**On the Threshold to Urban Panopticon?
Analysing the Employment of CCTV in European
Cities and Assessing its Social and Political Impacts**

RTD-Project (September 2001 – February 2004)
5th Framework Programme of the European Commission
Contract No.: HPSE-CT2001-00094

**info@urbaneye.net**
**www.urbaneye.net**

## Working Paper No.7

# Video surveillance in Austria

**Steven Ney & Kurt Pichler**

s.ney@iccr-international.org
k.pichler@iccr-international.org

**Interdisciplinary Centre for Comparative Research in the Social Sciences
Schottenfeldgasse 69/1, A-1070 Vienna, Austria**

**April 2002**

Project Co-ordination:

Centre for Technology and Society
Technical University Berlin
www.ztg.tu-berlin.de

# Table of contents

# 1 Introduction

In recent years, the use of video surveillance cameras throughout the world has grown to unprecedented levels. Many towns and cities are moving towards CCTV surveillance of public areas, housing estates, car parks and public facilities. The video surveillance of public space in Austria is at a far lower level than in North America or Great Britain.

A nation-wide application of CCTV does not exist, neither in the public nor in the private sector. Insofar as every user acts separately there is no network of CCTV-systems in Austria. The main purpose of video surveillance in Austria is traffic management / transport policy and the prevention of minor offences. The equipments currently-in-use are mainly cameras for recording and cannot be compared with automatic face recognition systems.[1]

All these circumstances lead to the legitimate question whether video surveillance is regulated by Austrian law and whether personal privacy is endangered.[2] This country report will give an overview of the development and purpose of CCTV systems, the legal framework and the policy debate. Future implications and the relationship between video surveillance and privacy will also be addressed.

---

[1] These contain a specific software programme which is able to automatically identify persons "of interests" to authorities. This already exists, e.g. in Newham, GB.

[2] For more than two decades, governments and companies have used powerful computer technology to collect, process and disseminate a vast spectrum of personal information. Since the late 1980s, when computer and telecommunications began to converge, this process has accelerated (www.privacy-international.org)

# 2 Development of CCTV surveillance in Austria

## 2.1 Technology development

In parallel with the rapid development of electronics and electrical engineering over the last two decades the camera technology has improved tremendously. Cameras may be as small as a matchbox, camouflaged as a wall or alarm clock, integrated in wristwatches, sunglasses or baseball caps. The new technology includes cameras with a superior quality (audio and visual) which provide a high standard of protection against vandalism or sabotage. They are mainly installed on inside or outside walls and can be recognised.

The closed circuit television (CCTV) is a generic term that describes visual surveillance of diverse situations. The clarity of the pictures is usually excellent, with many systems being able to read a cigarette packet at a hundred metres. The systems can often work in darkness, bringing images up to daylight level. The technology will ultimately converge with sophisticated software programs that are capable of automated faces recognition, crowd behaviour analysis and, in certain environments, intimate scanning of the area between skin surface and clothes.

The power and capabilities of cameras are continuously increasing, while the cost and size of technology is decreasing. This process also characterises the Austrian market, where however, video cameras with so-called "face recognition programmes" are still unknown.

## 2.2 Expansion rate

It is not exactly known, when video surveillance was first introduced in Austria. Video cameras are already used to protect banks, hospitals, shopping malls, residential areas, parking garages and government facilities. Lately, some cities and above all, Vienna as the capital city, have installed CCTV in the streets in an effort to control traffic flow, improve highway safety, and prevent crime.

An area-wide inventory control of private users has yet to be made but we can assume that the private sector faces an uncontrolled and rapid growth of video equipments. The reasons for this increase are decreasing costs and the fact that no registration of purchasers is required.

## 2.3 Areas of application

### *Traffic management*

In the public sector, video cameras are mainly used in the field of traffic management and traffic policy. The Traffic Management Controller ("*Verkehrsleitzentrale*"), a federal police department, owns 60 video cameras. They are located at important and highly

frequented traffic junctions and at the A23 ("*Südosttangente*"). The A23 is a motorway connecting the South and the East of Vienna. It has a daily traffic of more than 125.000 vehicles in both directions.[3] On this trunk road accidents and traffic jams occur frequently. A more comprehensive traffic management system involving monitoring and additional by-passes has been in demand for a long time. The Traffic Management Controller started to implement video cameras at the A23 and other relevant junctions. These cameras are pivotable, inclinable, and equipped with zoom-functions. They send black-and-white visual recordings without audio backup to ten monitors. The latter are observed by two civil servants per shift. Violations of road traffic regulations are not persecuted due to the fact that the mentioned cameras are not able to identify faces of drivers nor the licence plate of a car.

Video cameras can also be found at gateways of tunnels. Due to severe accidents[4] in the past, the aim in Austrian road safety policy is to promote "protection by design, prevention by monitoring and control, and response by plan".[5]

The *Wiener Linien* which manage public transport in Vienna and which are governed by private law are in the possession of more than 1000 video cameras. These are installed in underground stations, at departure platforms and in the area of escalators. Their purpose is to co-ordinate the intervals of trains, to provide a fluent traffic and to enable a smooth customs clearance.

To recapitulate, video surveillance serves as an advanced technological aid to avoid or recognise accidents and for providing fluency in traffic and transport.

### *Crime prevention/ Investigation/ Man-hunt*

CCTV is an emerging security tool utilised by private and public entities for monitoring and enhancing security. Austria has a high standard of living and a very low crime rate, especially with regard to violent crime. Crimes involving theft of personal property have increased in recent years. Austrian public authorities use video technology to detect or deter criminal offences or for inquiries and proceedings relating to law enforcement.

Governmental and ministerial buildings are protected by video cameras. The governmental area "Minoritenplatz" in Vienna is completely covered by video cameras. These display both the entrance of the buildings and the surrounding pedestrian area. It is possible to observe every single corner. According to the statements of the civil

---

[3] http://www.kfv.or.at/feedback.htm (homepage of the Austrian Curatorship for Road Safety)

[4] Fire was and still is the biggest threat to safety in tunnels. In addition to video control, also the question of providing two tubes in tunnels was pointed out.

[5] International Conference of TUNNEL MANAGEMENT INTERNATIONAL in Madrid, April 2001 (http://www.itc-conferences.com/_tmi/pdfs/0601p37.pdf)

servants on duty the pictures are not recorded but only serve for the security of the buildings.[6]

The international airport of Vienna is equipped with two different video surveillance systems. The first serves solely as a measure against fire and other cases of emergency. The second is provided with substantial modern equipment for security purposes.[7]

The Border Patrol of the Austrian police has a stock of 44 vehicles equipped with so-called caloric video cameras (*Wärmebildkameras*) which are used to spot illegal immigration along the borderline at night.

CCTV systems operated and managed by the private sector, such as businesses, individuals, commercial and residential associations, are used for protecting residential privacy and property against intrusion and other forms of crime. The cameras can either passively record and play back video or be actively monitored by security personnel. In case of theft or burglary, the recorded pictures are used as evidence in police inquiries.

### *Crowd management*

The Radio Control Centre (*Funkleitzentrale*), a federal police department in Vienna, as well as the Federal Ministry of the Interior have remote-controlled access to the video system of the Traffic Management Controller. These cameras are occasionally also used for the surveillance of state visits, demonstrations and sport events. According to the statement of the Federal Police Directorate, they do not record portraits of people who take part in demonstrations. On account of strong suspicion, police officers are nevertheless entitled to take pictures or record the scene or specific persons on-site.

During sport events in football stadiums the organisers usually cooperage with the police. If they already possess CCTV-systems they would tend to make them available to the local police. This is already the case in Austria's biggest football stadium (Happel-stadium) and there is an ongoing debate about installing CCTV cameras in other stadiums as well.

The Austrian Federal Ministry of the Interior manages two CCTV systems, one at the Stephansplatz (at the city centre), a second at the corner of Kärnterstraße/Opernring (close to the opera). Both systems are intended to allow the easier monitoring of public events. These two systems are also connected to the video surveillance system of the Traffic Management Controller.

---

6 König, Robert (2001): *Videoüberwachung. Fakten, Rechtslage und Ethik*, Wien: Verlag Österreich

7 According to R. König this system might be equipped with biometric face recognition programmes. This would be the first such system in Austria.

### *Other issues: economic and political interests*

"Though they have different reasons for doing so, each of the five countries is rapidly developing its domestic (regional and local) surveillance systems; (... ) Austria because post-modernist architects are creating "intelligent buildings", in which CCTV is an integral part of architecture."[8] According to many commentators, architects and urban planners are already incorporating visual surveillance in the design of new towns and buildings. CCTV as a fixed component could create attractive and seductive consumer spaces, which again would be of great interest for financial investors. Local politicians using these argument also take the factors amenity and public safety into account.

[8] A review of a TV-documentary "Achtung, Kamera" shown in the Austrian broadcast on 23 June 2000, (by Surveillance Camera Players, www.notbored.org/orf.html)

# 3 Legal Framework

In the opinion of most experts, the continuous video surveillance both by public and private entities does not present significant legal obstacles. This following section outlines the recent legal statutes and possible future implementations for the use of CCTV in Austria.

## 3.1 Regulation of video surveillance by public bodies

Three statutory mandates are especially relevant for visual surveillance:

- Code of Criminal Procedure
- Security Police Act
- Article 8 / ECHR

### *Code of Criminal Procedure*

In 1997 the Austrian Parliament adopted new amendments to the Code of Criminal procedure which made specific investigation measures admissible.[9] For the purpose of preventing and investigating organised crime, new methods in the area of audio- and visual surveillance were introduced. These new amendments allow police to use acoustic and optic surveillance with the aim of "hindering or solving serious crimes in cases in which no other investigation methods are likely to be successful." Electronic surveillance can also be used to hinder kidnapping or other forms of deprivation of liberty.

For a suspected crime punishable by more than ten years' imprisonment or for suspected involvement in organised crime, private premises may be monitored without the consent of the resident. Surveillance measures by an informer or an under-cover policeman are also covered by this law. The legal bearings of these operations are covered by articles §§ 149a ff. §149 d-f of the Code of Criminal Procedure (*StPO – Strafprozeßordnung*) or the so-called "major eavesdropping-attack"[10] (*Lausch- und Spähangriff*) and "search by screening"[11] (*Rasterfahndung*). The security authorities are able to intrude a house with a separate resolution of the court.[12]

---

[9] This provision became effective between October 1997 and July 1998, and was in effect until 31 December 2001. Subsequently the Austrian government changed this law from temporary to permanent status.

[10] This is the catchword describing the use by the police of bugging and other audio- and video surveillance equipment inside private locals and rooms.

[11] This term stands for the automated and comprehensive matching of personal data registered in electronic databases according to certain searched for characteristics. For example, a set of known features of an unidentified criminal is matched with all personal data in one or more data registers in order to find persons whose features match with those of a criminal.

[12] Refers to the decision of the examining magistrates and the Council's Chamber.

In cases other than kidnapping, the investigating judge or a council of judges must decide whether electronic surveillance is needed or not. The monitoring can continue for a maximum of 30 days (even on the ground of "suspicion"), and can then be extended for a further 30 days. In the latter case, "suspicion" does not constitute a sufficient reason; a judge would have to decide whether there are sufficient reasons for prolonging surveillance.[13]

In 1999 Austria faced the first "mayor eavesdropping-attack". Its aim was to observe, pick up information and to unearth new evidence in the case of drug-dealers. A unit for observation - SEO (*Sondereinheit für Observation*) was set up solely for the purpose of managing these types of operations. This unit is directly responsible to the General Directorate for public security. It has also the right to commandeer video cameras – installed for the purpose of traffic management – in order to observe an object, such as buildings, offices or residences.

### *Security Police Act*

Visual or audio surveillance is not mentioned in § 48.[14] This clause merely refers to the term "observation", and does not include the collecting or processing of personal data. According to § 48 (1-4) the police may observe:

- people, when it believes that it thus serves the prevention of probable and dangerous attacks against their life, health and liberty;
- governmental authorities (oberste Staatsorgane) if a dangerous attack against their activities is suspected;
- property, if an imminent danger against it or against the environment of a human being is suspected;
- property, if a partial damage is imminent;
- people and property according to obligations of international law.

In consideration of § 48 (5) the police may only enter a non-public space[15] with the permission of its owner.

Audio and optic surveillance is explicitly noted in § 53[16] and § 54[17]. According to § 53 (1) the police may already collect and process data, when it believes that it thus serves:

- the defence against criminal organisations,

---

[13] Immunity from surveillance is granted to conversations subjected to professional secrecy.

[14] Observation of people and property.

[15] Premises which are not accessible to the public.

[16] Comprises the legitimacy of collecting and processing personal data.

[17] Refers to certain regulations of collecting data.

- and the prevention of probable dangerous attacks against life, health, morality, liberty, property or environment or the maintenance of public order at the occasion of a particular event.

According to § 53 (4) the police authorities may use any measure, such as the observation and use of audio and video equipments, in order to collect personal data. The automated matching of personal data through visual surveillance would refer to "biometric face recognition programmes".[18] This is exempted and not allowed under the Security Police Act, and thus is a matter of §§ 149 of the Code of Criminal Procedure (search by screening).

According to § 54 (2) the use of video surveillance of public behaviour is admissible for the purpose of investigating planned offences and crimes imputed to a criminal organisation. In reference to § 54 (4) 2 the use of video surveillance of non-public behaviour is only allowed in presence of an informer or an under-cover policeman, and if the planned offence or crime is punishable by more than one year. § 54 (4a) refers to proportionality and the protection of privacy of the person concerned.

### *Article 8 / ECHR*

The Austrian Constitution does not explicitly recognise the right of privacy. Some sections of the data protection law 2000 have constitutional status. These rights may only be restricted under the conditions of Article 8 of the European Convention of Human Rights (ECHR). The entire ECHR has constitutional status and the most obvious area for the application of Article 8 is direct interference by a public authority with the privacy of an individual in the form of covert surveillance. The 1950 Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8 states:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health of morals, or for the protection of the rights and freedoms of others.[19]

Experts assume that the second endorsement, article 8 (2), could be used by the police or secret services to justify their bugging or other surveillance measures under the prevention of crime, national security and public safety.

---

[18] Biometrics is the process of collecting, processing and storing details of a person's physical characteristics for the purpose of identification and authentication. The most popular forms of biometrics hand geometry, thumb scans, fingerprints, voice recognition, and digitised (electronically stored) photographs.

[19] http://www.hri.org/docs/ECHR50.html#C.Art8; http://www.hmso.gov.uk/acts/acts1998/80042–d.htm; http://conventions.coe.int/treaty/en/Treaties/Html/005.htm#FN1

## 3.2 Legal position: Regulating surveillance by private entities

As described in the previous section, this chapter shall outline the legitimacy of video surveillance by private bodies and how individuals are protected by the Austrian law. The following four statutes are relevant:

- Data protection law 2000
- Labour law
- § 16 – Civil Code
- Copyright Act

### *Data protection law 2000*

By implementing the "EU-Directive on Data protection 95/46/EG" the Austrian Parliament passed a new data protection law, the so-called "Datenschutzgesetz 2000" or "DSG 2000". This went into force on January 1st, 2000.[20] The aim of the data protection law is to protect ***individuals***, their right to privacy, with regard to the processing of personal data. Personal data means any information relating to an identified or identifiable person, like religion, profession, income or marital status. **Article 1** of the Austrian Data Protection Act concerning everybody's right of securing confidentiality about his or her personal data is a fundamental right protected by the Constitution which means that this Article can only be changed by a qualified majority of two-thirds of the Parliament. The Act is enforced by the Data Protection Commission.[21]

According to this Act, data may only be used fairly and lawfully for specified, explicit and legitimate purposes by a Controller who has the legal authority for the data processing. The data processing must not offend the legitimate interest of the data subject in privacy.[22] Whether such legitimate interest is offended or not depends on the qualification of the data as sensitive or non-sensitive. Data revealing racial and ethnic origin, political opinions, trade-union membership, religious or philosophical beliefs, health or sex life are sensitive data. The legitimate interest in privacy with respect to such sensitive data is not offended if the data subject has given their explicit consent to its use or if the use of data is necessary to protect the vital interests of a person. The legitimate interest in privacy with respect to non-sensitive data is not offended if the Controller or a third person have a prevailing legitimate interest for the use.

---

[20] http://www.argedaten.at/office/recht/dsg2000.htm. See also http://www.bka.gv.at/datenschutz/

[21] Everybody can turn to the so-called "*Datenschutzkommission*" alleging a breach of data protection rights. This supervisory authority consists of 6 members and is independent of the government. The authority has the power of investigation and, regardless whether data is processed in the private or public sector, may decide in case of breach of the *right of access to data*. This authority however may only decide concerning processed data in the public sector whether there is a breach of the right of confidentiality of processing, of rectifying and erasing of data. As far as data is processed in the private sector, the data subject has to go to ***court*** to claim his rights.

[22] Entertainment Law Review, 2000 by Kristina Silberbauer (http://www.dbj.co.at)

### *Labour Law*

Two laws in Austria regulate electronic surveillance at work. The first is the Labour Constitution Act 1974 (*Arbeitsverfassungsgesetz* or ArbVG), especially sections 91 and 96.

Measures of control and technical control systems, if they touch upon human dignity, may be introduced only with the consent of the works council. Any measures infringing human dignity are unlawful. Such measures include:

- observation by closed circuit TV of premises at which employees work;
- personnel information systems that collect work-related data that might yield information about an individual's personality or that could create the impression of excessive personal surveillance and evaluation;
- any form of automatic control of entry and exit or presence on the job.

The second law is the Employment Contract Law, Adaptation Act 1993 (*Arbeitsvertragsrechts-Anpassungsgesetz*), especially section 10. All measures of control and of technical systems touching upon human dignity in the absence of a works council are declared unlawful, except by consent of the employee.[23] However, the legal basis for control is the employment contract itself.

### *§ 16 - Civil Code*

Another statutory provision is the general protection of a persons integrity which is provided by § 16 of the Civil Code (*Allgemeines Bürgerliches Gesetzbuch* – ABGB).[24] In the context of video surveillance this general right has to be construed in conformity with the fundamental right to privacy (Art 8 - EHRC). However, it does not automatically follow these two clauses that every single interference is unlawful. In fact, the interests between the observed person and the surveillant have to be considered and valuated. The Austrian Supreme Court dealt with two cases of video surveillance by private bodies and referred twice to § 16 - Civil Code:

- A landlady installed a video surveillance system with four cameras in her tenement viewing the main entrance, the staircase, and the house door of every single resident. One of the tenants sued the landlady for interfering in his privacy. The Supreme Court asserted that the protection of privacy does not end behind the house door yet also that the landlady has a legitimated interest to protect her property. For that reason the Supreme Court pronounced the following judgement: The video

[23] European Foundation for the Improvement of Living and Working Conditions (www.eiro.eurofound.ie)

[24] Every human being has inherent rights and has to be seen as a person. The right for privacy is an inherent right.

surveillance in front of the main entrance and within the staircase is admissible whereas the surveillance of the apartment door is not.

- The second case refers to a court procedure between two parties, in which one sued the other for installing a video surveillance system at its house. The problem was that one of these cameras displayed – at a certain visual angle – the land-property of the neighbours. The Court referred to clause 16 of the Common Civil Code as a legal basis and pronounced the following judgement: The unaccepted or undesirable surveillance of the own person and family is an interference with personal rights. The defendant was acknowledged the right to protect his own private property but was ordered to change the tilt angle of his video cameras so as not to view the neighbouring house or garden.

Hence, the consideration and valuation between the interests of both parties serve as a basis. This is important and relevant to adjudicate upon the violation of privacy.

### *Copyright Act*

According to § 78 of the Copyright law it is not allowed to circulate images of persons to the public if legitimated interests of this person are offended.

## 3.3 Conclusion

Video surveillance by public entities are subject to strict statutory controls. Audio and optic observation is covered by the Code of Criminal and the Security Police Act. The application of the regulation encounters difficulties since the wording of the law is open to various interpretations regarding the suspicion of probable dangerous attack and the maintenance of public order. This could lead to investigating data of persons not defined in advance and thus to the infringement of individual rights.

Other than the regulation of optic surveillance by public authorities, private bodies enjoy a larger opportunity to observe individuals and premises. There is no statute which explicitly regulates the use or setting up of CCTV. The relevant texts of the law do not include the regulation of optic surveillance. They refer to the basic rights and privacy of a person. This creates a certain legal vacuum.[25] Furthermore, insofar as there exists no specific prohibition regarding the utilisation of evidence in court, observers may conclude that "everything"[26] is allowed.

It can be concluded that the regulatory framework with regard to video surveillance by private bodies must be reconsidered. The increasing expansion rate of private users could otherwise lead to unintended negative effect.

---

[25] This is best illustrated by the example of private detectives. In Austria these professional groups very often run the risk to impinge upon the personal rights of observed people.

[26] Interview with Hans G. Zeger (13.02.02)

# 4 The policy process

## 4.1 The role of private actors and social movements

In the private sector it is mainly security firms which provide their clients with a modern standard of equipment in order to protect and secure their property. Nowadays they undertake many tasks of the police and for them permanent video surveillance is already a matter of course. The most famous security firm in Austria, Group 4 Securitas, makes advertisement for CCTV with a link on its homepage.[27] It is the only supplier with a publicity in the field of CCTV. Moreover, it offers planning and installation, and a counselling interview with security experts. The link also indicates the importance of video surveillance in the event of loss or damage.[28]

At the homepage, this company also advertises the visual copy cycle. Enterprises wishing more security may have the opportunity to install video cameras at their premises. These cameras provide a so-called visual copy cycle directly to the reception for emergency calls, so that the attendance of a security officer on site is not necessary or becomes redundant.

The mission of security firms in general is an advocacy for more surveillance in society. Therefore, these businesses can be seen as main proponents in the field of video surveillance.

At the other end of the spectrum we fine organisations such as the Austrian "ARGE Daten"[29] which attempt to raise public awareness and mobilise against surveillance. Since 1999 ARGE Daten together with other affiliate groups[30] present the so-called 'Big Brother Awards"[31] to government agencies, private companies and individuals who have excelled in the violation of privacy. This event can be seen as a campaign and a successful attempt to focus attention on the protection of personal privacy. None of the awards till now have dealt explicitly with video control.

---

[27] http://www.group4.at/frameset.htm

[28] Excursion: For that reason, many Austrian insurance companies require less premium in the case of installing video cameras.

[29] An independent, non-government organisation with the primary role of advocacy and support in the field of data protection and privacy issues

[30] Chello User Group (internetplatform for chello users), Public Netbase (institute for new culture technologies), Quintessenz (association for the restoration of civil rights in the information age), and Vibe!at (society of internet users in Austria)

[31] The awards were judged by a panel of experts, comprising lawyers, academics, journalists and civil rights activists. The nominations received covered a wide spectrum, ranging from large, well-known institutions, to smaller organisations which specialise in surveillance.

## 4.2 The role of political parties

There is no nation-wide demand for CCTV on the political level. Public space surveillance at the local level is a decision that primarily rests with mayors or city councillors. It is arranged either with local electronic retailers or – in most cases – with private security firms.[32] The deals are for the most part not publicised.[33]

At the political party level we find no party explicitly calling for video surveillance. However, the party programme of the FPOE[34] contains clauses with indications to measures of surveillance. In chapter 9 "Law and order", article 3(1) states that: "In the fight against crime (...) computer searches, electronic eavesdropping and rules concerning chief witnesses are suitable." Article 3(2) specifies nevertheless that: "The measures necessary for this purpose must not, however, degenerate into restrictive surveillance system. Their use must be subject to strict statutory regulations".[35] A more explicit declaration in favour of surveillance is found in the "Anti-terror-package"[36] of the FPOE. Two provisions contain the necessity of modern equipped electronic ID-systems, comprising biometric methods, and the expansion of precise data network. The latter even explicates that data protection should not stand for the protection of perpetrators. As mentioned in the legal framework, the introduction of biometric methods could immediately lead to visual surveillance by "face recognition programmes". Thus, the FPOE can be quoted as the leading advocator of surveillance. The position of the second governmental party, the OEVP[37], is less polemic yet still positive.

According to several political observers different positions[38] exist within the SPOE,[39] even though their position papers and party programme do not require surveillance methods and their press releases contain clear statements against any violation of civil rights.[40] The Austrian Green Party is the only political party which prioritises the protection of privacy and basic rights on their political agenda. Their steadfast refusal to vote in favour of increasing surveillance measures is mentioned in their manifesto. Their statements mainly refer to surveillance in general and not specifically to video surveillance. Their position against any threat to privacy or civil rights is clear and precise.

---

[32] Interview with H. Zeger (13.02.02) / Interview with Stephan Landrock (18.02.02)

[33] E.g.: The head of an Austrian security firm refused to name the city, with whose mayor he wanted to work out a security concept. This plan focused on positioning video cameras in public space.

[34] FPOE – Austrian Freedom's party (far right-wing, populist)

[35] Programme of the Freedom Party of Austria (www.fpoe.at)

[36] FPOE´s position paper on combating terrorism and crime/ 19.10.2001

[37] OEVP – Austrian People's Party (conservative)

[38] Interview with W.Peissl 26.02.02

[39] SPOE – Austrian Social democratic party

[40] www.spoe.at/index1.htm

The question of surveillance – scope and legitimacy – often stirs political confrontations at the local level.

- In Vienna the of the Freedom Party's (FPOE) top candidate for the municipal elections wanted to have video cameras installed at places where there was drug dealing. Pursuant to her statements and suggestions, the public entering this area should encounter the warning sign that these premises are under constant video surveillance.41
- A further demand for CCTV came from a politician of the Viennese People's party (OEVP at the district level. He wanted to install a so-called SOS-telephone with integrated cameras in public space. This statement was also made during the campaign for the municipal elections in Vienna. The administration of Vienna refused to consider this proposition.42

### 4.3 Three lines of argumentation

There has not been a public debate on video surveillance like in other countries, such as the UK and the USA. Discussions on the expert level referred mainly to the relationship of surveillance, security, privacy, proportionality and social costs.

Principally, there are three distinct lines of argumentation with regard to surveillance:

- The classical argument is, if "you are doing nothing wrong, surveillance does not matter".43 This statement refers to the spectrum which appreciates more surveillance in the hope to achieve more security.
- A minority dislikes any kind of surveillance, they even see the use of credit cards etc. as an interference with privacy.
- The third spectrum, which can also be found across nearly all political ideologies, questions the relationship of surveillance and security and brings in the factor of social costs. They argue that: [44]

  > The social cost of surveillance is not limited to the invasion of privacy. The collection, processing, storage and communication of personal data establishes norms of behaviour and standardises categories of social groups. This imposition of normality limits individual choice and restricts society's necessary potential for change. It also subjects individuals to discrimination.
  >
  > Therefore, surveillance systems should only be implemented if they are effective, not easily circumvented, and will produce a real security benefit. Surveillance systems should

41 APA – Austrian Press Agency 16.02.2001

42 Falter (16.10.2001)

43 CCSR – Centre for Computing and Social Responsibility (http://www.ccsr.cse.dmu.ac.uk)

44 Interview with W. Peissl, 26.02.02

only be implemented if the benefits are worth the social costs, including the invasion of privacy, loss of autonomy, social discrimination, or imposition of conformity? (This means applying the principle of proportionality.) If it will produce a security benefit that justifies the social costs, measures will have to be taken to minimise those costs. Before any surveillance system is implemented, legal mechanisms of oversight and redress will have to be established. The effects – both positive and negative – of the systems will have to be periodically reviewed by an independent publicly accountable body.[45]

[45] "Declaration of Amsterdam" (www.privacyconference.nl/decleration.html) - The text of this declaration was written by the Rathenau Institute in close co-operation with the different speakers of a conference. The "Declaration" served as a discussion paper. The subject of the contributors mainly referred to the relationship between surveillance and security, protection and violation of personal data and privacy. The Rathenau Institute, a technology assessment organisation of the Netherlands, brings together international experts on privacy and ICT (Information & Communications Technology) in order to explore the current practices and existing insights in different countries.

# 5 The Policy Debate

## 5.1 Media analysis

For the analysis of the term "video surveillance" in the Austrian press, the attention was drawn on 3 daily and 1 weekly newspapers ("Der Standard", "Falter", "Die Presse", and "Kronen Zeitung"). Three of them are published nation-wide and the fourth one ("Falter") is circulated only in Vienna. All four newspapers cover nearly the whole political spectrum from left-centre and liberal to centre-right as well as the right-wing populist.[46]

The articles for the analysis range from November 1998 to November 2001. By using keywords, such as video surveillance, road safety, crime, crime prevention, drugs and security services, 19 articles ("Der Standard"), 15 (Falter), 24 ("Die Presse") and 96 articles ("Kronen Zeitung") were collected through the archive search.

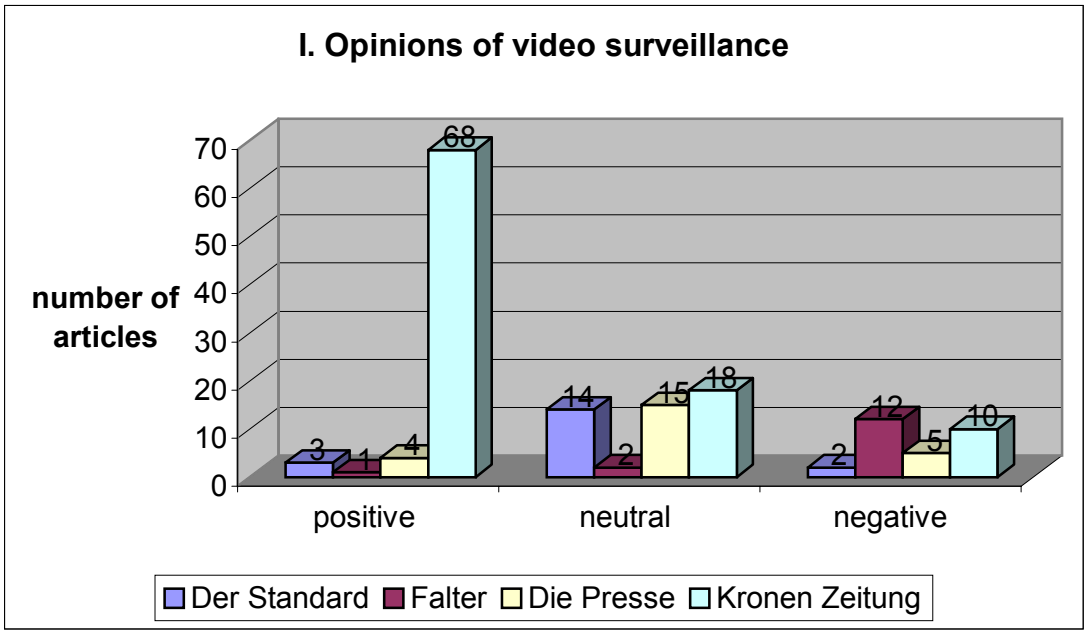



Figure I is a clear proof of the positive orientation of the yellow press, namely the "Kronen Zeitung", to surveillance. 68 out of 96 articles (over 70 percent) displayed a positive opinion as compared to 3 out of 19 (16 percent) in the case of "Der Standard", 4 out of 24 (16 percent) in the case of "Die Presse" and 1 out of 15 (6 percent) in the case of "Falter". It is worth noting furthermore that in terms of political orientation the "Kronen Zeitung" is the most extreme and right-wing insofar as xenophobia is concerned.

[46] "Der Standard": liberal; "Falter": centre-left/ liberal; "Die Presse": conservative; "Kronen Zeitung": right-wing populist

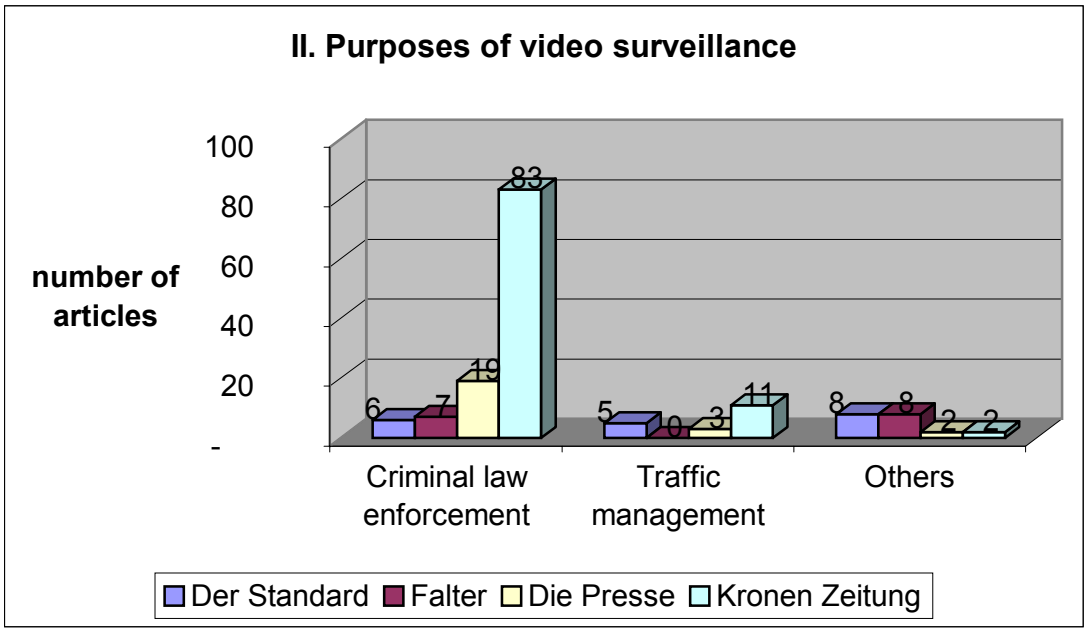



Figure II shows the frequent association between video surveillance with security and criminal law enforcement, especially in the yellow press, namely "Kronen Zeitung". The articles in the "Kronen Zeitung" relate mainly to the cases of crime and drug prevention as well as the enforcement of criminal law, whereas other newspapers articles tend to deal more frequently with the problem of traffic management and transport policy. The very high number of articles in the time spread of 1999 (Figure IV) are due to a severe accident in a tunnel[47] and on highways.

[47] Tauerntunnel Fire/ 29 May 1999: 12 people died, 47 were seriously injured (http://www.land-sbg.gv.at/lkorr/1999/05/31/19793.html

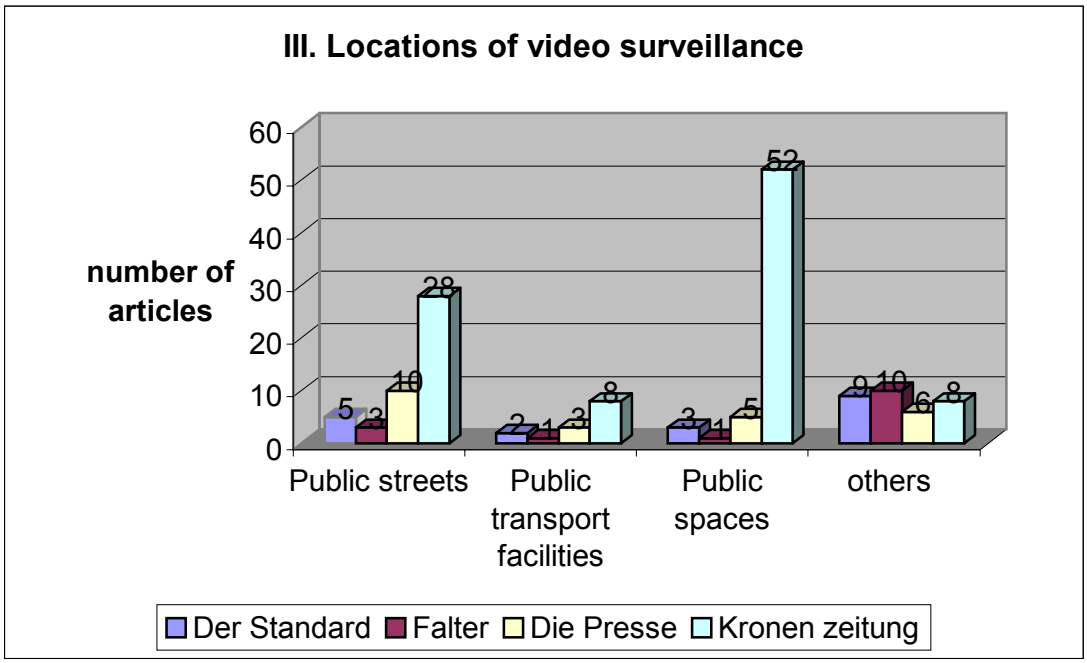
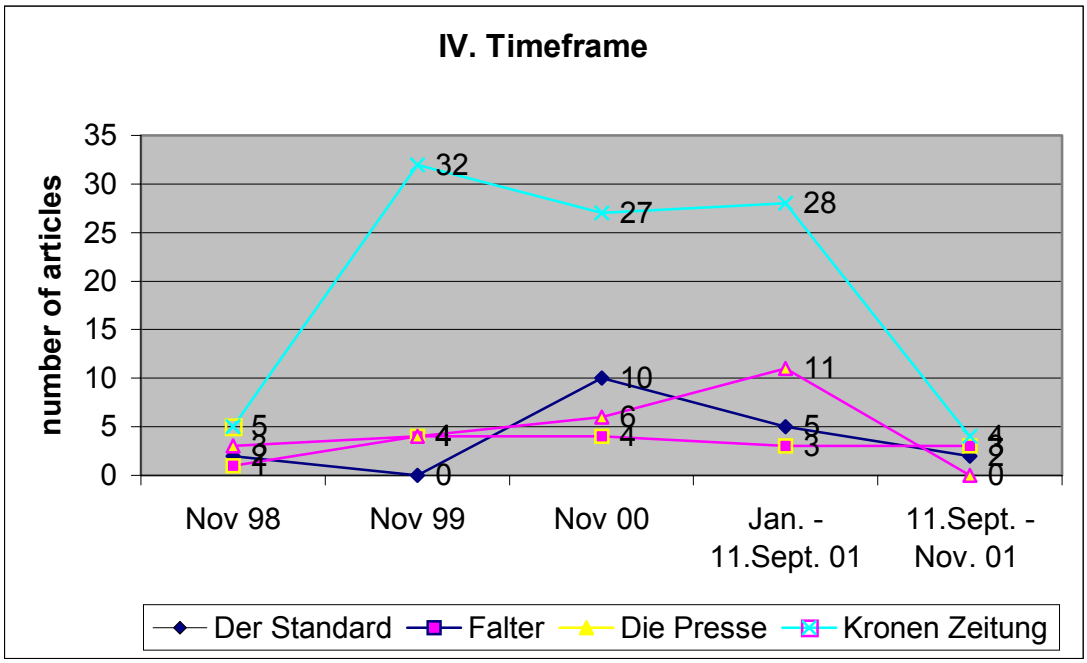



Figure III shows the frequency of reference to the location of video surveillance in media reports. The results are best appreciated if one considers the overall positive orientation of the "Kronen Zeitung" to video surveillance (Figure I).

The remarkable point is that the articles only mentioned the use of video surveillance secondarily. The only exception were two articles from the Falter. The first analysed the possible danger of surveillance, and furthermore, questioned the relationship of security and privacy. This article with the main title "filmen, filzen, und fassen" [48] ("filming, searching, and seizing") dealt further with the possible introduction of face recognition programmes and their risk. The second article was a TV-preview of an American film ("Enemy of the State"), and analysed the possible dystopian vision of total surveillance in public space.

[48] Der Falter / 16.10.2001




In figure IV the attention was drawn on the timeframe, especially the time span after the 11th of September 2001. The research ranges only from September to November 2001, in other words two months, but there is no significant increase of articles written on the topic of video surveillance in any mentioned newspaper, except the article of the Falter mentioned in the previous chapter. The date of publication of this article is worth mentioning. It was edited a few weeks after the terror attacks. During this time many ideas of surveillance and measures restricting privacy, such as biometrics methods including video cameras with face recognition programmes, were put on the political agenda.

## 5.2 The position of Austrian society towards video surveillance

The very important part of empirical research is the appreciation of the competing interests between privacy and security. Only one survey was conducted in Austria on public opinion towards video surveillance.

According to this study, 84% of Austrian citizens are in favour of video and more generally electronic surveillance in the field of organised crime. 68% are in favour of this method for combating serious crime (capital crime), whereas 63% dislike this system if it is used for the persecution of small-time criminals. 58% of Austrian citizens do not feel threatened in their privacy through the new tracing methods, whereas 39% fear to come in contact with the police or judiciary by mistake. [49]

[49] Survey conducted by "SWS – Sozialwissenschaftliche Studiengesellschaft" in 1999

# 6 Conclusion

At one level, the policy process and debate on video surveillance in Austria concentrates on transport policy and traffic management. At another level, including justice and home affairs and not least the media, we can observe a gradual sensitisation – both in positive and negative terms – towards the close link between video surveillance and crime / security but also privacy.

At the expert level, there are no doubt clear concerns that the surveillance of public space could lead to a serious loss of autonomy and the endangering of privacy and freedom, leading in turn to changes in social behaviour. Every dissenting behaviour could be interpreted as criminal. Diversity and variety, which define society, would break down. The use of video cameras for the purpose of preventing crime or tracing criminals could revert the so-called presumption of innocence which is one of the pillars of a liberal constitutional state.[50]

With regard to the future expansion of video surveillance in public space there are different positions. Some consider it likely that Austrian cities develop in the same direction like UK cities over the next 15 years.[51] Others argue that Austria will never face the same pattern as in the UK. The division of opinion in this respect is no surprise as it is also closely linked with different values and preferences on the same subject.

There is a consensus on the expert level that video surveillance in the private sector will increase in the following years. There is no doubt about this development and the expansion rate. The desire to use video surveillance as a means of deterring crime and averting violence is increasing. The pressure to use video surveillance for purposes other than public order law enforcement may become hard to resist and, in the future, technology may be used in ways which are increasingly more privacy invasive. Therefore, strict policies regarding the use of video surveillance in private sector should also be created, applied and revised as appropriate.

[50] Interview with W. Peissl (26.02.02)

[51] Interview with R. König (07.03.02)