intelligence gathering performed prior to the order for an investigation subject to a judicial permit or the permit of the minister of justice, may only be used for criminal proceedings – notwithstanding the general rules if the conditions set forth in Section 201 also apply to the given, or the other criminal proceedings, and the purpose of using the results corresponds to the original objective of covert data gathering or covert intelligence gathering.”31 The court has to make the whole documentation to be the substance of the trial and has to examine the legitimacy and truthfulness of the evidence during the deliberation of evidence. The evidence provided plays an important role next to other evidence, but not enough to prove the commission of the crime and culpability. The content of evidence has to be judged with the results of other means of evidence. The evidence provided by gathering covert information or data has to be judged in its entirety, details can not be used separately.

“The results of covert data gathering may not be admitted as evidence, if covert data gathering was terminated because in the case of an exigent order, the court has rejected the motion, or because its

28 Act XIX of 1998 Section 205 subsection (2)
29 Act XIX of 1998 Section 205 subsection (3)
30 Act XIX of 1998 Section 206 subsection (1)
31 Act XIX of 1998 Section 206 subsection (3)
maintenance is unlikely to yield any result, or because at the request of the judge having issued the permit, the prosecutor shall present the data obtained by covert data gathering until the time of such request. Should the judge establish that the permit has been misused, he shall, while in the event of other breach of law, he may terminate the covert data gathering, or if the person affected by the covert data gathering – without a court permit – is the defence counsel acting in the case, or a person who may not be heard as a witness or may refuse to testify.”

The result of gathering covert information which was permitted by the court may be used as evidence in the criminal proceedings if conditions of gathering covert information consist in relation of the crime might be testified, or the requesting authority of the covert information gathering forthwith ordered the investigate or forthwith lodged a complaint. The fact of gathering covert information based on the permission of the court is verified by the president of the Metropolitan Court in Budapest. The verification contains the data of the case permitted and the frames of the permission.

If the information or data is used as an evidence, it ceases to be classified data, unless it is classified data itself.

III. Non-domestic remedies for safeguarding private data concerned

1. Approach by the ECHR filter

The above-mentioned tools which are used during gathering of covert information may spell danger to the fundamental rights of the person affected and others in his atmosphere.

To make sure of ward off this danger, fundamental rights are set up in numerous legal documents. The Universal Document of Human Rights (hereinafter: UDHR)\(^{33}\) says in Article 12, that no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence. The Council of Europe agreed on the European Convention on Human Rights (hereinafter: ECHR)\(^{34}\) for collective enforcement of fundamental rights. Article 8 orders the right to respect for private and family life.

The Charter of Fundamental Rights of the European Union\(^{35}\) was formed by the Union to preserve and develop common values. Article 7 and 8 includes regulation for respect for private and family life and protection of personal data.

The regulation in this field has two levels, by the side of the international documents the national governments produced rules in compliance with the international documents above.

---

\(^{32}\) Act XIX of 1998 Section 206 subsection (4)

\(^{33}\) Adopted by the General Assembly of the United Nations on December 10, 1948

\(^{34}\) The Council of Europe agreed at Rome 4\(^{th}\) day of November 1950

\(^{35}\) 2000/C 364/01
The Fundamental Law of Hungary makes rules for right to the protection of his or her private and family life, home, relations and good reputation and right to the protection of his or her personal data in Article VI. When these rights provided in international and national documents, conventions, charters are endangered effective remedies are needed to recover those.

The European Court of Human Rights rules on individual or State applications alleging violations of rights set out in ECHR.

In case of trespass of the Charter of Fundamental Rights of the European Union citizens may challenge the legality of a measure in the General Court. But most instances begin before national courts. For example in the form of preliminary ruling, the European Court of Justice decides whether the EU law is properly applied or not.

In Hungary if a procedure infringes fundamental human rights or freedoms of the accused there are two types of remedies available. During the investigation the accused may protest a complaint within eight days of the statement presuming he/she deems the decision either deficient on legal or factual basis or unlawful. The accused may also file a complaint on constitutional basis supposing the judgement contravenes right provided in the Fundamental Law of Hungary. The proceeding Constitutional Court of Hungary admits complaint only if the damage of the Fundamental Law significantly affects the judicial decision or has a high fundamental influence. Fruit of the poisonous tree is an applicable doctrine in Hungary, therefore evidence gathered by illegally acquired information must be excluded.

The European Court of Human Rights (hereinafter: ECtHR or the Court) analyses – depending on the circumstances – the collection, the use, the disclosure of private data in the context of right to respect for private and family life.

The ECtHR interprets private life in a broad concept: as the right to identity and personal development, the right to establish and develop relationships with other people and the personal environment. In a case the Court stated that storing informations by a public authority related to an individual's private life amounts to an interference within the meaning of Article 8 and protection of personal data has a fundamental importance to a person's enjoyment of his or her right to respect for private and family life. Based on this the Court found Article 8. applicable for information contained in a criminal record because it is available for public authorities and linked to a person's

36 Case of E.B. and others v. Austria (Application nos. 31913/07, 38357/07, 48098/07, 48777/07, 48779/07)
private life. The applicants were convicted for homosexual acts with consenting adolescents within the age bracket of 14 to 18. This provision has been repealed and replaced therefore there has been a violation of Article 8 and in conjunction with Article 14.

Firstly the court decides, whether there has been an interference or not. If there is no interference then there is no violation of Article 8. In a case\(^{37}\), where a divorced mother had written an open letter in a newspaper for the Children's Rights Ombudsman complaining that the Children's Welfare Service had done nothing for her son in the custody proceedings. In this open letter the mother disclosed her and her son's forename and surname and other data. The Children's Welfare Service wrote an article about their work. It described the situations they are facing day-to-day. This article presented the custody proceedings, which previously was the subject of the open letter. It contained only the medical state of the boy without mentioning names and other data. The mother (applicant to this case) complained that the Children's Welfare Service had disclosed information regarding her private life and the health of her minor son. In the applicant's opinion she and her son were recognisable from the article and it has interfered with her right to privacy. The Court examined all the circumstances, and concluded that it was not possible to identify neither the mother nor the children from the article's content, thus there has been no interference under Article 8.

When there is interference with the rights under Article 8, then the Court studies if it was justified or not. The second paragraph defines the exceptions. According to that it has to be in accordance with the law and necessary in a democratic society, and enumerates the interests it has to be for.

To fulfil the obligation to be in accordance with the law has more requirements. It shall have a legal basis in domestic law which has to be accessible and precise enough to enable to foresee the possible consequences. In a case\(^{38}\) the national provisions did not meet this requirement because it has contained uncertain general terms and it has not defined with sufficient clarity the rules regarding home search. The Court stated that general terms cannot replace individual authorisation of a search. Two police officers contrary to the domestic law carried out a search at the home of the applicant who has not been there and has not given any permission to do so without the prosecutor authorisation. Therefore it is not necessary to examine whether the interference pursued a legitimate aim and was proportionate, because the interference was not lawful.

A legitimate aim and necessity has to justify the interference with Article 8. In a case\(^{39}\) 3 applicants who had non-blood management treatment complained that the prosecutor's office had asked for their medical files without consent and any criminal investigation warrant. This constituted an interference with the right to respect for their private lives. There was an accessible legal basis with

\(^{37}\) Case of Varapnickaitė-Mažyliene v. Lithuania (Application no. 20376/05)
\(^{38}\) Case of Kilyen v. Romania (Application no. 44817/04)
\(^{39}\) Case of Avilkina and others v. Russia (Application no. 1585/09)
foreseeable consequences in the domestic law for the prosecutor to the disclosure of medical files. Therefore it was in accordance with the law. The Government considered the protection of public health and the rights of individuals the legitimate aim. The Court did not find a fair balance between the applicant's right to respect for their private life and the aim mentioned by the Government and there has been no sufficient safeguard to prevent the disclosure of the medical data. The Court concluded that there has been violation.

The interference can only be justified if it is necessary in a democratic society. In a case\textsuperscript{40} the applicant was called upon to act as a court-appointed/registered expert. The applicant offered to draw up a report corroborating the claim for money in exchange. This offer has been disclosed and a warrant has been drawn up allowing the police to install covert listening devices and mark banknotes which would hand to the applicant. It was not disputed that by installing cover listening advice there would be an interference with the applicant's rights under Article 8. The Court deemed that the interference was in accordance with the law. The necessity of it was undeniable because it was used for the prevention of the serious crime of bribe-taking. The Court considered tapping of the telephone necessary in a democratic society for the protection of the rights of others in another case\textsuperscript{41}. The applicant was a public figure because of engagement in politics. At first he applicant was only the third party communicating with a later convicted person who was the subject of telephone tapping. This conversation has been disclosed in unidentified way via television. A conversation between the applicant and the State President had been tapped and used in the framework of Constitutional Court. The ECtHR declared that the tapping and disclosing the conversation between the applicant and the President is not a violation of the Article 8. The reason was that this conversation did not contain any details about the applicant's private life and it was necessary for protection of the rights of others. A violation has been occurred by the disclosure of the first conversation when the right to respect for his private life was damaged.

In the Court's judgements it is generally reiterated that the interference, the purpose and the necessity has to be proportionate. In a case\textsuperscript{42} the applicant was a suspect of participation in a terrorist movement. He was occasionally kept under visual surveillance, the entries of his flats were filmed by video cameras, the telephone in the house and telephone box situated nearby was intercepted. S. a person who the applicant spent time with had been the subject of the use of covert surveillances. A GPS receiver was built into S's car, and whenever they used the car together it was used on the applicants’ as well. The Court established that is was in accordance with the law. The applicant's surveillance was ordered in order to investigate a several counts of attempted murder.

\textsuperscript{40} Case of Goranova-Karaeneva v. Bulgaria (Application no. 12739/05)
\textsuperscript{41} Case of Drakšas v. Lithuania
\textsuperscript{42} Case of Uzun (Application no. 35623/05)
and it was applied to prevent further bomb attacks, it served the interest of national security and public safety, the prevention of crime and the protection of the rights of the victim. Therefore it was necessity in a democratic society and it is proportionate to the legitimate aim pursued. The visual surveillance and surveillance via GPS affected him only for shorter periods and very serious crimes was investigated. There was no violation in the Court's opinion.

The Court has set up common rules which have to be observed and which will guide an applicant throughout the case.

Based on the introduced practice of the Court a list of the most important steps can be made. It contains firstly to decide whether there has been an interference or not. If there has been one the next is to examine if it is justified or not. By this step the Court investigates if the measure is in accordance with the law. It shall have a basis in the domestic law and to be compatible with the rule of law. The law must to be accessible and foreseeable, it must afford adequate legal protection. The purpose of the law must be a legitimate aim and be necessary in a democratic society. The national security, public safety or the economic well-being of the country can be applied as an aim as well as the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. Proportionality is needed to ensure the balance.

In case of passing through this on a domestic Hungarian procedural filter it is similar, almost same.

2. Approaching the issue at the European Union’s Judicial Supremacy’s level

Before the Charter of Fundamental Rights of the European Union had become legally binding with the entry into force of the Treaty of Lisbon, the Court of Justice of the European Union (CVRIA) cited ECHR and judgements of ECtHR. In a preliminary ruling case the CVRIA decided on the interpretation of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the processing of personal data and on the free movement of such data when examined if a State control body collects and discloses data on the income of persons employed by the bodies subject to that control infringes the right to respect for private State or not. This decision states that ECtHR does not interpret private life restrictively and not only reiterates but applies the conditions defined by ECHR and EctHR. It scrutinizes the case with the requirements for justification of the interference. The national law is drawn up in a way that complies with the foreseeability as the paragraph is sufficiently precise to enable citizens to adjust his conduct accordingly. The legitimate aim for revealing the salaries and persons earning this salaries is to put pressure on public bodies to keep salaries within reasonable limits, resulting in preserving the economic well-being of the

43 In Joined Cases C-465/00, C-138/01 and C-139/01
country and serving the public interest by monitoring the proper use of public funds. The CVRIA leaves to the national courts to decide whether disclosure of this data is proportionate to the aim or not.

Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometric passports and travel documents issued by Member States was the subject to a case after the Charter became legally binding. Mr. Schwarz claimed that taking his fingerprints to issue his passport infringes his right to the protection of personal data laid down in article 7 of the Charter and it relates to the right to respect for private life located in Article 8. Article 52 (1) of the Charter allows the limitation of the exercise of that rights, as long as the limitations are provided by the law, respect the essence of those rights and in accordance with the principle of proportionality, necessary and meet the objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. The Regulation objects two specific aims to prevent the falsification of passports and fraudulent use thereof, practically illegal entry into the European Union. The CVRIA identified by checking whether there is measure which will interfere less, and if it is proportionate, that the protection against fraudulent use of passports justifies the interference and it does not go beyond what is necessary to achieve the purpose. The CVRIA is applying the same requirements when deciding a case concerning fundamental rights ensured in the Charter.

In case of passing through this on a domestic Hungarian procedural filter it is similar, almost the same. The Fundamental Law of Hungary Article I (3) declares that a fundamental right might only be restricted in order to allow the exercise of another fundamental right or defend any constitutional value. It introduces the requirements which are necessary to such a restriction. These are that it has to be the extent absolutely necessary, in proportion to the desired goal and in respect of the essential content of such fundamental right. Based on the cases introduced above, the practice of the European Court of Human Rights, the CVRIA and the Hungarian Constitutional Court applies similar premisses when deciding whether there has been a violation or not, and if there has been one is it justified or not, and the criteria to the justification.

Case C-291/12
IV. Conclusions:

1. As a result of the thorough analysis demonstrated above one should definitely make the statement that Hungary has been showing Legislative and Practical Compliance with the CoE’s and the EU legislative environment and architecture at a satisfactory and undoubtedly positive level almost since the very beginning of the new political-social-economic era (i.e. 1989).

2. Although European Union has produced its own Fundamental Legal Source as basic safeguarding tool for securing these elemental rights and freedoms it is clear that the CVRIA has been law-abiding to the ECHR. Some cases nevertheless display that the Charter of Fundamental Rights has also started to occupy its real place in the coordinate system of the Primary Law of the EU.

3. We would like to emphasize the importance of a possible theoretical “fusion” of the doctrines having been represented on the open surface of the jurisdiction rendered by the two great Judicial Supremacies: the ECHR and the CVRIA. This question however belongs to the subsidiary approach while it is indisputable that Parties of the CoE and MS of the EU might be reserving their judicial sovereignty in the field of Constitutional Jurisdiction on their own.

***

De lege ferenda proposals

In the field of European criminal law the EU has two basic tools: on the one hand, the harmonisation of Law and the Law Approximation, on the other hand, the principle of mutual recognition, which are essential prerequisites for the application of this legal principle in practice is that the Member States mutually trust each other’s legal systems. There is no doubt that the application of this principle raises the most difficulties in the field of criminal law. Concerning covert investigations the ‘regular’ tools obviously demonstrate controversial issues. It is a sensitive area of criminal law, with special regard to human rights.
Therefore a need for uniform rules for cooperation in combating crossborder crime should mean actions and normative legal prescriptions on a EU (and CoE) level eligible to give an adequate response to the request: quickly and effectively accept the evidences from other MS deriving from a trustable cooperative investigative source even breaking through the digital borders.

In our opinion in the future of Europe there will be better opportunities than the actual ones in the area of secretful methods and covert investigations.

Besides the above mentioned tools, such as the harmonisation of Law, the Law Approximation and the principle of mutual recognition, are those different solutions providing the healthy and EU-law conform working of non-EU bodies and offices. Toward the current institutions, rationale of the European Public Prosecutor’s Office (hereinafter EPPO) are for a more effective and harmonised fight against frauds damaging the Union’s financial interests. The European Union has a special responsibility to protect the Union’s own financial interests against fraud, corruption and similar offences, but at this stage it is an ongoing legislation. On 17th July 2013, the European Commission proposed a regulation on establishing the EPPO. According to the proposal, Article 27, the EPPO shall have the power to request or to order investigative measures when exercising its competence in connection with the covert investigations. For instance, EPPO shall intercept telecommunications, including e-mails, to and from the suspected person, on any telecommunication connection that the suspected person is using; undertake surveillance measures in non-public places, by ordering the covert video and audio surveillance of non-public places, excluded video surveillance of private homes, and the recording of its results; undertake covert investigations, by ordering an officer to act covertly or under a false identity.45 Fort he time being this is just a proposal, but according to our standpoint, this kind of ruling might make covert investigations more “slippery”, besides we would like to emphasise the application of 'ultima ratio' when using covert measures by the EPPO.

There are other more significant challenges in the field of crossborder actions. Crimes across the digital borders signify a special area, so it requires special concentrated action. From 1 January 2013, the European Cybercrime Centre (hereinafter EC3) commenced its activities, as a special agent of the Europol. The EC3 will be focusing on the EU’s fight against cybercrime, contributing to faster reactions in the event of online-commited crimes, subserving operational and analytical capacities for cybercrime investigations.46

In our point of view, the EC3 speeds up, simplifies and increases the efficiency of investigative

---

procedures, and it is desirable to cooperate and support the competent authorities of the EU and the MS in preventing or combating the forms of cybercrime in more and more actions. Furthermore, cybercrime, which almost demands the use of covert investigations will be definitely more effectively defeated by providing these state-of-the-art tools.

Consequently, the constant developments within the EU evidently will show up very significant consequences for the legal civilization of our century. Considering this process however, one could find numerous questions raised in connection with the covert investigation:

- is it justifiable to limit the competence of Member States in settling the covert investigation on the grounds of the efficiency objective, or on the grounds of the vision of creating the Area of Freedom, Security and Justice? If we believe in the maximum advantage theory or in the utilitarian approach, the realization of deeper integration should be welcome. We think the concept of the European Criminal Justice System's \textit{conditio sine qua non} also follows this line of thought. We would say that this substance consists of the establishment of safeguards for keeping the balance between the protection of legal goods and the guarantee of people’s freedom through the Constitutions of member states as well as through the Charter of Fundamental Rights and the European Convention on Human Rights in order to be able to control all the observed deviances.

***

The Hungarian Team:

\textit{Miss Dalma MOLNÁR}

\textit{Miss Orsolya HORVÁTH}

\textit{Miss Andrea SZABÓ}

Judicial trainees

\textsuperscript{47} The concept of a European Criminal Justice System is then used with reference to the emerging system structure of the European Union level and that is therefore centred on the function to implement the growing body of an autonomous European criminal law.