

Admissibility of Wiretaps

Audio vs. Transcripts in Criminal Proceedings

Tamás BÁLINT¹

Introduction: The use of wiretap recordings obtained through covert intelligence gathering and the use of covert devices as evidence in criminal proceedings has long been a subject of scrutiny, particularly with regard to their probative value and objectivity. At the same time, it is unclear whether the contents of transcripts prepared during the analysis of audio recordings can be used without playing the original recordings, or to what extent the reading of such transcripts in court proceedings complies with the requirements of due process.

Objectives: The aim of this study is to determine under what conditions audio recordings obtained through wiretapping conducted during covert information gathering and the use of covert devices, as well as their transcripts, may be considered objective evidence in criminal proceedings.

Methodology: The research is based on a dogmatic legal analysis grounded in the interpretation of the evidentiary system of criminal proceedings and the legal framework governing the use of covert intelligence gathering and covert devices. In this study, the author compares the specific characteristics of audio recordings and transcripts as interpreted in the context of evidence based on objective evidence, taking into account the principle of the directness of judicial evidence and the requirements for the enforcement of rule-of-law guarantees. The analysis places particular emphasis on the issue of the objectivity of evidence, as well as the examination of potential sources of distortion arising during the evidentiary process.

Results: According to the results of the study, the hearing of original audio recordings obtained through covert information gathering and the use of covert devices during a trial ensures the highest degree of objectivity in evidence, as these directly reflect the full context of the communication, including emphasis, intonation and other nonverbal elements. In contrast, transcripts are necessarily the result of an interpretive process, during which the selection, structuring, and

¹ PhD candidate, Ludovika University of Public Service, Doctoral School of Law Enforcement, e-mail: balint.tamas@stud.uni-nke.hu

linguistic recording of content are influenced by subjective factors. Transcripts may therefore distort the original meaning and are unable to fully convey the informational content of audio recordings. The study also highlights that the use of transcripts as exclusive or primary evidence may violate the principles of immediacy and due process.

Conclusion: The primary finding of the research is that, in criminal proceedings, only the original audio recordings obtained through covert information gathering and the use of covert devices can be considered fully valid as objective evidence. Another important finding is that transcripts can only be used in a supplementary capacity, in conjunction with the audio recordings, and cannot be endowed with independent probative value. A relevant direction for future research is to examine how technological advancements – particularly artificial intelligence-based audio processing – may influence the assessment of the evidentiary value of audio recordings and transcripts.

Keywords: secret information gathering, wiretapping, audio recording, transcription, criminal proceedings, objective evidence, judicial authorisation, evidentiary procedure, metadata

Introduction

The use of covert intelligence gathering and covert devices is an indispensable yet constitutionally sensitive area of modern criminal justice. As a result of the development of digital communication, the use of data derived from wiretaps for evidentiary purposes raises new questions regarding legal interpretation and procedural conduct. The central question of this study is not to establish a hierarchy of evidentiary tools, but to examine under what safeguards, within the framework of Act XC of 2017 on Criminal Procedures (hereinafter: Be.), audio recordings and transcripts thereof may be evaluated during court proceedings.

The need for covert information gathering and the use of covert devices as tools for criminal investigation and crime prevention emerged at the same time as the development of criminal procedure; however, the continuous refinement of the statutory provisions governing this legal institution has become – and will continue to become – necessary in the future, keeping pace with the ongoing advancement of forensic technology. As law and technology evolve, it becomes necessary from time to time to establish increasingly detailed rules regarding the collection of confidential information and the use of covert investigative tools. The legal framework surrounding authorisation, issues of verifiability, usability and legality, as well as the protection of fundamental human rights affected by these measures and the criteria for their restriction, are the detailed rules that require continuous development.

A key conceptual element of the tools used for covert information gathering and the use of covert measures is that their application occurs without the knowledge of those affected; and their use involves a deep intrusion into the private sphere of those concerned

and surveillance in order for the authorised authority to obtain information regarding criminal offenses and offenders.

The covert surveillance of communications is one of the most sensitive areas of a democratic state governed by the rule of law, as state intervention directly affects the right to privacy and the constitutional protection of the secrecy of correspondence and communications (Act CXXV of 1995). As a result of the rapid development of digital technology, forms of communication have become extremely diverse: in addition to traditional telephone calls, encrypted messaging apps, internet-based voice calls, social media platforms, and other data transmission channels have emerged. At the same time, the technical and procedural legal frameworks for wiretapping have also become more complex.

In Hungary, the National Security Service (hereinafter: NBSZ) is responsible for the technical implementation of wiretapping activities; as a specialised agency with nationwide jurisdiction, it provides the technical infrastructure necessary for the collection of classified information. However, the NBSZ is not a decision-making body but an executive one: in all cases, a judge, prosecutor, or minister is authorised to order wiretapping measures based on the relevant statutory authorisation.

The audio recordings generated during wiretaps are the most important products of covert intelligence gathering. If the recorded conversations can be linked to a criminal offense, the recordings – *subject to appropriate safeguards* – may also be used as evidence in criminal proceedings. However, domestic judicial practice varies regarding the inclusion of audio materials obtained as a result of wiretapping activities conducted during covert intelligence gathering or the use of covert devices as part of the record of judicial proceedings.

Among the courts operating in various regions of Hungary, some allow the audio recordings obtained as described above to be played during evidentiary proceedings, while others have the transcripts of the audio recordings read aloud, or, in some cases, display the text of the transcripts while the audio recordings are being played; I have also encountered a “solution” where, in connection with the hearing of the audio recordings, the defence counsel is summoned to listen to the recordings outside the courtroom and to submit comments during the proceedings.

However, many domestic courts do not listen to the entire audio recording but instead use a written transcript prepared from it, which allows the content of the conversation to be assessed quickly and clearly. Thus, the accuracy, completeness, and verifiability of the transcript become a key factor in a fair trial (JANCSÓ 2018).

In this study, I seek to evaluate from a procedural law perspective the manner in which audio recordings obtained during the investigative phase through covert information gathering or the use of covert devices – specifically, those obtained through wiretapping – are utilised in the judicial phase I seek to evaluate, from a procedural law perspective, the manner in which such audio recordings must be utilised when they are admitted as evidence, because, as noted above, domestic judicial practice varies significantly regarding how audio recordings generated through covert information gathering or the use of covert devices are utilised as *evidence – specifically, regarding their content* – during the evidentiary proceedings before the court.

While numerous authors have analysed the legal framework governing the admissibility of evidence obtained through covert information gathering or the use of covert devices, I consider the number of scholarly analyses focusing on the inclusion of such data in the case file to be extremely limited.

Research methodology and sources

The research is based on normative and dogmatic analysis, supplemented by domestic judicial practice and the relevant case law of the European Court of Human Rights. The study focuses not on the technical details of implementation, but on the guarantees applicable in the evidentiary process and the verifiability of evidence.

In preparing this study, I employed normative, dogmatic, criminalistic and comparative methods. As part of the normative analysis, I reviewed the main laws regulating wiretapping: Act CXXXV of 1995 on National Security Services (hereinafter: Nbtv.), Act XC of 2017 on Criminal Procedures, and Act C of 2003 on Electronic Communications (hereinafter: Eht.).

The dogmatic analysis examines the theoretical framework of covert information gathering and covert means, with particular regard to the necessity-proportionality test, the authorisation mechanism, the safeguards for data processing, and the question of what constitutes objective evidence under criminal procedure law.

The forensic approach focuses on issues related to the metadata, integrity and expert examination of audio recordings. The comparative analysis, meanwhile, examines the case law of the European Court of Human Rights (hereinafter: ECtHR) – *in particular the cases of Szabó and Vissy v. Hungary, Zakharov v. Russia, and Weber and Saravia v. Germany* – which provide guidance for interpreting domestic regulations (European Court of Human Rights 2016; European Court of Human Rights 2015; European Court of Human Rights 2006).

Pursuant to the statutory provisions set forth in Sections 204–205 of Act XC of 2017 on Criminal Procedures, physical evidence includes any object or electronic data suitable for establishing the fact to be proven. This category includes both audio recordings made during wiretapping and their transcripts. Procedural law does not prescribe a predetermined probative value; the evaluation of evidence is based on the principle of free evaluation of evidence pursuant to Section 167 of the Be.

Restrictions on rights for law enforcement purposes applied in the Member States of the European Union and in Hungary

Restrictions on rights for law enforcement purposes applied in the Member States of the European Union

In the course of covert information gathering and the use of covert investigative techniques, the authorities authorised by law to permit and carry out these activities are

subject to a so-called additional obligation to justify and account for their actions before the courts. This so-called additional obligation to provide justification exists in contrast to cases of open evidence collection, since the use of these covert measures, by their very nature, takes place without the knowledge of the persons concerned, thereby necessarily precluding the presence of legal counsel and the possibility of legal remedy, which would otherwise arise as legitimate claims on the part of the persons concerned.

During the use of these tools, other fundamental rights derived from the right to privacy – such as the right to respect for private and family life, the home, communication and reputation, as well as the right to self-determination regarding the protection of personal data – may be infringed upon during covert surveillance.

The broader concept of covert intelligence includes covert intelligence for national security, counterterrorism and law enforcement purposes, the aim of which is not to prepare for criminal proceedings but to lay the groundwork for official measures that can be implemented using national security, counterterrorism and law enforcement tools (FINSZTER 2024).

The narrower concept of covert intelligence includes the gathering of information for law enforcement purposes, which is systematically situated within criminal proceedings (FINSZTER 2024).

Based on the provisions of national legislation enacted by the Member States of the European Union, criminal intelligence (covert and overt information gathering) is defined by the Criminal Procedure Act as the prevention of a suspected planned crime within the investigative authority's jurisdiction, the detection and disruption of a prepared or attempted crime, the detection of a committed crime, the acquisition of physical evidence and documents, the identification and location of the perpetrator for the purpose of apprehension, the recovery of property derived from the crime, the protection of participants in criminal proceedings, members of the prosecuting authority, and persons cooperating with the administration of justice, internal crime prevention and detection checks, the fight against terrorism, as well as covert or disguised information-gathering activities conducted for the protection of persons of particular importance and the security of undercover investigators and cover organisations (Act XC of 2017 on Criminal Procedures; European Union 2016; RATCLIFFE 2016; Europol 2020).

According to the European Union's technical document from Belgrade: "Special Investigative Means (SIM) refer to those special tools and methods used to covertly obtain evidence, information, or analyzed data without the knowledge of the person concerned. Their use invariably entails varying degrees of infringement of civil rights, and it is the responsibility of the investigating or judicial authority applying them to justify their legitimacy." The essence of special means is that, through their use, the authorised bodies prevent the commission of crimes or detect crimes, uncover the circumstances of the commission of crimes, identify the perpetrators, obtain information, and map out the perpetrators' potential network of contacts (Council of Europe Office in Belgrade 2013)

The purpose of secrecy is not to change the behaviour of the suspected perpetrator, but to obtain information (NYESTE–SZENDREI 2019). The restriction of fundamental rights necessarily entails the use of covert measures, as through these activities, authorised authorities intrude into the private sphere of the individuals concerned without their

knowledge, thereby restricting the right to privacy. However, a condition for the applicability of such restrictions on fundamental rights is that they must be proportionate and necessary.

The secrecy of the application means that the measures are carried out without the knowledge of the target person or persons; however, secrecy does not and cannot mean that the measures themselves or the rules governing them are secret, because measures restricting citizens' rights must be precisely defined and accessible under national law, and the purpose of secrecy is to obtain information.

The responsibility of the user lies in ensuring that, for the information and evidence obtained as a result of the use of these tools to be admissible, the entire procedure must comply with the rules governing special operations and the requirements set forth therein.

Restrictions on rights for law enforcement purposes subject to judicial authorisation in Hungary

In Hungary, covert measures subject to judicial authorisation during the preparatory proceedings discussed in Part Nine of Act XC of 2017 on Criminal Procedures may be used to establish suspicion of a criminal offense, against a person who may be considered a suspect in the commission of the crime, or who can reasonably be presumed to be in direct or indirect contact with a person who may be considered a suspect in the commission of the crime.

It is necessary to note here that the currently effective procedural law defines the concept of covert investigative measures in accordance with the foregoing, incorporating the most essential elements. Pursuant to the statutory provision set forth in Section 214(1) of the Be., the use of covert investigative measures constitutes a restriction on the fundamental rights to the inviolability of the home, as well as to the protection of private correspondence, the confidentiality of correspondence and personal data, and is carried out by authorised bodies without the knowledge of the person concerned (Act XC of 2017 on Criminal Procedures).

The Criminal Procedure Code, in accordance with European Union requirements, specifically stipulates that only authorities expressly authorised to do so may use covert investigative techniques for the purpose of carrying out their law enforcement duties as defined in the applicable legislation, and exclusively in accordance with the provisions of the law. The Criminal Procedure Code also sets forth the criteria for applicability, stipulating that covert investigative techniques may be used only if it can be reasonably presumed that the information or evidence to be obtained is indispensable for achieving the objective of the criminal proceedings and cannot be obtained by other means, and that its use does not entail a disproportionate restriction of the fundamental rights of the person concerned or of any other person in relation to the law enforcement objective to be achieved, and that its use makes it probable to obtain information or evidence. In the event that the use of covert devices subject to judicial authorisation is ordered, the authorising judge may review the use of the covert device from the perspective of legality; based on the provisions of the procedural law, the user is obligated to present the available

data within eight days upon the authorising judge's request (Act XC of 2017 on Criminal Procedures).

The legal status and scope of responsibilities of the National Security Service

In 1990, the National Assembly of the Republic of Hungary enacted Act X of 1990, which authorised the newly established national security services and the police to use special intelligence service tools and methods. Later that same year, the Government adopted Decree 26/1990 (II. 14.) MT on the transitional regulation of national security tasks, pursuant to which two civilian and two military national security services – the Information Office, the National Security Office, the Military Intelligence Office and Military Security Office – began operations on 1 March 1990. Following the 1990 – *so-called transitional* – law, the National Assembly enacted Act CXXV of 1995 on National Security Services (Nbtv.). The Nbtv. defines the National Security Service (NBSZ) – *separated from the National Security Office* – as the fifth national security service, an agency with jurisdiction over the entire territory of the country. By performing the tasks set forth in the law, and through the use of open and covert intelligence-gathering tools and methods, promotes the enforcement of Hungary's national security, law enforcement and criminal investigation interests. In terms of its position, role and tasks, it occupies a special position compared to the other services, as it does not perform law enforcement tasks independently but provides services exclusively upon the request of organisations authorised to do so (Főző 2020).

The legal status of the NBSZ is defined by Act CXXV of 1995 on National Security Services, which stipulates that the specialised service is a body belonging to the civilian national security services with independent tasks and powers. The NBSZ's task is not to detect crimes or conduct investigations, but to ensure the technical conditions for the collection of classified information. In this context, the NBSZ, on the one hand, establishes connections with the networks of telecommunications service providers, and on the other hand, ensures the operation of interception points, thirdly, records and archives the audio materials and related metadata, and finally, transmits the data in an authenticated manner to the ordering authority.

Telecommunications service providers are subject to a duty to cooperate under the provisions of Act C of 2003 on Electronic Communications: they are required to establish and maintain technical interfaces that enable lawful interception. This obligation includes the secure design of interception access points, traffic logging and the preservation of metadata integrity. The NBSZ's technical monopoly also requires extremely strict internal regulations, as security and data protection considerations directly affect the protection of fundamental rights.

The legal framework for interception

The legal basis for interception in Hungary is provided by two main regimes: interception for criminal proceedings and covert information gathering for national security purposes. The Criminal Procedure Code regulates the monitoring of communications among covert investigative measures, which may be used exclusively with a court order and under strict conditions. One of the basic conditions for ordering wiretapping is that there must be a suspicion of a serious criminal offense, and other, less intrusive measures are unlikely to yield results (Act XC of 2017 on Criminal Procedures, Sections 214–218; Act CXXV of 1995 on National Security Services, Sections 56–59).

Act C of 2003 on Electronic Communications requires service providers to retain cell data for individual mobile phones for three years (Act C of 2003 on Electronic Communications, Sections 159/A–159/B). Mobile service providers have thousands of cell towers nationwide, and based on these – or rather, the cells defined by the cell towers – a mobile phone's location can be determined using a method known as “triangulation”. A mobile phone connects to one cell tower at a time, but the others can also detect it. Therefore, it is perfectly clear at the central office which cell tower a mobile phone is connected to with what signal strength via its SIM card, and which of the other two towers can detect it: based on this data, the device's position can be determined with an accuracy of 50–100 metres. Maintaining and improving the security of public telecommunications networks, as well as ensuring their interceptability, is a matter of national security. Hungarian electronic communications providers are required to ensure technical conditions and cooperation enabling lawful access by competent authorities to subscriber-related traffic data, within the framework of statutory authorisation and procedural safeguards (Act C of 2003 on Electronic Communications, Sections 92, 157–159/A; Act CXXV of 1995 on National Security Services, Sections 56–59). However, domestic mobile operators do not record the content of either text messages or calls, as there is no data storage facility capable of holding such a large volume of data. It is noteworthy that in some Western European countries and the United States, there are automated eavesdropping systems that randomly intercept conversations on various mobile numbers and, if they deem them suspicious based on keywords (e.g. bomb, terrorist attack, etc.), adds them to a blacklist database and records traffic on the specified number for the following month.

In the case of *Szabó and Vissy v. Hungary*, the ECtHR ruled that Hungarian national security wiretapping regulations failed to meet the requirements of Article 8 of the Convention on several points, as the authorisation for surveillance was too broad and effective control mechanisms to prevent abuse were lacking (European Court of Human Rights 2016).

In the *Zakharov* case, the Court explained in detail that covert surveillance is compatible with the rule of law only if the law precisely defines the subject matter and duration of the surveillance, the rules governing access and storage, and ensures independent oversight and the possibility of subsequent legal remedy (European Court of Human Rights 2015).

Handling of wiretap recordings

The handling of audio recordings derived from wiretaps conducted by intelligence agencies is of paramount importance from an evidentiary standpoint. During digital recording, not only the audio material itself but also a significant amount of metadata is generated: timestamps, channel identifiers, file identifiers and hash values. Together, this metadata verifies the authenticity and integrity of the recording.

In forensic and judicial practice, the integrity of the chain of custody must be ensured, meaning that every handling step of the evidence must be documented; otherwise, the reliability of the evidence may be questioned, potentially leading to its exclusion (Act XC of 2017 on Criminal Procedures, Sections 165–167; European Court of Human Rights 2010; CASEY 2011).

In general, it can be stated that in all ongoing criminal proceedings where covert information gathering subject to judicial authorisation or covert devices were used as part of the investigation, the complete original audio recording is available and may be played during court proceedings as evidence.

The role of transcripts and requirements for their preparation

According to the author's explicit position, in Hungarian judicial practice, audio recordings and/or their transcripts serve as "practical" means of evidence. Upon examining the uniformly established and consistently applied judicial practice, we find that, during the evidentiary proceedings it conducts, the court presiding over the criminal proceedings plays back the audio recordings – in the presence of the prosecution, the defence, and, of course, the court, or makes the content of the conversation available to the parties in writing, in a clear and understandable form.

It can be stated unequivocally, however, that a transcript based on audio recordings can never constitute so-called "self-evident" evidence; it must always be interpreted in conjunction with the original audio recordings. Therefore, I fully agree with the position represented by defence attorneys in criminal proceedings that the original audio recordings can be considered objective, direct evidence, while transcripts prepared from the audio recordings are so-called secondary extracts that also contain subjective elements.

When preparing a transcript from audio recordings obtained through covert information gathering or the use of covert devices, accuracy, completeness and objectivity must be fundamental principles. Thus, according to the established theoretical position, the transcript must, as far as possible, reproduce the content of the conversation verbatim or in a manner very close to it (BÓCZ 2004; TREMMEL 2006). The prohibition of interpretative additions is not explicitly codified, but it follows from the requirement of authenticity and reliability of evidence, as established by statutory provisions and judicial practice.

Although not exhaustively codified in a single provision, the required elements of transcripts derive from procedural law requirements concerning documentation and reliability of evidence, data protection obligations, and established forensic standards

(Act XC of 2017 on Criminal Procedures, Sections 78–79, 165–167; European Union 2016; CASEY 2011).

On this issue, the author takes the position that in those rare cases where the original audio recording is no longer available, but the documentation of the transcription's creation and authenticity is adequate, the court may still admit it as evidence with limited probative value. However, this is an exceptional situation that requires heightened caution when evaluating the evidence.

Preparation of transcripts during the review of wiretap recordings obtained through covert intelligence gathering or the use of covert devices

The processing of audio recordings made during covert intelligence gathering is one of the most sensitive and labour-intensive areas of modern criminal justice. Transcripts are the structured, textual representation of raw audio material, which investigative authorities, experts, and the prosecution use for the purpose of evidence analysis. The process is subject to strict legal, procedural and professional requirements, as covert information gathering deeply impacts privacy and human rights safeguards; therefore, content irrelevant to the case in question must be deleted.

Transcription preparers

In Hungarian practice, the text transcripts of wiretaps are primarily prepared by two groups of actors:

- Police operational analysts and investigators: The primary preparation of transcripts is carried out by analysts, operational officers, or designated professional staff of the agency conducting covert intelligence gathering – typically a specialised criminal investigation unit. Their task is to organise the recordings chronologically, identify the participants (if possible), accurately describe the essence of the conversations, and highlight and mark the relevant sections. The first transcript is always a working draft, which is later subjected to multiple reviews.

- Forensic linguists or audio experts: If the accuracy of the transcript is disputed, if the audio quality is poor, if identification based on the audio is necessary, or if the defence raises an objection, a forensic expert prepares an authentic, professionally validated transcript.

The experts use specialised software (e.g. audio filtering, spectral analysis) to clean up and clarify the content of the audio recording (NYESTE–SZENDREI 2019).

Methodology for transcription

Transcribing wiretaps into text is not merely a matter of transcribing speech; it requires the creation of a structured, protocol-like document.

Each paragraph of the transcripts is time-stamped, allowing for parallel tracking of the audio material and the text. The identification of speakers can also be indicated with the labels “male voice”, “female voice”, or “unknown voice” if personal identification cannot be established.

In police practice, there are two types of transcripts:

- verbatim transcript: a detailed, word-for-word version that marks interruptions and unintelligible parts
- summary: an excerpt presenting the essence of the conversation, which is often attached to case files

In Hungarian criminal procedure, a summary of a recorded communication – presenting the essential content of the conversation – is often prepared and attached to the case file. Although such summaries are not regulated as a distinct legal institution, their use derives from the general rules on the documentation of procedural acts and the admissibility of documentary evidence. Consequently, summaries function as auxiliary evidentiary documents that facilitate the processing and evaluation of extensive material within the framework of criminal proceedings.

In cases of disputed content, judicial practice generally accords priority to the original audio recording or a verbatim transcript, as these provide a more reliable and direct representation of the evidence (Act XC of 2017 on Criminal Procedures, Sections 163–167; European Court of Human Rights 2010, 2015).

Accuracy requirements and verification

Two main criteria apply during the verification of the transcript:

- consistency with the audio recording
- authenticity and impartiality, which are validated by multiple verifiers

The European Court of Human Rights has consistently held that secret surveillance measures are compatible with Article 8 of the Convention only if they are carried out within a clear, accessible and foreseeable legal framework providing adequate safeguards against abuse (European Court of Human Rights 2015, paras. 229–230; European Court of Human Rights 2016, paras. 56–63).

This directly impacts the practice of preparing transcripts, which must be transparent, regulated and verifiable.

Covert surveillance can only remain within the framework of the rule of law if the documentation – including the recording of audio, the handling of metadata and the preparation of transcripts – is carried out in a transparent, verifiable and accountable manner.

Section 246 of the current Criminal Procedure Code regulates the rules regarding the deletion and retention of data generated during the use of covert devices. Accordingly, within thirty days of the termination of the use of covert devices, all data that is not related to the purpose of the device's use must be deleted, as well as all personal data that is not necessary for the purposes of criminal proceedings, and – *with the exception of the data specified in Section 346(2)* – all data that cannot be used as evidence in criminal proceedings. In the preparatory proceedings or the investigative phase, the member or head of the authority conducting the proceedings may decide on the destruction of data, while in the trial phase – *although practice does not always reflect this* – the prosecutor exercising supervisory authority may decide based on the results of the use of the device, and may even formalise this decision in a ruling.

The scope of means of proof in criminal proceedings

In Hungarian criminal procedure, the purpose of evidence is to enable the court – and where necessary the prosecution and investigating authorities – to establish the facts of the case truthfully, comprehensively and beyond reasonable doubt (TREMMELE 2006; KIRÁLY 2008; Act XC of 2017 on Criminal Procedures, Sections 163–165).

The Hungarian Criminal Procedure Code adopts an open system of evidence, according to which any means of proof may be used, provided that it is suitable for establishing the facts of the case and has been obtained lawfully [Act XC of 2017 on Criminal Procedures, Sections 163(1), 164(1)–(2), 165(1)].

The statutory provision set forth in Section 165 of the Criminal Procedure Code expressly lists the types of evidence; however, the list is not exhaustive. The essence of the system is that any material, personal, or digital information compatible with the purpose of criminal proceedings may be evaluated as evidence, provided that it does not violate any prohibitions and its acquisition does not infringe upon fundamental rights.

The current Criminal Procedure Code regulates the handling of data generated by covert devices, their evidentiary role, and the obligation to document them in the context of the use of covert devices. In this regard, it should be emphasised that Section 243(1) of the Criminal Procedure Code clearly stipulates that “a report or record must be prepared” regarding the use of covert devices, which serves as one of the guarantees for subsequent evidence.

According to the Commentary on Section 243(1) of the Criminal Procedure Code, the investigating authority is also required to prepare a report or record regarding covert investigative measures. In accordance with the general rules on records, the report and the official record must indicate the competent authority (prosecution service, investigating authority or authorised body) as well as the case number [Act XC of 2017 on Criminal Procedures, Section 79(1)]. The report must include the description of the criminal offense forming the basis of the proceedings, the name of the suspect or the person concerned, or a designation suitable for identification, the place and time of the procedural act, the names of the prosecutor, the member of the investigative authority, the recording clerk and the interpreter, the names of any other persons present during the use of the covert

device, and their capacity in relation to the procedural act. The record must contain, in the necessary detail, the course of the procedural act, the events that occurred during it, and other circumstances relevant to the evidence, such that it can be determined from the record whether the procedural rules were observed. The record must include the name of the prosecutor or member of the investigative authority present during the use of the covert device, the location and time of the use, the names of the persons involved, the names of other persons present during the use of the covert device and their capacity, and a brief description of the course of the use of the covert device, such that it can be determined from the record whether the procedural rules were observed. When using covert devices, the general rules shall apply *mutatis mutandis*, and it is incumbent upon the authority authorised to use the covert device to prepare a report or record of the operation. It is generally advisable to prepare a report on the use of a criminal trap, not a memorandum. It is also advisable to draw up a report regarding the prospect of avoiding criminal liability, surveillance conducted with consent, covert investigation, or the covert inspection of mail. In the latter cases, it is advisable to simultaneously make video and audio recordings. However, if false or misleading information is provided to the person concerned, this may affect the lawfulness and evidentiary value of the report, potentially leading to its exclusion from the evidence [Act XC of 2017 on Criminal Procedures, Sections 78–79, 165(1)].

Unless otherwise ordered by the prosecutor, reports or records related to covert surveillance measures do not form part of the case file until the conclusion of the operation. While such reports constitute documentary evidence, the probative value of data recorded by technical devices is generally considered higher due to their more direct and less mediated nature [Act XC of 2017 on Criminal Procedures, Sections 216(6), 217(3), 167(1)].

Pursuant to Section 249(1) and Section 250 of the Criminal Procedure Code, data derived from covert devices – *including audio recordings made with technical devices* – expressly constitute part of the case file; however, they must be handled separately until the use of the covert device is concluded, and therefore cannot be considered case files that are fully accessible.

According to the case law of the Hungarian Supreme Court (Curia), the evidentiary value of recorded communications depends on their verifiability and proper documentation; therefore, in disputed cases, the content of such recordings must be reliably reconstructed, typically by means of a verbatim transcript.

The Supreme Court's practice confirms that neither audio recordings nor transcripts have predetermined probative value. In cases of disputed content, however, listening to the audio recording is an indispensable tool for verifying authenticity.

The fundamental principle of Hungarian criminal procedure is the free evaluation of evidence, under which the court freely assesses all evidence. At the same time, the unlawful acquisition of evidence may affect its admissibility, as reflected both in the Criminal Procedure Code and in the case law of the European Court of Human Rights, which examines whether the use of such evidence compromises the overall fairness of the proceedings [Act XC of 2017 on Criminal Procedures, Sections 163(1), 165(1)–(2);

European Court of Human Rights 1988, para. 46; European Court of Human Rights 2010, paras. 89–90].

In the case published under No. Bf.199/2024/18, the Budapest Court of Appeal noted that, pursuant to Section 167(4) of the Criminal Procedure Code, when evaluating evidence, the authorities freely form their convictions by weighing the evidence in accordance with the rules of logic and reason within the system of evidence defined in the Criminal Procedure Code. Section 167(3) of the Criminal Procedure Act also stipulates that evidence does not have a preset probative value under the law. Accordingly, transcripts of wiretaps constitute evidence in their own right; typically, they represent manifestations of the same evidence in a different source or form of evidence, and their creators are responsible for their factual accuracy, thus they may be subject to evidentiary evaluation. There is no doubt that the recorded audio recordings may even serve to refute the transcripts; however, the necessity of their hearing is not a matter related to the legality of the evidence, but rather to the clarification of the facts, which does not concern usability, but rather its well-foundedness.

The defendant's and the defence counsel's full access to the audio materials is primarily a prerequisite for the exercise of the right to a defence and one of the means of establishing the authenticity of the transcripts derived from them; thus, their playback during the trial may be necessary if the content of the transcripts or excerpts prepared from them is reasonably disputed, or if their authenticity cannot be assessed in any other way.

The necessity of hearing the complete audio material obtained during wiretapping as evidence in court proceedings

In this study, I take the position that the hearing of the original, available audio recordings during a trial may be classified as objective evidence as interpreted under the Criminal Procedure Code, regarding which the defendants and their defence counsel, as well as the representative of the prosecution, may make comments and submit motions.

It should be noted that courts currently engaged in judicial practice apply differing standards regarding the use of audio recordings obtained through wiretaps conducted with judicial authorisation – carried out during covert information gathering or the use of covert means – in evidentiary proceedings, specifically when incorporating the content of such recordings into the case file.

In criminal proceedings pending before the Budapest Metropolitan Court of Appeal as the court of first instance under case number 19. B.487/2022, the court did not play the audio recordings obtained during the investigation in the evidentiary proceedings because neither the defence attorneys, nor the defendants, nor the representative of the prosecution requested the playback of the audio recordings; they were satisfied with the reading of the transcripts.

In the criminal proceedings pending before the Gyula Regional Court as the court of first instance under case number 2.B.35/2024 – which, however, has not yet been finalised with legal force – the court of first instance, upon a motion by the defence

counsel, requested the defence counsel to specify in detail those communications which he proposed be heard during the evidentiary proceedings. When the defence counsel identified all relevant communications – *individually and identifiably* – the court rejected the defence counsel’s motion because, in the court’s view, hearing the audio recordings would lead to a prolongation of the proceedings. In this regard, the prosecuting attorney proposed to the defence that it listens to the audio recordings obtained during the investigation outside of the trial and submit written comments regarding their content. Subsequently, the court refrained even from reading the transcripts aloud during the trial – *from including them in the record of the proceedings* – but referred to this evidence on several occasions in the findings of fact of the first instance judgment.

In the criminal proceedings pending before the Győr Regional Court as the court of first instance under case number 38. B.9/2023, ordered that the relevant audio recordings be played in their entirety during the evidentiary proceedings, while comparing the content of the transcripts – displayed via projection – with the content of the audio recordings.

In light of the above, I must take the position that in criminal proceedings, only the hearing of legally admissible audio recordings during the trial can be considered evidence.

In my view, the mere reading of transcripts during the evidentiary proceedings cannot be considered objective evidence, because a certain subjective element arises during the preparation of the transcripts: the evaluative activity of the analyst who prepared them, which manifests itself in the fact that, while listening to the available audio recordings, it is up to the analyst’s subjective decision as to which content is considered relevant.

Furthermore, in my view, the reports prepared by the analyst in question while listening to the audio recordings would be considered objective evidence only and exclusively if the court were to hear the author of the report as a witness regarding why, during the review of the audio recordings, they deemed it important to highlight precisely the content included in the report (transcript). It is not inconceivable that, during the listening to the audio recordings, other content might also be deemed important by the prosecution, the court, the defendants, or possibly the defence.

In my view, during the evidentiary proceedings to be conducted by the courts, it is not necessary to present what an unknown person – *who, while listening to the otherwise fully available audio material, prepared so-called excerpts from it* – considers relevant from a given conversation, but rather what was actually said, since the contents of the reports generated during the review of the audio recordings merely reflect the subjective judgment of the analysing officer. I wish to note here that while the contents of the transcripts may in themselves assist in guiding the direction of the investigation, they cannot be evaluated with complete objectivity in the evidentiary proceedings before the court.

Furthermore, it is not only the content of the conversations that is significant; the parties’ tone and intonation carry equal weight, and these cannot be reconstructed even from verbatim transcripts. (I refer here to the famous ambiguous statement by Archbishop János of Esztergom regarding the murder of Gertrudis: “Reginam occidere nolite timere bonum est si omnes consentiunt ego non contradico”.)

For the reasons stated above, any misunderstandings that may arise in audio recordings obtained through covert information gathering or the use of covert means

can only be clarified through comments, motions, questions which may only take place during their hearing.

I must take the position in this regard that if the court intends to consider audio recordings made from legally obtained wiretaps as objective evidence when rendering its judgment, then it is necessary to include them in the trial record through their hearing.

In my view, during the presentation of evidence by the court in criminal proceedings, it is not necessary to describe what an unknown person considers relevant from a given conversation, but rather what was actually said, since the content of the read-out reports merely reflects the subjective assessment of the specific analyst who transcribed the audio recordings obtained during the wiretapping; therefore, the objectivity of the content conveyed in the transcripts may be called into question.

Furthermore, I maintain that it is absolutely necessary to play the audio recordings made during the wiretap in court proceedings, even if the defendant, the defence, or the representative of the prosecution does not request that the audio recordings be played.

The clear reason for this is that the principle set forth in Section 163(4)(c) of the Criminal Procedure Code – *that there is no need to prove facts whose truth is jointly accepted by the prosecutor, the defendant and the defence counsel in the given case* – must not be confused with the legality of evidence as interpreted under the Criminal Procedure Code. For while in the former case there is no need to conduct a trial at all, in the latter case it is the court's duty to ensure compliance with the legality of the evidentiary proceedings conducted.

Thus, if the court expressly fails to order the playback of audio recordings made through wiretaps during the evidentiary proceedings at the trial because any participant in the proceedings waives this right, it violates the provisions regarding the legality of evidence.

The Budapest Court of Appeal, in its Order No. Bf/7/2021/169, overturned the judgment of the Budapest Regional Court No. 1.B.346/2015/286-I and explained that

“[312] The court of first instance failed to conduct the examination described above – namely, a substantive analysis of the volume of information – and indeed precluded any possibility of doing so when it did not include the wiretap material in the trial record and did not conduct the relevant evidentiary proceedings. Consequently, its conclusion regarding the violation of the principle of immediacy – that is, the reason for excluding the evidence – became unfounded and devoid of any factual basis. All of this, incidentally, led to such a degree of lack of investigation in the first instance judgment that it cannot be remedied in the second instance proceedings”.

Summary

It can be stated that the purpose of criminal proceedings and, at the same time, the duty of the courts participating in criminal proceedings is to reach a well-founded and free from doubt judgement regarding the defendant's guilt. To achieve this objective, it is necessary during the evidentiary proceedings to examine the evidence obtained

during the investigation and its objectivity. Such evidence may include the content of wiretaps lawfully obtained through covert information gathering or the use of covert devices, which can be evaluated as evidence within the framework of the rule of law, while fully preserving procedural guarantees, by listening to the audio recordings within the context of the evidentiary proceedings and by ensuring the right of the defendants, the prosecution and the defence to make comments and submit motions.

References

- BÓCZ, Endre (2004): *Kriminalisztika 1–2* [Criminalistics 1–2]. Budapest: BM Kiadó.
- CASEY, Eoghan (2011): *Digital Evidence and Computer Crime*. Cambridge, Mass.: Academic Press.
- Council of Europe Office in Belgrade (2013): *Mutual Legal Assistance Manual (Criminal Asset Recovery Project in Serbia – CAR Serbia, EU-funded)*. Belgrad: Dosije studio.
- European Court of Human Rights (1978): *Klass and Others v. Germany* (Application No. 5029/71). Online: <https://hudoc.echr.coe.int/>
- European Court of Human Rights (1988): *Schenk v. Switzerland* (Application No. 10862/84). Online: <https://hudoc.echr.coe.int/>
- European Court of Human Rights (2006): *Weber and Saravia v. Germany* (Application No. 54934/00). Online: <https://hudoc.echr.coe.int/eng?i=001-76586>
- European Court of Human Rights (2010): *Bykov v. Russia* (Application No. 4378/02). Online: <https://hudoc.echr.coe.int/>
- European Court of Human Rights (2015): *Roman Zakharov v. Russia* (Application No. 47143/06). Online: <https://hudoc.echr.coe.int/eng?i=001-159324>
- European Union (2016): *Directive (EU) 2016/680 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA*. Online: <https://eur-lex.europa.eu/eli/dir/2016/680/oj>
- Europol (2020): *European Union Serious and Organised Crime Threat Assessment (SOCTA)*. Online: https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf
- FINSZTER, Géza (2024): A titkos eszközök alkalmazásának jogi alapjai [The Legal Basis for the Use of Covert Measures]. *Belügyi Szemle*, 72(6), 961–974. Online: <https://doi.org/10.38146/bsz-ajia.2024.v72.i6.pp961-974>
- FÖZŐ, Eszter (2020): 30 éve a szakértésben – az igazságügyi szakértői tevékenység múltja és jelene a Nemzetbiztonsági Szakszolgálat Szakértői Intézetben [Thirty Years of Expertise – The Past and Present of the Forensic Expert Activities in the Institute of Expert Services of the Special Service for National Security]. *Nemzetbiztonsági Szemle*, 8(1), 108–125. Online: <https://doi.org/10.32561/nsz.2020.1.7>
- JANCSÓ, Gábor (2018): Leplezett eszközök alkalmazása: titkos információgyűjtés az új büntetőeljárási törvényben [The Use of Covert Measures: Secret Information Gathering in the New Criminal Procedure Act]. *Acta Humana*, 6(1), 19–34. Online: <https://folyoirat.ludovika.hu/index.php/actahumana/article/view/880>

- KENESE, Attila (2013): *A titkos információgyűjtés és adatszerzés alkalmazása és eredményének felhasználása során felmerülő jogértelmezési kérdések a bírósági gyakorlat tükrében* [Legal Interpretation Issues Arising from the Application of Covert Information Gathering and Data Acquisition and the Use of Their Results in Light of Judicial Practice]. Online: www.jogiforum.hu/files/publikaciok/kenese_attila__a_titkos_informaciogyujtes_es_adatszerzes%5Bjogi_forum%5D.pdf
- KIRÁLY, Tibor (2008): *Büntetőeljárási jog* [Criminal Procedure Law]. Budapest: Osiris.
- NYESTE, Péter – SZENDREI, Ferenc (2019): *A bűnügyi hírszerzés kézikönyve* [Handbook of Criminal Intelligence]. Budapest: Dialóg Campus.
- POLT, Péter ed. (2018): *Kommentár a büntetőeljárási törvényhez* [Comprehensive Commentary on Act XC of 2017 on Criminal Procedures]. Budapest: Wolters Kluwer.
- RATCLIFFE, Jerry H. (2016): *Intelligence-led Policing*. Abingdon: Routledge. Online: <https://doi.org/10.4324/9781315717579>
- TREMME, Flórián (2006): *Bizonyítékok a büntetőeljáráásban* [Evidence in Criminal Procedure]. Budapest–Pécs: Dialóg Campus.