DECISION 36/2005 (X. 5.) AB

IN THE NAME OF THE REPUBLIC OF HUNGARY

On the basis of a petition submitted by the President of the Republic seeking the prior constitutional review of certain provisions of an Act of Parliament adopted but not yet promulgated, the Constitutional Court – with concurring reasoning by dr. László Kiss and dr. István Kukorelli, Judges of the Constitutional Court – has adopted the following

decision:

1. The Constitutional Court holds that Section 30 para. (3), the provision on the storage period of 30 days in Section 31 para. (2), and the provision on enforcing within three working days the right to informational self-determination in Section 31 para. (4) of the Act on the Regulation of Activities of Personal and Property Protection and Private Investigation adopted by the Parliament at its session of 2 May 2005 are unconstitutional.

2. The Constitutional Court holds that the provisions on the electronic visual surveillance system in Section 28 para. (2) and Section 29 para. (1) of the Act on the Regulation of Activities of Personal and Property Protection and Private Investigation adopted by the Parliament at its session of 2 May 2005 are not unconstitutional in the context of the petition.

The Constitutional Court publishes this Decision in the Hungarian Official Gazette.

Reasoning

1. At its session of 2 May 2005, the Parliament adopted an Act on the Regulation of Activities of Personal and Property Protection and Private Investigation [hereinafter: the Act].

On 5 May 2005, the Speaker of the Parliament sent the Act to the President of the Republic for promulgation, without a request of urgency. The President of the Republic, exercising his right granted under Article 26 para. (4) of the Constitution, submitted a petition on 20 May

2005, within the required deadline, initiating a prior constitutional review of the Act of Parliament adopted by the Parliament but not yet promulgated.

The President of the Republic supports his petition with the following arguments:

1.1. In his opinion, the provisions in Sections 28 and 29 of the Act concerning the electronic visual surveillance system do not contain an adequate guarantee for the protection of fundamental rights, this resulting in the violation of several fundamental rights granted in the Constitution. Putting the Act in force would violate the right to human dignity [Article 54 para. (1) of the Constitution], the right to the protection of privacy, and the right to informational self-determination [Article 59 para. (1) of the Constitution].

According to Section 26 para. (1) item e) of the Act, personal and property guards performing tasks of property protection may use a technical security system for property protection in when guarding the principal's facilities not qualifying as public ground. According to the interpretative provision in Section 74 item 6, such a system can be either an electronic surveillance system (area surveillance) without recording, i.e. operated for direct monitoring purposes, or one with sound or image recording. As a guarantee provision, the Act prohibits the abuse of the affected persons' personal data [Section 29 para. (1)] on the one hand, and, on the other hand, it requires an informative sign or notice on the operation of an electronic surveillance system (area surveillance) to be posted and the affected persons' consent to be given either expressly or by way of implicit conduct [Section 28 para. (2) item c) and Section 30 para. (3)].

It is pointed out by the President of the Republic that although the provisions referred to in his petition are important elements of guaranteeing the provision and the protection of the right to informational self-determination, they are – in his opinion – insufficient. The affected person is not always in a position to freely decide on entering a given facility, therefore such a person cannot freely decide on giving consent to being recorded. What is more, Section 30 para. (3) of the Act only requires consent for making a recording with a surveillance system, but not for real-time surveillance without recording. According to the President of the Republic, there are cases – the most serious ones with regard to the protection of fundamental rights – when human dignity and privacy (in certain instances, the protection of personal data) can be violated by both the presence and the activity of the person surveying the site and the

existence of technical surveillance (recording by camera). The situation is the same when surveillance is only performed by a property guard and no information is forwarded to unauthorised persons, as in such cases anybody whose presence or surveying activity is against the affected person's will is to be regarded as unauthorised. This means that there are no adequate provisions guaranteeing the protection of general personality rights and the right to informational self-determination, for example, by expressly restricting or prohibiting real-time electronic surveillance or requiring compliance with substantial criteria. When reviewing the provisions of the Act, the President of the Republic found no such guarantees.

1.2. Section 30 para. (3) of the Act is deemed unconstitutional by the President of the Republic, who claims that the provisions on consent required for electronic surveillance violate human dignity and the protection of privacy [Article 54 para. (1) and Article 59 para. (1) of the Constitution].

According to the second sentence of the challenged provision, the consent to surveillance – given by way of implicit conduct – may not violate human dignity. It is pointed out by the President of the Republic in this regard that it is not the affected person's "consent" that may violate, in a given situation, his or her own human dignity, but the situation of surveillance performed by recording, resulting from the implicit consent of the person surveyed. From the above, the President of the Republic draws the conclusion that in the case of certain well-defined sensitive circumstances, the Act should prohibit electronic surveillance or the personal presence of the property guard expressly and in a detailed manner.

1.3. The President of the Republic also challenges the constitutionality of the provision on the storage period of electronic recordings made with the aid of a surveillance system, as contained in Section 31 para. (2) of the Act. In his opinion, the period of 30 days defined without differentiation and justification is disproportionately long and consequently violates the general personality right and the right to informational self-determination [Article 54 para. (1) and Article 59 para. (1) of the Constitution].

Sections 30-31 of the Act contain the detailed rules on electronic surveillance systems recording sounds, images, and ones recording both sounds and images. According to Section 31 para. (2) of the Act, sound, image, or sound and image recordings made in such an area of a private property that is open to the public shall, if not used, be destroyed or deleted within

thirty days, or, in the case of certain service providers engaged in monetary and banking activities listed exhaustively and in detail, within sixty days.

It is pointed out by the President of the Republic that while surveillance without recording might restrict personality rights and the right to informational self-determination in given cases, the possibility of electronic recording constitutes a restriction in itself, because the making and storage of recordings qualify as data handling. The storage of recordings – as pointed out in the petition – increases the danger of them being manipulated and the danger of the recording itself or the personal information contained therein being disclosed to unauthorised persons. It is also claimed by the President of the Republic that the unjustified storage of recordings is contrary to the constitutional principle of data handling adhering to a specific objective, as it constitutes storage for the purpose of stocking. According to the petitioner, when adopting the challenged provision, the legislature failed to justify the setting of thirty days as the maximum storage period for all types of activities that may be concerned. For this reason, one cannot establish whether the restriction of fundamental rights as a consequence of recording is really made necessary by the aim of property protection used as justification for such restriction, and whether it is proportionate to that aim.

1.4. Furthermore, Section 31 para. (4) of the Act is also deemed unconstitutional by the President of the Republic as the challenged rule provides for an unreasonably short period – of three working days – for the entitled person to exercise his or her right to self-determination. According to the petition, this violates the right to informational self-determination [Article 59 para. (1) of the Constitution], and in some cases it may prejudice the right to defence [Article 57 para. (3) of the Constitution].

With regard to the justification of constitutional review, it is emphasised by the President of the Republic that the principle of self-determination or personal participation is an essential element of the right to informational self-determination, i.e. the subject of personal data shall be allowed to dispose – within the limits of the Act – over the data handled in relation to him or her even if such data are lawfully handled by another person. The challenged provision of the Act tries to comply with the above requirement by providing that the person affected by surveillance and recording may ask for storing his or her data beyond the deadline specified.

The petition refers to the fact that in the original text of the submitted Bill both the general storage period [Section 31 para. (2)] and the period open for the entitled person [Section 31 para. (4)] were three working days as a uniform rule. While during the parliamentary debate of the Bill the storage period was raised to 30 days, the deadline for requesting the postponement of data deletion was left unchanged. In the opinion of the President of the Republic, the possibility of exercising the right to self-determination must be available as long as the data (in the present case, the recording made by the surveillance system) regarding the entitled person are handled (stored); provisions to the contrary are unconstitutional in respect of the fundamental rights concerned.

2. The provisions of the Constitution referred to in the petition are the following:

"Article 54 para. (1) In the Republic of Hungary everyone has the inherent right to life and to human dignity. No one shall be arbitrarily denied of these rights."

"Article 57 para. (3) Individuals subject to criminal proceedings are entitled to legal defense at all stages of the proceedings. Defense lawyers may not be held accountable for opinions expressed in the course of the defense."

"Article 59 para. (1) In the Republic of Hungary everyone has the right to the good standing of his reputation, the privacy of his home and the protection of secrecy in private affairs and personal data."

3. The provisions of the Act taken into account when judging the petition are the following:

"Section 28 para. (2) In the case of protecting a private property open to the public, the person protecting the property shall post – in a well visible place, in a readable form, in a manner suitable for the purpose of informing third persons who wish to enter the area – a warning sign or notice on the

a) measures specified under Section 26 para. (1), and the possibility thereof;

b) objects prohibited to be taken into the area, and the nature of such objects;

c) fact of using an electronic surveillance system in the given area (area surveillance);

d) aim of surveillance by using an electronic security system, and of making sound and image recordings containing personal data by using such system, the aim of storing such recordings, the legal basis of data handling, the place of storing the recordings, the period of storage, the person using (operating) the system, the scope of persons entitled to have access to the data, and the provisions of Act LXIII of 1992 on the Protection of Personal Data and the Disclosure of Information of Public Interest (hereinafter: the DPA) on the rights of data subjects and the provisions pertaining to the enforcement thereof;
e) proceedings of seeking legal remedy against injuries caused by measures taken by the person engaged in property guarding."

"Section 29 para. (1) When implementing the measures regulated in Sections 26-28, the person engaged in property guarding shall ensure that unauthorised persons have no access to the personal data of the affected person, in particular to his or her private secrets and the circumstances of his or her private life "

"Section 30 para. (3) In such part of a private property that is open to the public, sound, image, or sound and image recordings may only be made with the express consent of the affected natural person. Consent may be given by way of implicit conduct provided that such consent does not harm human dignity."

"Section 31 para. (1) Electronic surveillance systems in the form of recording sound, image, or sound and image may only be applied if the circumstances of performing the assignment make it likely that this is the only way suitable for detecting unlawful acts against persons and property, for surprise in the act, or for preventing or proving such unlawful acts, as well as if the application of such technical devices is absolutely necessary, and if it does not result in the disproportionate restriction of the right to informational self-determination."

"Section 31 para. (2) Sound, image or sound and image recordings made in such part of a private property that is open to the public shall – when not used – be destroyed or deleted within thirty days, or within sixty days in the case of principals engaged in financial services, supplementary financial services, mortgage-credit institution services, investment services, stock exchange services, keeping securities in deposit, managing securities deposited, clearing house services, insurance, insurance agency and insurance consulting services, postal money transfer services, receiving and delivering domestic and international postal orders, with

regard to their areas of private property open to the public, as necessary for performing their tasks."

"Section 31 para. (4) Anyone whose right or lawful interest is affected by the recording of sound, image or sound and image, or the recording of other personal data may – in compliance with the provisions contained in paragraph (2), concurrently proving his or her right or lawful interest – within three working days or sixty days from the recording of the sound, image, or the sound and image, request the data handler not to destroy or delete the data. On the request of a court or other authority, the sound, image, or sound and image recording or any other personal data shall be forwarded to the court or the authority without delay. If no request is made within thirty days from the date of asking for non-destruction or non-deletion, the sound, image, or sound and image recording and any other personal data shall be destroyed or deleted, save if the deadline of sixty days specified in paragraph (2) has not lapsed yet."

"Section 74 item 11 Area of a private property open to the public: an area of private property open to anybody without restriction, including parts of public ground having been taken possession of by the principal giving assignment for personal or property protection on the basis of a legal transaction under civil law, in particular a legal relation of rent or lease, provided that a) the use of the area part is closely related to the activity pursued on the public part of the private property guarded by the party engaged in personal and property protection, in the form of supporting it or its continuity, or b) it is used for the purpose of placing the chattels of the principal or of the public using the open part of the private property;"

II

For the examination of the unconstitutionality of the provisions challenged by the President of the Republic in his petition, the Constitutional Court reviewed its relevant practice related to human dignity, the right to informational self-determination and the activity of property guards.

1. As stated by the Constitutional Court in its Decision 8/1990 (IV. 23.) AB, the right to human dignity is considered to be one of the designations of the so-called general personality right, which includes – among others – the right to the free development of one's personality,

the right to self-identification, the freedom of self-determination, as well as the general freedom of action. The general personality right is a subsidiary fundamental right for the protection of the individual's autonomy (ABH 1990, 42, 44-45).

However, in the practice of the Constitutional Court, the right to human dignity is considered to be absolute and unrestrictable only as a determinant of human status and in its unity with the right to life. [Decision 64/1991 (XII. 17.) AB, ABH 1991, 297, 308, 312] Therefore unrestrictability "only applies to cases where life and human dignity inseparable therefrom would be restricted by others." [Decision 22/2003 (IV. 28.) AB, ABH 2003, 235, 262] Its component rights, such as the right to self-determination, may be restricted in accordance with Article 8 para. (2) of the Constitution just like any other fundamental right. [Decision 75/1995 (XII. 21.) AB, ABH 1995, 376, 383]

The Constitutional Court pointed out concerning the State's interference with privacy: "Article 54 para. (1) and Article 59 para. (1) of the Constitution protect the privacy of people as well as their private secrets, good standing of reputation, and personal data. According to the standing practice of the Constitutional Court, it is the violation of the above rights originating from the fundamental right to human dignity when the State interferes without due reasons with relations that fall into the scope of privacy, for example, through the authorities using coercive measures against individuals without due grounds. 'Therefore, any legal regulation which allows this to happen is unconstitutional without regard to the percentage of cases in which such unconstitutional legal consequence actually occurs.' [First: Decision 46/1991 (IX. 10.) AB, ABH 1991, 211, 215] 'Given constitutional rights and liberties, the sovereign power may only interfere with one's rights and freedoms on the basis of constitutional authorisation and constitutional reasons.' [First: Decision 11/1992 (III. 5.) AB, ABH 1992, 77, 85] The limitations of State interference are set by the formal and content requirements defined under Article 8 para. (2) of the Constitution, and eventually by the requirements of necessity and proportionality elaborated by the Constitutional Court on the basis of the Constitution." [Decision 50/2003 (XI. 5.) AB, ABH 2003, 566, 578]

2. In its Decision 15/1991 (IV. 13.) AB, the Constitutional Court interpreted the right to the protection of personal data, having regard to its active aspect as well, as a right to informational self-determination rather than as a traditional protective right. Thus, the right to the protection of personal data, as guaranteed by Article 59 of the Constitution, means that

everyone has the right to decide about the disclosure and use of his or her personal data. Hence, approval by the person concerned is generally required for the registration and use of personal data; the entire route of data processing must be monitorable and checkable by the person concerned, i.e. everyone has the right to know who, when, where and for what purpose uses his personal data. In exceptional cases, an Act of Parliament may require the compulsory supply of personal data and prescribe the manner in which these data may be used. Such an Act restricts the fundamental right to informational self-determination, and such restriction is only constitutional when in accordance with the requirements specified in Article 8 of the Constitution.

Adherence to the purpose to be achieved is a condition of and at the same time the most important guarantee for exercising the right to informational self-determination. The enforcement of this principle means that personal data may only be processed for a clearly defined and lawful purpose. Each phase of data processing must comply with the notified and authentically recorded purpose. The purpose of data processing must be communicated to the data subject in a manner making it possible for him to assess the effect of data processing on his rights, to decide with due basis on the disclosure of data, and to exercise his rights in the case of the use of data for a purpose other than the specified one. Consequently, the data subject must be notified of changing the purpose of data processing. Data processing for a new purpose without the consent of the data subject is only lawful if it is expressly provided for in an Act of Parliament with respect to the specific data and data processor. It follows from the principle of adherence to the purpose that collecting and storing data without a specific goal, "for the purpose of storage"[1], i.e. for unspecified future use are unconstitutional. (ABH 1991, 40, 41-43)

3. The Constitutional Court has already examined the legal regulation of electronic visual surveillance, as a case falling into the category of the right to informational self-determination (in connection with such activities performed at sports events). According to Decision 35/2002 (VII. 19.) AB (hereinafter: CCD1), recordings made on any medium during visual surveillance qualify as personal data. It established that "the provision under review cannot be justified on constitutional grounds, since it also allows the forwarding of the recording of persons other than the ones prohibited from visiting certain sports events, and since the

[1] Translator's remark: instead of "for the purpose of storage", a more accurate translation would be "for the purpose of stocking", i.e. "for the purpose of accumulating stocks of data", however, in texts quoted from earlier Decisions of the Constitutional Court, the original translation was left unchanged for the sake of consistency.

forwarding of such recordings, qualifying as personal data, to organisers of sports events of the same type or similar types is also allowed, without the guarantees of data protection. Thus, the challenged regulation is aimed at the prevention of a remote and abstract danger, and it is for this purpose that it requires, without due constitutional guarantees, the handling of data 'to be stored'[2]." (ABH 2002, 199, 208) Thus, in the opinion of the Constitutional Court, the constitutional requirement of adherence to the purpose demands the existence of an actual and direct threat rather than a potential one.

However, in CCD1, the Constitutional Court did not establish the unconstitutionality – i.e. the violation of Article 59 para. (1) of the Constitution – of further provisions concerning recordings made at sports events. It was acknowledged that such recordings may be handled for the purpose of facilitating criminal or administrative infraction proceedings. The storage period for such recordings made by camera was not objected to either, as within the period of 30 days, the investigation authorities shall decide whether the acts committed necessitate the institution of criminal or administrative infraction proceedings. In view of the above, the Constitutional Court considered the 30-day period of data handling allowed for organisers of sports events to be an acceptable term with respect to the realisation of the constitutional guarantees of data protection. This is so because, according to the regulation, the handling of data by the organiser of the sports event is related to a constitutionally protected objective, i.e. the protection of public order and public safety; the affected person is informed of the handling of his data, the forwarding of the recorded data to the investigation authorities is statutorily allowed, and in that respect the route of his data can be traced by the affected person. (ABH 2002, 199, 209-210)

4. The Constitutional Court made several statements – relevant in the present case as well – during the examination of the unconstitutionality of certain provisions of Act IV of 1998 on the Regulation of Activities of Personal and Property Protection and Private Investigation Performed on an Entrepreneurial Basis, and on the Professional Chamber of Personal and Property Protection and Private Investigation (hereinafter: PPP).

[2] Translator's remark: instead of "the handling of data to be stored", a more accurate translation would be "the handling of data for the purpose of stocking", i.e. "for the purpose of accumulating stocks of data", however, in texts quoted from earlier Decisions of the Constitutional Court, the original translation was left unchanged for the sake of consistency.

The safeguarding of property on an entrepreneurial basis is a form of realising property protection in the technical sense; it is reasonable that the law should provide for a possibility to safeguard property, determining at the same time the scope of the rights and obligations of the principal (owner) and the agent (property guard). As pointed out in Decision 3/2001 (I. 31.) AB, by adopting an Act on the criteria of property protection on an entrepreneurial basis, the purpose of enhancing the constitutional protection of property is also met by the State. (ABH 2001, 68, 73)

However, the implementation of the technical protection of property and the elaboration of the related set of instruments have constitutional limitations – in view of the protection of other fundamental rights. In the procedure of the Constitutional Court, the above requirement has made it necessary to examine whether the legislature complied with the requirement contained in Article 8 para. (2) of the Constitution on the unrestrictability of the essential content of fundamental rights.

In Decision 22/2004 (VI. 19.) AB (hereinafter: CCD2), the Constitutional Court annulled the provision of the PPP on the checking of bags, and it established an unconstitutional omission of legislative duty on account of the lack of rules on confidentiality and data handling. (ABH 2004, 367)

The reason for the unconstitutionality was that the undifferentiated rules enacted by the legislature provided for a too general and as a result too broad authorisation for restricting to the same extent the right to the protection of privacy in various situations, and that the regulation was also incompatible with the requirement of applying the least severe tool. (ABH 2004, 367, 375)

In CCD2 the Constitutional Court established in principle: "[…] while ensuring the protection of property in a technical sense, within the scope of the constitutional protection of property rights, the State must at the same time guarantee that no other fundamental right is injured disproportionately as a result." (ABH 2004, 367, 374)

III

The Constitutional Court examined the provisions of the Act related to the electronic visual surveillance system [Section 28 para. (2) and Section 29 para. (1)] and Section 30 para. (3) with consideration to the protection of privacy, on the basis of the right to human dignity.

1. In the Act, the application of the electronic security system is presented as a tool for the protection of property in the technical sense, serving the purpose of surveillance, recording, as well as storing and – in some cases – forwarding recordings. This way, the regulation under review empowers certain subjects of private law (property guards as agents) to monitor persons entering or staying within the area controlled by them, to make recordings of such persons, and – on the basis of Section 31 para. (3) or para. (4) of the Act – to forward such recordings on the request of State authorities (courts or other authorities) for use as evidence. With regard to the character of the facilities monitored by camera (private property, or area of private property open to the public), it is necessary to emphasise that no restriction is made by the Act, i.e. surveillance may be performed anywhere.

The use of electronic surveillance systems is becoming increasingly widespread world-wide. In Hungarian law, there are several Acts of Parliament allowing such surveillance (e.g. Act on the Police, Act on Public Ground Patrols, Act on Sports). Common features in the contents of these regulations are the definition of the aim, scope and conditions of surveillance in accordance with the activity of the organisation concerned, and the limitation of the safeguarding (storage) period of the recording. Other Acts of Parliament (e.g. regulations on proceedings by the authorities, on labour control) empower persons acting on behalf of the authority to make image and sound recordings in the course of control.

The primary function of most camera surveillance systems is to make people obey the norms, but in the case of a breach of law, the application of technical devices serves the purpose of supporting the procedure of calling the perpetrator to account and facilitating the application of sanctions.

2. Although the application of a camera as a technical tool of protecting property is suitable for safeguarding objects of property, it inevitably involves the possibility of targeting persons, human behaviour, habits and actions, or the human body itself. Therefore, surveillance performed electronically can penetrate into the privacy of persons, recording

intimate (sensitive) situations of life, even in such a way that the affected person is not aware of being recorded, or is not in a situation to decide whether or not to consent to such recording, bearing in mind the consequences thereof. In addition to the violation of the right to privacy, recording performed in the above manner may affect – in a broader and deeper sense – the right to human dignity in general. It is the essential conceptual element of privacy that others should not have access to or insight into such private sphere against the affected person's will. When an unwilled insight nevertheless happens, the violation may affect not only the right to privacy itself, but also other rights in the realm of human dignity, such as the freedom of self-determination or the right to physical-personal integrity.

As privacy is not limited to one's private home and the area belonging to it, the legal regulations must take note of the fact that areas sensitive with regard to the protection of privacy may also be affected by the use of technical security systems enabling visual insight. However, the provisions of the Act under review do not make such a distinction; the regulation is uniform: an electronic surveillance system may be operated in any case where there are no other means suitable for detecting unlawful acts against persons or property.

Indeed, the most general rules in the Act concerning electronic surveillance systems are found in that part of the Act where the legislature intended to eliminate or, at least, minimise the violations of fundamental rights resulting from surveillance [Section 30 para. (1), Section 31 para. (1) of the Act]. According to the opinion of the Constitutional Court detailed in Decision 36/2000 (X. 27.) AB, the criteria of constitutionality for an Act allowing the restriction of any fundamental right are not met if the statutory regulation merely repeats the abstract standard of constitutionality. The restriction of fundamental rights must be based on a firm statutory provision in terms of the relation between the desired objective and the measures applied. (ABH 2000, 241, 273-274)

Section 31 para. (1) of the Act sets the limits of surveillance – without consideration to the above criterion of constitutionality – by merely prescribing that technical tools may not be used beyond the necessary extent and by prohibiting in general the disproportionate restriction of the right to informational self-determination. According to Section 30 para. (3) of the Act – challenged in the petition –, the affected person's consent is only required for recording (and not for remote surveillance without recording), and that requirement is considered to be met even if consent is given by way of implicit conduct.

3. The Constitutional Court has established that the essential content of the right to human dignity granted under Article 54 para. (1) of the Constitution is affected if the regulation allowing the application of electronic surveillance systems fails to address the respect and protection of privacy. In CCD2, the Constitutional Court pointed out that although the rights of the property guard practically stem from the contract of agency belonging to the realm of civil law, they extend beyond the scope of the contractual relationship, since the protection of property on an entrepreneurial basis affects the right to the protection of privacy guaranteed by the Constitution. (ABH 2004, 367, 370)

3.1. Section 30 para. (3) of the Act tries to eliminate the violation of fundamental rights in the course of recording sound and images by providing that the implicit consent given to recording may not violate human dignity. Presumably, the legislature intended to ensure that no recording is made if it would harm the human dignity of the person under surveillance. However, neither the actual provision nor the presumed intention of the legislature covers two further types of cases, namely: direct (unrecorded) surveillance and recorded surveillance with explicit consent. As there are problems of interpretation concerning the regulation and in some parts the regulation is incomplete, certain especially sensitive fields of privacy (intimate situations: e.g. being in fitting rooms, restrooms, changing-rooms, toilets) cannot be completely excluded from the scope of surveillance.

The other provisions of the Act do not contain adequate guarantees for the protection of fundamental rights in relation to recordings, either. Section 31 para. (1) not challenged in the petition – as mentioned above – sets too broad and too inclusive limits for the application of sound and image recording. As in the Hungarian law in force there is no specific Act of Parliament on the application of electronic surveillance systems and the criteria thereof, no background guarantee provisions – containing prohibitions or restrictions – could be taken into account in the course of the constitutional examination.

The Constitutional Court stressed in several of its decisions that the restriction of a fundamental right may only be regarded as constitutional if it is indispensable, i.e. if it is the only way to secure the protection of another fundamental right, liberty or constitutional value. [see for example Decision 30/1992 (V. 26.) AB, ABH 1992, 167, 171; Decision 6/1998 (III. 11.) AB, ABH 1998, 91, 98-99; Decision 44/2004 (XI. 23.) AB, ABH 2004, 618, 648]

The Constitutional Court has established in connection with Section 30 para. (3) of the Act the lack of a forcing necessity that would make the extension of surveillance to the sphere of intimacy constitutionally acceptable. Such restriction of a fundamental right that affects human dignity is not justified – in the scope of performing tasks of property protection – merely by the protection or enforcement of another fundamental right, namely the right to property. The statutory condition according to which the affected person's consent to the restriction of his or her fundamental right by way of implicit conduct provides sufficient justification for him or her being surveyed even in an intimate situation violates the fundamental constitutional right to human dignity. In fact, it may vary from case to case what is and what is not considered as implicit conduct, and this opens the way for an arbitrary interpretation of the law, as it is up to the property guard to decide whether a statutory condition is fulfilled or not. It is the task of the legislature to define implicit conduct and to determine when (in what cases an in what fields) it may be regarded as lawful justification for surveillance.

Furthermore, the Constitutional Court notes that there are several other instruments available for the prevention of unlawful and criminal acts affecting one's property that do not harm human dignity and offer an effective technical means for protecting property.

Consequently, the Constitutional Court has established that Section 30 para. (3) of the Act does not ensure the protection of privacy, therefore it is in conflict with Article 54 para. (1) of the Constitution.

3.2. The regulation in Section 28 para. (2) of the Act concerning electronic visual surveillance systems does not contain provisions on the conditions of using the technical instrument concerned, instead, it specifies the content of warning (information) to be provided on surveillance to the public under surveillance. This includes the communication of the fact of surveillance, together with the aim thereof, the legal basis of data handling, the place and the period of storing recordings made in the course of surveillance, the person operating the surveillance system and some further provisions of data protection. None of the above has been challenged in the petition as unconstitutional.

Section 29 para. (1) of the Act provides for the protection of private secrets learnt by the property guard and for the safeguarding of things seized, but is contains no specific and direct rules related to the electronic surveillance system.

It is not the regulatory content of the provisions concerned but the lack of guarantees ensuring the operation of surveillance systems in a constitutional manner that is objected to in the petition. When specifying the reasons for the unconstitutionality of Section 30 para. (3) of the Act, the Constitutional Court referred, in connection with the right to human dignity, to the guarantees which are indispensable for the enforcement of this fundamental right, but the lack of such guarantees does not result in the unconstitutionality of the provisions of a technical nature reviewed here. The provisions related to informing persons affected by electronic visual surveillance serve the very purpose of complying with certain constitutional requirements.

In view of the above, the Constitutional Court has established that in the context of the petition, the provisions related to electronic visual surveillance systems in Section 28 para. (2) and Section 29 para. (1) of the Act violate neither Article 54 para. (1) nor Article 59 para. (1) of the Constitution.

IV

The Constitutional Court has examined certain provisions of Section 31 paras (2) and (4) of the Act basically in relation to the right to informational self-determination. However, in accordance with the petition, it has taken account of the right to human dignity and the right to defence as well.

1. As established in CCD1, recordings made on any medium as a result of visual surveillance qualify as personal data. (ABH 2002, 199, 208) According to the interpretative provision, in force since 1 January 2004, of Act LXIII of 1992 on the Protection of Personal Data and the Disclosure of Information of Public Interest (hereinafter: the DPA), taking photographs and recording sounds or images qualify as data handling. Section 30 para. (1) of the Act explicitly provides that the person performing surveillance is to be regarded as a data handler, who may only act in compliance with the requirement of enforcing data protection rights. It is also noted by the Constitutional Court that one can draw conclusions from the

events, acts as well as related venues and dates shown by the recordings that affect the general personality right deduced from human dignity.

One of the provisions challenged by the petitioner, namely Section 31 para. (2), specifies that the image, sound, or image and sound recordings are to be deleted or otherwise destroyed within thirty days of being made. The Act provides for three exceptions to the rule on the general safeguarding (storage) period. The first exception is that the storage period may be sixty days if the principal is engaged in certain financial-postal activities [Section 31 para. (2)]. The second exception is the case when the recordings are used, i.e. when the court or other authority uses the recordings as evidence in its proceedings [Section 31 para. (3)]. Finally, the third case is when the person affected by the recording (the one who exercises his or her right to self-determination) requests the extension of the storage period (thirty or sixty days) [Section 31 para. (4)]. With regard to the latter provision, the petitioner objects to the fact that while in cases subject to the sixty days' rule the entitled person may exercise his or her right to self-determination throughout the whole period, in cases subject to the general rule (thirty days) there are only three working days open for such action.

2.1. Adherence to a specific purpose is one of the most important elements of protecting personal data. Among others, it follows from the above principle that collecting and storing data without a specific goal, "for the purpose of storage"[3], i.e. for unspecified future use are unconstitutional. [see Decision 15/1991 (IV. 13.) AB, ABH 1991, 40, 42] Accordingly, in the present procedure, the Constitutional Court first examined whether the general data storage period (thirty days) specified in the Act is in conflict with Article 59 para. (1) of the Constitution.

In addition to its preventive function, the application of the electronic surveillance system regulated in the Act is justified by the need to facilitate the procedure of calling perpetrators to account for unlawful acts affecting property. Indeed, this second function is the one that forms the basis for allowing the safeguarding (storage) of camera-made recordings for a specific period. Area surveillance systems are suitable for recording not only the commission of an unlawful act but the elements of the preparatory phase as well, and such recordings can

[3] Translator's remark: instead of "for the purpose of storage", a more accurate translation would be "for the purpose of stocking", i.e. "for the purpose of accumulating stocks of data", however, in texts quoted from earlier Decisions of the Constitutional Court, the original translation was left unchanged for the sake of consistency.

be used by the authorities later on, following the commission of the criminal offence (or administrative infraction).

When regulating the general storage period, the Act makes no difference by either the specific activities performed by property guards or the nature of the facility guarded, nor does it take into account the value of the protected property or the level of its endangerment. It is stressed by the Constitutional Court that not only the principal's activity but also the actual situation of property protection can be relevant to determining the safeguarding period. It is therefore an important factor, for example, whether the electronic surveillance system focuses on goods directly accessible by customers or on the place where the delivery (transfer) of cash is done in the department store. In the latter case, the need to protect fundamental rights (arising due to the endangerment of human life, physical integrity, or personal freedom) extends beyond the general protection of property, justifying the stronger restriction of the right to informational self-determination, which is realised by setting a longer storage period for recordings. The same applies to cases where – beyond the technical protection of property – the data handling performed is related to a constitutionally protected objective, i.e. the protection of public order and safety [see CCDl, ABH 2002, 199, 209].

However, in all situations where area surveillance is merely related to the protection of objects of property endangered to an average extent, the storage of recordings for thirty days results in the disproportionate restriction of the right to the protection of personal data. If the operation of the surveillance system is effective and compliant with statutory provisions, it can certainly be found out in much less than thirty days whether the recording is to be used, i.e. whether any proceedings are to be instituted by the authorities. In such cases, the mere interest in the efficiency of the proceedings does not justify a longer storage period for recordings possibly showing preparations for an unlawful act affecting the property concerned. All the above support the argument that the protection of property can also be ensured by less severe tools that restrict the right to the protection of personal data to a lesser extent.

Consequently, the Constitutional Court has established that the provision on the storage period of recordings containing sound, images, or sound and images in Section 31 para. (2) of the Act violates Article 59 para. (1) of the Constitution.

2.2. In addition to examining the violation of the right to informational self-determination, the Constitutional Court has also considered whether the longer storage period of recordings is contrary to the enforcement of the right to human dignity.

With regard to the provisions of the PPP the Constitutional Court established that their undifferentiated nature had resulted in the disproportionate restriction of the right to the protection of privacy. It was pointed out in particular in CCD2 that the violation had basically been caused by the legislature allowing the restriction of the fundamental right to the same extent in various situations, which was at the same time incompatible with the requirement of applying the least severe tool. (ABH 2004, 367, 375)

In giving a reasoning for the unconstitutionality of Section 30 para. (3) of the Act, the Constitutional Court stressed the primary importance of the protection of privacy in connection with the right to human dignity.

The statutory limitation of the – adequately differentiated – storage period of recordings serves not only the purpose of eliminating arbitrary storage (accumulation of stocks), but also that of minimising abuses related to electronic recordings, i.e. protecting the autonomy of individuals. The greatest possibility of abusing recordings is opened when the data handler allows unauthorised persons to have access to them. There can be several reasons for obtaining the recording in this manner, for example the aim of manipulating the original recording or a copy thereof or one's intention to gain personal information contained on the recording and to use such information for private purposes or to use it unlawfully in proceedings at an authority for purposes other than the protection of property. The recording itself or the data that can be retrieved from it might contain sensitive content with regard to one or more persons surveyed for completely different reasons. Human dignity can be violated not only by the electronic recording of intimate life situations, but also by the recording – and even more by the storage – of everyday situations that do not at all seem to be of a sensitive nature. The latter makes possible – throughout the whole period of storage – the abusive handling of recordings obtained by the property guard incidentally, i.e. not in direct relation with the protection of property, and that of the data retrieved therefrom.

The Constitutional Court emphasises that there are strict constitutional limits to operating electronic surveillance systems in the scope of property guarding activities organised on

entrepreneurial grounds. When setting such limits, the point is to create a balance in the enforcement of competing fundamental rights rather than to allow a shift towards extremities. Imposing a complete ban on the protection of property in a technical sense would be legally impossible, violating the constitutional right to property as well. The other – constitutionally unjustifiable – extremity would be the empowerment of owners or property guards acting on their behalf to use any tool whatsoever for the protection of property items. Undoubtedly, the use of any tool suitable for killing a human being (e.g. electric current in a fence) is constitutionally unacceptable as a means of technical protection. It is logical that the legal regulations must define the set of tools suitable for protecting property together with the conditions of their application, and as an indispensable part of such definition, due account must be paid to the level of restrictability of other fundamental rights.

The Constitutional Court points out that the level of the constitutionally acceptable restriction of fundamental rights is not the same in respect of the various elements of the electronic surveillance system. In the phase of surveillance (making a recording) the level of restriction is lower: it is the untouchable nature of the sphere of intimacy that plays a paramount role in setting the constitutional limits of the activity; beyond that, the presence of persons at the place under surveillance and their usual conduct in line with the nature of the place are not subject to any restriction of surveillance. Acknowledging and allowing it is justified as the items of property and the persons present in the area (in the facility) cannot be separated due to the technical character of surveillance. In the phase of storing the recording (handling personal data) the level of restriction is higher because recordings showing persons who are necessarily surveyed in the course of surveillance but who commit no unlawful acts at all might even contain sensitive content until being finally deleted. The documentary character of the recording makes it especially suitable for abuse resulting in the violation of the right to privacy. Consequently, any regulation allowing the storage of electronic recordings for a period longer than justified by the specific situation of property protection is in conflict with the protection of the individual's autonomy, and thus with the enforcement of the right to human dignity.

In view of the above, the Constitutional Court has established that the provision on the storage period of recordings containing sound, images, or sound and images in Section 31 para. (2) of the Act also violates Article 54 para. (1) of the Constitution.

3. The essence of the regulatory provision in the first sentence of Section 31 para. (4) of the Act is that the person affected by surveillance may request the data handler not to destroy the recording. The constitutional concerns raised by the President of the Republic are based on the fact that as a general rule, an unreasonably short deadline has been set by the legislature for such requests, furthermore, there appears to be a conflict between the two provisions [paras (2) and (4)].

3.1. First, the Constitutional Court examined whether the right to informational self-determination is violated by the rule providing for a short deadline for requesting the postponement of the deletion of data, and in particular by the fact that the entitled person may only make such a request during a certain part of the storage period.

According to the decisions of the Constitutional Court explaining the content of the right to informational self determination, and on the basis of the DPA, it is clear that the principle of self-determination or personal participation is an important element of the fundamental right concerned. [Decision 20/1990 (X. 4.) AB, ABH 1990, 69, 70; Decision 15/1991 (IV. 13.) AB, ABH 1991, 40, 42; Decision 29/1994 (V. 20.) AB, ABH 1994, 148, 159, Decision 46/1995 (VI. 30.) AB, ABH 1995, 219, 221] This means that persons subject to electronic surveillance have the right to dispose – under the relevant statutory conditions – over the recordings made and stored, even if such recordings – showing such persons – are handled by another person, such as a property guard in the present case. Naturally, this right of disposal may be exercised by the entitled person until the end of data handling.

It is within the right of disposal of the person affected by data handling to ask – concurrently proving his or her lawful interest – for the postponement of the destruction (deletion) of stored recordings of him or her. Although the statutory provision under review acknowledges this right, it sets an unjustified time limit: it only allows the enforcement thereof within a certain part of the storage period (within 3 working days from the recording of the personal data). A restriction of such an extent may result in the complete loss of the practical enforceability of the right of disposal. The Constitutional Court has established that such a limitation would result in the restriction of the essential content of the right to informational self-determination, therefore the text "[within] three working days" in Section 31 para. (4) of the Act is in conflict with Article 59 para. (1) of the Constitution.

With regard to the above, the Constitutional Court notes that the unconstitutional text and Section 31 para. (2) of the Act are indeed contradictory, as referred to in the petition. The contradiction was presumably caused by the inconsistent amendment of the text of the Bill in the course of the parliamentary debate. As far as the deadlines are concerned, the provision on deferring the deletion of recordings makes an explicit reference to the rule defining storage periods, i.e. specifically to the provision defining thirty and sixty days and making a distinction on that basis. Consequently, the unconstitutional provision violating a fundamental right might even cause an actual problem of interpretation resulting in legal uncertainty, but for lack of an express request therefor in the petition, the Constitutional Court has not examined that issue.

3.2. In his petition, the President of the Republic explicitly requests the Constitutional Court to establish that the provision under review violates not only the right to informational self-determination but also the right to defence.

According to the consistent practice of the Constitutional Court, the right to defence provided for by Article 57 para. (3) of the Constitution is embodied in the rights of the defendant and the defence counsel. The defendant is entitled to defend himself and to use the services of a defence counsel freely chosen by him. The constitutional interpretation of the right to defence may only be based on the joint consideration of the rights of the defendant and the defence counsel. [Decision 6/1998 (III. 11.) AB, ABH 1998, 91, 93; Decision 14/2004 (V. 7.) AB, ABH 2004, 241, 256; Decision 17/2005 (IV. 28.) AB, ABK April 2005, 218, 223]

In Decision 6/1998 (III. 11.) AB, the Constitutional Court examined the requirements of the right to defence ensuring effective and appropriate preparation, and – in that context – the requirements of fair trial manifesting itself in the principle of equal arms. As pointed out in that decision, it is a precondition for the equality of arms that the prosecution, the defendant and the defence counsel have access to the relevant data of the case in the same completeness and depth. The Constitutional Court concluded that "The right to defence and the principle of equal arms are applicable to the possession and free use of all documents available […] to the prosecution as well." (ABH 1998, 91, 100)

As referred to by the Constitutional Court several times in the present Decision, it is one of the functions of electronic surveillance systems to support the procedure of calling

perpetrators to account for their unlawful – mainly criminal – acts affecting property. If, in the opinion of the property guard, based on surveillance, a criminal act has been committed (catching in the act), then – according to Section 27 para. (2) of the Act – the guard shall hand over the perpetrator to the competent investigating authority, or – if not in a position to do so – he or she shall notify such authority of the unlawful act. If criminal proceedings are instituted on the basis of the notification, the data handling property guard shall immediately forward the stored recording to the requesting court or other authority, in compliance with Section 31 para. (4) of the Act. Requests for using data as evidence may be submitted throughout the whole storage period, which is not the case for requests for postponing the deletion of the recording that may be submitted by the person having the right to informational self-determination (person affected by the surveillance and subjected to proceedings). However, if the recording is not used (no request is filed by the authorities) and the entitled person fails to exercise his or her right within the deadline of three working days, he or she may not arrange for the postponement of the deletion of the recording, thus losing the opportunity to use it as a tool of defence in the criminal proceedings.

The following can be concluded from the above: with regard to the use of electronically made and stored recordings as tools of evidence or defence, the prosecution and the defence do not have equal opportunities. Accordingly, the provision causing such imbalance in opportunities violates the principle of equal arms, and therefore it is in conflict with the enforcement of the right to defence. Therefore, the Constitutional Court has established that the text "[within] three working days" in Section 31 para. (4) of the Act is in conflict with Article 57 para. (3) of the Constitution as well.

The Constitutional Court has ordered the publication of this Decision in the Hungarian Official Gazette in view of the establishment of unconstitutionality.

Budapest, 3 October 2005

Dr. András Holló
President of the Constitutional Court

Dr. István Bagi
Judge of the Constitutional Court

Dr. Mihály Bihari
Judge of the Constitutional Court

Dr. Árpád Erdei

Dr. Attila Harmathy

Judge of the Constitutional Court, Rapporteur

Dr. László Kiss
Judge of the Constitutional Court

Judge of the Constitutional Court

Dr. István Kukorelli
Judge of the Constitutional Court

Dr. Éva Tersztyánszky-Vasadi
Judge of the Constitutional Court

Concurring reasoning by Dr. István Kukorelli

I agree with the holdings of the Decision. However, in my opinion, the primary constitutional question is whether electronic surveillance for the purpose of property protection can be brought into accord with the Constitution and with the earlier practice of the Constitutional Court related to the right to privacy.

1. To answer that question, I consider that the arguments detailed in the dissenting opinion attached to Decision 35/2002 (VII. 19.) AB are to be followed. First of all, camera surveillance, which has become part of everyday practice, is in itself a restriction of a fundamental right. Those who perform visual surveillance cannot avoid collecting personal information about persons present on the private or public ground under surveillance. When storing or forwarding the recordings made in the course of surveillance, one's fundamental right is even more severely restricted. This is so because in such cases it is possible to create a database containing personal or even sensitive data collected. "The large amount of these interconnected data, of which the person in question generally has no knowledge, renders the person defenceless and creates unequal communication conditions. A situation in which one party cannot know the information the other party possesses about him is humiliating and prevents free decision-making." [Decision 15/1991 (IV. 13.) AB, ABH 1991, 40, 51]

The existence of security cameras make people feel being watched all the time, which automatically grants to watchers (State authorities or market players) a position of power. We cannot be sure of being watched, but we can be sure that it might happen anytime.

2. In the present case, the legislature defined the improvement of public order and safety, and in particular the protection of persons and property as well as the enhancement of the efficiency of crime prevention as the aim of electronic surveillance and in general as the aim

of the Act. At the same time, the scope of the Act covers activities of personal and property protection performed on an entrepreneurial basis, as well as private investigation activities. Thus, for subjects of private law the Act specifies as an aim a task to be performed – according to Article 40/A para. (2) of the Constitution – by the police: the protection and improvement of public safety. In my opinion, institutions not authorised to do so by the Constitution may not collect personal data on private ground for the purpose of prosecuting and preventing crime. (Even the police may only collect information on private ground in specific cases and to a limited extent, within the framework set by the Constitution). In the case of electronic surveillance performed in a private sphere and particularly in such parts of private areas that are open to the public, the State's interest in making citizens obey the law and the market interest in learning about consumers' habits are mingled and reinforce each other.

3. Activities of personal and property protection performed on an entrepreneurial basis and private investigation activities are part of business life. Therefore, in this field, the rules of private law prevail. State interference respecting fundamental rights and the principle of market economy can only be justified if and to the extent it is accepted in general in a legal relationship under private law.

The Act allows camera-made recordings in the private sphere, defining the protection of property as its legitimate purpose (Section 30). The Constitutional Court should also have examined whether electronic surveillance is really needed for the achievement of the designated purpose or it can be replaced by other instruments restricting rights to a lesser extent. In my view, the legislature chose for the purpose of protecting property a tool which is not the least severe one with regard to the right to privacy protected under Article 54 para. (1) of the Constitution and to the right to informational self-determination granted in Article 59 of the Constitution. There are effective tools for the realisation of the aims of property protection that restrict these aspects of human dignity in a smaller number of cases and to a lesser extent (e.g. electronic protection of goods, labels, product detectors, etc.). In addition, according to Section 31 para. (1) of the Act, the recording of sound and images is allowed even if it is only likely to be the only means suitable for detecting unlawful acts against persons and property, for surprise in the act, or for preventing or proving such unlawful acts.

In my opinion, the statutory regulation allowing the application of security cameras on private ground constitutes an unnecessary restriction of the right to human dignity enshrined in

Article 54 para. (1) of the Constitution, more specifically of the right to the protection of privacy.

4. Section 28 para. (2) of the Act obliges the security guard to inform the affected person of the application of area surveillance in some way [item c)]. Moreover, it provides that the property guard shall inform the affected persons on the aim of surveillance and of making and storing sound and image recordings containing personal data, on the legal basis of data handling, the place of storage of the recording, the period of storage, the person operating the system, the scope of persons entitled to have access to the data, and on the rights of the affected persons and the rules pertaining to the enforcement thereof [item d)]. Section 30 para. (3) of the Act requires the consent of the private person concerned to the making of a sound and image recording. At the same time, such consent can be given by implicit conduct, which means that mere entry into an area under camera-surveillance may be regarded as giving consent.

In my view, this does not mean that the affected persons voluntarily agree to surveillance in all cases. They do not have a real choice, as they are not equal partners in negotiating the conditions that affect their fundamental rights when they are, for example, doing shopping in shopping centres or markets. Due to the imbalanced situation, made worse by the legislature by allowing the use of electronic surveillance systems, those who complain about surveillance are unable to enforce their rights by means of private law. When deciding on the constitutionality of the Act, the defenceless position of the affected persons may not be disregarded – although one has to take into account the fact that the provisions at issue pertain to business life.

To sum up, the operation of an electronic surveillance system on private ground for purposes of property protection violates the freedom of privacy and the right to informational self-determination. As it is the basic concept of the Act to allow electronic surveillance for the purpose of property protection, building certain constitutional guarantees into the Act does not make the entire regulation constitutional. Although security cameras seem to only affect the external manifestation of human personality in society, in fact, they are technically able to harm the innermost sphere of one's personality. However, on the basis of Article 54 para. (1) and Article 59 of the Constitution, an individual may legitimately expect to have his or her intimacy preserved. There is significant risk in failing to examine thoroughly whether security

cameras are really indispensable tools in such a field of our life and in expecting that the operators of surveillance systems will act in a self-restrictive manner.

Budapest, 3 October 2005

Dr. István Kukorelli
Judge of the Constitutional Court

I second the above concurring reasoning:

Dr. László Kiss
Judge of the Constitutional Court