



The Legal Regulation of CCTV in Europe

Marianne L. Gras¹

Abstract

This paper explores the recent history of CCTV system regulation in England and Wales questioning whether recent additions to the law can be regarded as providing for effective regulation, in particular, of camera numbers. It goes on to explore the legal landscape relating to public and private use of CCTV to subject publicly accessible space to surveillance in Germany as well as giving an overview of the regulatory systems in France, the Netherlands and Sweden. Drawing from this analysis, minimum standards for effective regulation are explored in terms of fulfilling both the letter and the spirit of laws across Europe.

CCTV and Legal Regulation in Britain

What is the legal regulation of CCTV? Simply, a body of legal norms to regulate surveillance cameras and their use to observe individuals in a public space. A few years ago, in the mid 1990s when CCTV systems were starting to be installed in town centres across England and Wales any English (or Welsh) lawyer could more or less happily have said regulation isn't necessary according to English law. He or she would have pointed out that there is no right to privacy (at least not independent of property rights) in this country, so there is little a person unhappy about being subjected to surveillance can do. The lawyer might have pointed out that where local authorities spend money on CCTV systems, they have a legislative basis for doing so (para. 163 of the Criminal Justice and Public Order Act 1994, London Local Authorities (No. 2) Act 1990) and furthermore, that a possibility for real control, namely the need for planning permission, (Town and Country Planning (General Permitted Development) Order 1995 Part 33, SI 1995 No. 418) had been deliberately abolished in relation to camera installation. Those more concerned with privacy, may have pointed to article 8 of the European Convention on Human Rights which gives even British subjects a right to privacy. A certain amount of jurisprudence from the Human Rights Court could also have been cited to support this line of argument. One could, however, also point to other judgements of the same court underlining the difficulty of satisfactorily proving a measure (already installed) as unnecessary in a democratic society. The more cynically inclined could point to reactive British legislation born of

¹ Abteilung Kriminologie der Juristischen Fakultät der Georg-August-Universität Göttingen, Germany.
<mailto:mgras@uni-goettingen.de>

(at least expected) condemnation from the Strasbourg court, making the actual situation worse in the name of fulfilling the letter of the European Convention on Human Rights. One could, however, be certain of one matter, no British court could ever demand legal regulation of CCTV based on the legal situation at the time.

That the tenor of debate has changed, since the 1998 Human Rights Act, there is no doubt. Even British subjects (or are we now citizens?) have a right to privacy, also in public places. With reports of over 4 million cameras in use in Britain (McCahill and Norris, 2004), European lawyers seem uneasy. How can so many cameras be regarded as satisfying a test of proportionality. The Home Office, however, pronounces itself "confident" that British CCTV practice is in line with the Human Rights Act (Henderson 2001). The recent hearing of *Peck v. United Kingdom* in Strasbourg, in spite of the complaint for treatment which can only be described as an ultimate breach of privacy (at least in continental European terms) being upheld, seems to confirm this view. The Court did not appear overly keen to criticise the prolific use of CCTV in Britain. Indeed there is reason to believe that the mere use of CCTV surveillance will not suffice to invoke article 8 (see e.g.: Taylor, 2002: 76)

We have also seen the 1995 European Data Protection Directive put into practice by the 1998 Data Protection Act. By 2003 all CCTV systems controllers were required to register with the Information Commissioner and to ensure they are operating in line with data protection principles. These were made explicitly applicable to all CCTV systems and specifically defined in a Code of Practice for CCTV. Although the legal status of these rules isn't entirely clear, anyone operating a system would be unwise not to adhere to them. Breach of the law, as defined by these guidelines, is a crime and the principles laid down sound rather good: open, fair, proportional. Surely that's regulation of CCTV and quite good too?

Well it is. And yes, one could describe British systems which work by the rules as well regulated. The fact that the regulation came after a great deal of the systems had been installed is, to European minds, a bit peculiar, but then history works in strange ways and it's the end result that counts. To be fair, the end result cannot yet be seen and there are signs that the changed legal situation is making a difference. In June 2003 a High Court ruled that "name and shame" campaigns using CCTV recordings could be illegal. The law contains potential to alter the (mal-) practices which appeared to have been frequent in the past.

The law also contains requirements such as proportionality which, as we will see, could be a key to setting quite different standards and ultimately requiring that systems currently in place in Britain might have to be dismantled. The law has this potential, if it is interpreted and enforced in this way. And here lies the crux. The essence of the threat many regard as emanating from CCTV is not captured well by legislation concerning data protection. A growing net of cameras with the potential to surveil an individual day in, day out may in fact do no more than give that individual the perception of being under surveillance. That is what CCTV systems and even dummy cameras intend to do in order to deter that individual from committing a crime. Regulation dealing with factual gathering of personal data will not be invoked in the vast majority of cases. This is particularly true in light of the recent Court of Appeal decision in *Durant v. FSA* ([2003] EWCA Civ 1746) limiting the definition of 'personal data'.

Even beyond legal argument and assuming CCTV systems will remain fully subject to data protection legislation, for very practical reasons, like the actual resources available to enforce these rules, serious doubts remain that Britain, has *effective* regulation. Regulatory bodies in the UK notoriously lack resources and are reliant upon the good-will and co-operation of those they are regulating and their activities are frequently triggered by a specific complaint (see e.g.: Sanders and Young, 2000: 365). These issues become all the more relevant in the data protection field where breaches of regulation will not leave any physical trace.

Let us however assume that CCTV systems in the UK work according to data protection regulation and are within the ambit of what is regarded as necessary in a democratic society as defined by the European Convention. In that case, the legal situation in England and Wales could be said to regulate CCTV. It is, however, no more than regulation of work with CCTV. It is by no means regulation of the main issue surrounding CCTV. Namely legal control of whether a camera may be installed or not. How could it be? The cameras were there first. We cannot conclusively say that it never will effectively regulate CCTV, although the idea of installed systems being dismantled due to these regulations doesn't fit easily with the development in England and Wales so far. Any ruling coming after the fact – unless it is effectively forbidding it – must surely lead to far-reaching changes before it can be claimed to be doing anything more than just clearing up the mess and damming in the damage.

The regulation of CCTV in Britain can at most be regarded as potentially interesting for others in terms of good practice. But as far as the most basic issue of regulating CCTV is concerned, namely regulating the number of cameras installed, English law cannot be said to be of any interest to another country.

As the above analysis has demonstrated, in Britain we have not been able to rely on European privacy law to regulate CCTV use. Although the issue is controversial, it is difficult to conclusively declare the British situation as compatible with or in breach of European legislation. Thus the search for European regulation becomes a question of whether other European countries have regulated CCTV at a national level. As Britain is still regarded as world-wide leader as far as camera surveillance is concerned, it would appear that Britain is either quicker than the others or that they have more effective regulation.

In terms of avoiding high camera numbers, Denmark certainly has stronger regulation than Britain. CCTV surveillance is generally forbidden there. There are exceptions for owners of certain kinds of property, such as petrol stations. They are subject to a strong requirement to inform those subjected to surveillance about it. Public authorities and the police are permitted to use CCTV. The police can also do so covertly. These exceptions may appear far reaching, but if one considers the proportion of British cameras which were installed and are owned by non-public bodies, but which make up such a significant part of the surveillance net, it is not difficult to imagine how different the situation might be, if a general ban on such systems had been in place during the 1990s. Denmark's position is however unique.

Before I can begin an more in-depth analysis of other European legal systems, some closer definition of the subject matter would appear necessary. As has frequently been pointed out, CCTV surveillance is a diverse phenomenon (see e.g.: Norris and Armstrong, 1999: 55). For this paper's purpose, it is sufficient to define it as camera surveillance of publicly accessible space. Publicly accessible space can be a street or square, but also includes what is factually private property, open to the public, such as banks, petrol stations, etc. A CCTV system can be run by a public authority, like the police, or by a private owner or body. As we will see, the regulation of CCTV within Europe usually differentiates between private and public, in particular police, CCTV.

Germany

Germany is a case in point. The situation there is complicated by the country's federal structure. As far as video surveillance is concerned, it is sufficient to say that the installation of cameras to surveil an area permanently, in so far as this is done by a public authority, is governed by state or 'Länder' police law. This means that each of the 16 German Länder can have differing situations. In fact, there are not 16 different solutions; about 3 can be easily identified: a) Länder with no legal basis for CCTV surveillance as British people know it, b) states allowing video surveillance by the police in certain, relatively well-defined situations and c) states with a wider ranging legal permit for police and occasionally other public authorities, to install CCTV systems, to make recordings and to store these for a relatively long period of time (Weinbrenner, 2001).

CCTV can of course not only be installed by public bodies (and for the most part in Germany, discussion about allowing public instalment of CCTV focuses almost exclusively on the police) but also by private persons or entities. Where private property is open to the public, this too falls under the law. As in other continental legal systems, however, a private person wishing to use cameras to watch over his or her own property is regarded as entirely different to the police wishing to observe a public road or square.

Surveillance by Private Persons or Entities

A person may install and use CCTV on the basis of his or her rights as the owner of property (Hausrecht). This right is, however, not unlimited, as his or her actions touch upon the human rights of those affected, namely their right to develop their personality freely (Recht auf freie Entfaltung der Persönlichkeit). This right is protected by article 2 I of the German constitution in connection with article 1 I. This general right to one's own personality includes the right to one's own picture (BVerfGE 34, 238, 246, 248). The legality of an interference with this right, is judged according to the 'Sphären' or 'Drei-Stufen-Theorie' (sphere or three steps theory) of the Federal Constitutional Court. According to this theory, every person has three levels of privacy. She or he has a right to privacy, but as a social being is also required to accept a certain limitation of this right. Centrally, there is the intimate sphere (Intimsphäre) or the core area (Kernbereich) of his or her personality, which receives absolute protection. Beyond that, there is the basic private sphere (die schlichte Privatsphäre) and the individual sphere (Individualsphäre). These can be interfered with on the condition that Verhältnismäßigkeit - proportionality - is preserved in doing so. This has particular relevance in relation to CCTV, because any recording

made can be used before a court, which is regarded as state (i.e. a higher level of) interference. The property owner's or (where recordings are to be used before court) general public's interest is weighed against the individual's right to privacy and the former must outweigh the individual's in order for surveillance to be permitted, i.e. the general public's interest in prosecuting crime must be weightier in order for recordings to be admissible as evidence (BVerfGE 34, 238, 247).

Interference by CCTV will often be considered as comparatively light as it only takes place for as long as one is within a certain space. Surveillance is even more likely to be regarded as proportionate, if one gives persons who become the objects of surveillance a choice whether or not to subject themselves to it by informing them of this surveillance. In this case, the arguments against CCTV are regarded as fairly weak because there is implicit consent to CCTV surveillance. The fact that a person who, for example, needs to travel may have to enter a train station with CCTV to do so and, therefore effectively has no choice, has yet to be addressed. It is likely to become more controversial as camera numbers increase. This situation cannot really said to be one of satisfactory regulation and is the subject of frequent criticism in particular by the Data Protection Commissioners of the federal states and at national level. The new Federal Data Protection Act does nothing to improve the situation. As the number of cameras grows, however, the pressure for more regulation is growing too.

On a positive note, one should mention that the courts do perform a real balancing evaluation. Where people are being filmed regularly near their homes or where the court has deemed milder measures more suitable, an order will be made to dismantle a camera. In the most famous case the Federal Court ordered one party in a conflict between neighbours to remove the camera he had installed to document high noise levels being caused by his neighbours. The court surmised that those affected were subjected to a feeling of being watched permanently and that the interests of the other party could not justify this, particularly as other less intrusive methods, could achieve any documentation deemed necessary (see BGH-Urteil NJW 1995, 1955). Furthermore, although there is a central weakness: that illegally obtained pictures are also weighed against the individual's interest, one recent court decision, shows that this type of regulation does have some effect. In this case, the court refused to admit recordings of a customer apparently swapping price labels in order to purchase a purse at a significantly lower price, because the department store detective had used the CCTV (which was considered secret because no signs drew attention to it) to secure evidence of a crime and not to prevent damage being caused to the owner by it. In other words, secret CCTV would be permissible if used to take immediate steps and to prevent crime. Where this purpose is not served, individual privacy is more important. Where CCTV is used more as a form of entrapment to secure evidence, the courts will declare this use unfair and illegal, if no warning of potential surveillance is given.

Nevertheless, as far as privately owned property is concerned, the ability to film and surveil using CCTV is far-reaching and recordings made will often be admissible before a court. Even illegally made recordings may well be considered to be admissible evidence of a crime (Beulke, 2002: 474).

The use of CCTV by private persons and entities accounts for the vast majority of installations. This is true both in Germany and in the UK. A recent study illustrates very clearly how these installations contribute to the surveillance net and it should, of course, not be forgotten, that these cameras also present a resource to the police (For clear illustration of the role and extent of such surveillance to protect buildings and traffic networks in London and Berlin see Töpfer *et al.*, 2003: 33-40; and McCahill and Norris, 2002: 6-10, in particular). Where the police work actively to integrate such cameras into their strategy (as e.g.: in Munich, see: Simon, 2000) this is all the more true.

Police Surveillance

As far as surveillance by public authorities (and in Germany this usually means the police) is concerned, we have an entirely different situation. There is a very complex constitutional argument about whether mere observation of a scene in which no individual person is identifiable via a camera, is an interference with a German citizens' basic rights and therefore requires specific legal regulation. This debate has, however, become unimportant in practice because: a) it is now almost superfluous, as the majority of Länder and the Federal government have introduced permissive legislation for CCTV surveillance and b) because CCTV as it is used in the UK, and as the police in Germany are finding they wish to use it, is not about observing unidentifiable groups of people, a central aim is precisely the ability to observe an individual and to enable his or her identification. The latter is unquestionably an interference with a person's basic rights according to German constitutional law.

We can, therefore, assume that using CCTV without a permissive legal basis is illegal. For this reason most Länder have introduced legislation more or less like that of Saxony, for example, where § 38 2 of the Saxon Police Act allows police to surveil and record in various (broadly defined) geographic areas where actual indications justify the assumption that, in this type of place or at objects of this sort, offences will be committed which endanger persons, objects or assets (so-called Vermögenswerte).

These laws are not quite as broad as they sound at first as they are subject to the constitutional principles of *Verhältnismäßigkeit* and *Erforderlichkeit* - as are all state institutions in the exercise of their power. *Verhältnismäßigkeit* or proportionality means that the method chosen may not be disproportional to the problem to be solved. Accordingly, some experts regard the interference with constitutional rights as illegal in order to combat crimes of a trivial nature. Indeed some states expressly forbid this.

Erforderlichkeit means that the method chosen must be appropriate and necessary, i.e. it must be one which promises to solve the problem and must be the mildest possible method in the sense that it interferes as little as possible with the rights of those affected.

The Impact of Legislation

The practical effects of this legislation, and in particular of the debates which surrounded the creation of permissive regulation, have been that the police and those legislating for police forces, appear to feel a need to justify the use of CCTV. Thus an installation will often be preceded by a crime rate analysis to prove the need for CCTV and this analysis will continue whilst the cameras

are in action. Persons running CCTV systems might well argue that no legal regulation is necessary to achieve this and they may well be right. Well run systems should be doing this anyway. A legal requirement to do so is still a different matter. Furthermore, it should be stressed that German law requires a justification and legislative basis for interference with an individual's rights. This may not seem like much in the face of the potential threat to these rights some of us regard CCTV as being, particularly since the police can and do still install. Nevertheless, I think it is safe to say that so far the legal requirements have led to police and decision makers being cautious about the installation of CCTV. This is reflected in the relative limited number and size of CCTV systems in Germany (which usually consist of less than 10 cameras) and the fact that in Leipzig one camera was dismantled after it was deemed no longer to be necessary. A system, in Bielefeld, also stopped operating for some time for the same reason. Comments can also be found in the press which illustrate a greater awareness of potential controversy, thus one can read for example, that a chief superintendent (in Leipzig) has no interest in linking police to private cameras, not because of technical difficulties but because "we do not want an English situation" (Holzer and Krischer, 2000). There is evidence of general awareness that there is a conflict of interests.

The legal regulation in Germany is one matter and its power should not be over-estimated. In spite of all I have said, the use of CCTV is increasing and it is not always being used in ways one would regard as compatible with the stringent enforcement of the principles mentioned above. Nevertheless, in comparison to the British situation it must be regarded as advantageous. The need for permissive legislation meant that parliamentary debate had to ensue, relatively strong data protection institutions were able to give these debates a serious critical flavour, which even hard-line CCTV supporters were forced to acknowledge. In some cases, they led to legal restrictions in the police use of CCTV (Northrhein-Westphalia), in others they did not. But at least an atmosphere was created from the very beginning in which police were aware that some citizens would question their use of CCTV. Whilst the use of CCTV will certainly continue to grow, potentially excessively, especially if surveillance by private owners is not regulated in some way other than a post-hoc appeal possibility before courts, one can say that legal regulation of CCTV exists in Germany. As far as use by public owners is concerned, this regulation has been relatively successful, so far, in ensuring that CCTV is used - I would like to say only in situations in which it is truly necessary, that would however be overly optimistic - only in fairly limited circumstances. This may change as post 9.11 legislation comes into use. So far, however, the spread has not been extensive. Public systems are small and still relatively low in number.

As far as the regulation of privately owned systems are concerned, there are other examples of regulation in Europe which require an installation to be approved. This would appear to be a potentially effective means of regulation.

France

In France for example a 1995 law and a 1996 decree require that the Prefect in each French *Département* (administrative region) be informed of any plans to install a CCTV system and that he or she decide whether the installation is to be approved. In making this decision, the Prefect

must consult a local committee, the CDV, which is presided over by a judge. Alongside the judge, the CDV is manned by another magistrate, a representative elected by the local trade chamber, an elected politician such as the mayor and a person with technical knowledge (who may, however, not be a serving police officer). Their decision is made by majority vote and is a recommendation to the Prefect, which he or she will, however, almost always go by, because the CDV is more competent to make the decision than he or she is. The Prefect's decision is final but can be contested before an administrative court (i.e. is subject to judicial review). An applicant must prove that the area one wishes to protect by CCTV is an object particularly liable to theft or attack.

By the end of 1999, 38.520 CCTV installations had been approved. In 1999, 4500 applications to install CCTV were filed, 4200 were approved, 300 were refused, because they violated the law. In other words a considerable number of CCTV systems are applied for and only a small minority do not gain approval (most of whom are told what needs to be changed in order to gain approval). This has been the subject of particular criticism. It should, however, be noted that of these figures, a large number of applications stemmed from banks, petrol stations and shops. Areas in which, in Britain but also in Germany, CCTV installations have long taken place and are regarded as relatively uncontroversial. In how far this will prove to be an effective control of CCTV remains to be seen. Clearly the legal and institutional potential to effectively regulate the use of CCTV systems is there, in how far practice will do this, is another matter. The failure to include police cameras in this legal framework is a subject of considerable controversy in France (Oqueteau, 2001).

Sweden

Another, at least apparently, well-regulated system is the Swedish one. Here, again, there is a kind of licensing system. All potential CCTV users (except for those who wish to use cameras to observe a 'protected object', to improve a drivers sight when installed onto a vehicle, if the national road authorities wish to observe traffic flows, weather conditions etc., or where the police use CCTV against speeding offences or to observe a particular location for up to one month with grounded suspicion that a particular serious crime or accident will take place there) must make an application to the County Administrative Board. This application must contain detailed information about the planned system and surveillance area, as well as include agreement to surveillance by any employees affected. There is a general requirement to inform of the surveillance by signposting outside of the surveillance area. Installation may only be for crime prevention and detection reasons and the cameras must be fixed and may not have a zoom function. An application will be approved if the interest in the surveillance in question outweigh the individual's interest in not being surveilled in those particular circumstances. There are some circumstances, e.g. banks, where owners only have to inform of surveillance, i.e. where it is always considered acceptable. A representative of the area to be surveilled must be heard. An application can be granted in part or as a whole or only for a limited period of time. An appeal can be made against the Board's decision before an administrative court.

This sounds like a very privacy protecting system and comparatively, it certainly is. Actual practice has, however, been criticised because the County Administrative Boards are also required to supervise surveillance systems and have been found not to be doing so. For example, of an estimated 11 500 cameras, the Stockholm Board had only inspected 400 between 1998 and 2000. When the Swedish Helsinki Committee did a random survey of surveillance sights, they found many CCTV systems to be in breach of the law, in particular due to a lack of signposting, but also due to filming a larger or different area than was allowed. A complaint about this state of affairs to the Parliamentary Ombudsman resulted in a statement that one could not oblige the County Administrative Boards to perform their legal duties as long as they are financially incapable of doing so, which they claimed to be. A potentially attractive regulatory solution must of course be adequately financed (Hårdh, 2001).

It should be noted, however, that the requirement even for the police to have to apply for CCTV installations, may still be considered an effective control and is likely to enhance some of the beneficial effects found in Germany further. Also one should remember that in 2000 Sweden was estimated as having 30 000 CCTV cameras installed, with systems consisting of 3,2, cameras on average. A very different situation than in Britain. To enable a comparison; this would mean approximately one camera per 300 Swedish citizens, as opposed to roughly 1 per 14 British citizens.

The Netherlands

Another interesting case is that of the Netherlands where CCTV was first installed in the late 1990s. In the meantime, 80 of 550 municipalities have at least one installation. Public authorities must make an application to install to the *gemeenteraad* (municipal council) which is considered according to local needs. The view in the Netherlands was that international treaties, the Dutch constitution and the European Data Protection Directive provided a basis for a comprehensive regulatory scheme. This was regarded as requiring that surveillance must not be secret (unless required to be so for detection of a specific crime), be for a closely defined purpose to detect or prosecute defined crime or behaviour and it must be necessary for the owner to perform his or her duties. The duties of a private person are regarded as limited to his or her property. Public places are the responsibility of the mayor assisted by the police. As in Germany, less intrusive measures must be considered not only before installation but also periodically in reviewing CCTV surveillance. A complaint about unsuitable surveillance can be made to the local council and by civil writ to a court. In addition the Data Protection Board has a duty to supervise CCTV surveillance and has inspection powers. In order to consolidate these regulations, the Dutch government drew up laws specific to CCTV surveillance and has expressly forbidden the secret use of CCTV surveillance in public places (Offens, 2001).

The Spirit of the Laws in Europe

The law in France, Sweden and the Netherlands requires that attention be drawn to CCTV surveillance by signs placed outside of the surveillance area so that a person be made aware of

entering it. In Germany signposting significantly lowers the level of interference with constitutional rights CCTV surveillance is seen as causing. In the UK the advent of data protection legislation applicable to CCTV systems led to a proliferation of signage. Across Europe it would seem, there is agreement that those subjected to surveillance should be made aware of it. There can only really be one reason for this; where an area is generally under surveillance any person entering it having been informed of the surveillance implicitly agrees to it. The general stance would appear to be, if privacy rights are affected by surveillance at a general level (and it would appear the jury is still out on this one), implicit consent by the individual under surveillance negates any breach.

The legal concept of consent is, however, not a simple matter. There is agreement that to be valid, consent must be full and free (Alexander, 1996: 165). This indicates that the person giving consent must have the capacity to do so based upon sufficient information and must have a choice in doing so. There is plenty of controversy here. Given the doubts expressed in relation to CCTV's publicly propagated image as an effective crime prevention tool (see e.g.: Coleman and Norris 2000: 166) or that the general public know the workings of CCTV systems (see e.g.: Squires and Measor, 1996: 8), it is difficult to argue that consent is full. As the numbers of camera installations grow and especially when a surveillance density such as in the UK is reached, the issue of freedom rears its head. If I cannot purchase food without coming under surveillance, how can my consent to that surveillance be said to be free? If I can only avoid surveillance by leading a self-sufficient life on my own private property, surely my consent to surveillance cannot be considered to be free? Anything which forces me to make such a choice must surely be interfering with my human rights? The obvious response is of course that no ordinary reasonable man would respond in this way because it is disproportionate. One might even try to argue that there is no breach of any rights or that interference is only slight. In which case we return to the original question; why the requirement to signpost? Why is consent to the surveillance by those subjected to it regarded as at least desirable?

Furthermore given that the European Human Rights Court have refused to exclude very public spaces and actions from the realms of privacy law (Niemetz v Germany (1992) 16 EHRR 97), surely such a level of surveillance must affect my right to privacy if this is to afford any protection to social interaction even in public space?

It has been pointed out that the right to privacy as defined over time is of little help when it comes to regulating low level, general surveillance (see: Stalder, 2000) and indeed CCTV surveillance is a case in point. The weakness of focusing on privacy in a data protection sense becomes obvious. The German notions of spheres of privacy, which can also be seen in the European Court's doctrine (see: Taylor, 2002: 73-) are more helpful. And indeed the Federal Constitutional Courts judgement highlighting the right to informational self-determination, the so-called Volkszählungsurteil, focused not only on a right to determine what happens to one's data but also on the data subject's behaviour in response to the potential collection of data (BVerfGE 34, 238; see also: Bäuml, 2000: 3). Following this line of legal argument, an interference with the right to privacy can not only be caused by gathering data but by causing a person to adapt his or her behaviour. A focus on the reaction to surveillance means that privacy issues arise not

only where the person is in fact under surveillance but also where she or he believes s/he might be. Thus a dummy camera or even a sign indicating surveillance becomes privacy relevant.

There can be little doubt, that surveillance will be allowed in many cases. Deterring crime or using cameras to assist police work are doubtless legitimate aims necessary in a democratic society. However, whether this will remain the case once surveillance density passes a certain point, can be seen as a different matter. Where public space is increasingly subjected to surveillance, the nature and weight of the privacy rights of those within it must change if the notion of some kind of privacy protection in it is not to become a farce. This argument only becomes more weighty in interaction with issues of consent.

Issues of this kind are often not apparent when reading the letter of the law but the spirit of European and national law and jurisprudence provides some foundation for such argument. The increase of CCTV use in countries with a long-term constitutional commitment to privacy is likely to alter the terms of debate surrounding CCTV.

Providing Effective Legal Regulation

From the examples of legal regulation above, one can gain a good impression of what good regulation should provide for. The most important element would appear to be to provide an opportunity for serious debate. This can only be achieved where there is some legal requirement preventing those who wish to install CCTV from being able to do so without consultation. This is best served either by a need for a permit or a constitutionally anchored requirement for permissive legislation.

Whether it would be sensible and practicable to require police to apply for each individual system is bound to be controversial. The police have the legal duty and right to interfere even with the most important of human rights under certain circumstances so it may well be regarded as sufficient if, in relation to CCTV, these circumstances were defined by a democratically legitimated process. A definition of the parameters of CCTV and the acceptability of its use is, however, a if not the central pre-condition. This requires a debate of some sort as to what level of surveillance is acceptable altogether, what crimes CCTV can legitimately be used to fight, how etc. These then need to be moulded into clear laws, where necessary augmented by clear guidelines at a local level, including provisions (in so far as the law does not provide) for a review of each installation before it takes place, but also with mechanisms to review the need for CCTV surveillance on a regular basis. Given that the police are regarded as serving not their own but general public interest, this must be defined. Since the police are concerned with fighting crime and public order issues, it seems inappropriate to require or expect them to consider privacy and human rights issues and to get the balance right. This is a job for the legislature.

As far as private systems are concerned, the issues are quite different: the conflict is between many individuals privacy and usually the owner's interest in protecting his or her property. Whilst the legitimacy of protecting property needs to be considered, it would seem wrong to neglect the public interest element entirely, e.g. by only recognising a conflict where one individual complains

that his rights have been interfered with in a specific case. Simply balancing one individual's property rights with one other's privacy rights is only part of the issue. The property rights must be balanced against a larger number of individuals' privacy rights. This and effective legal regulation can only realistically be achieved by a permit system. Where, however, such a large number of applications to install cameras are made that one would consider an area as a whole to have too much CCTV, there must additionally be a possibility of rejection on these grounds, i.e. the ability to review each application to install a camera in a greater context of how widespread surveillance already is. A first come first serve basis for deciding who may install would, however, in itself be constitutionally problematic and so we return to issues of planning. Ultimately legal regulation in this field also requires the pre-condition that decisions have been made as to how far CCTV surveillance is acceptable.

Again installations should be subject to continual reviews as to their necessity and it must be possible to order a system to be dismantled.

Legal regulation on a micro-level is relatively straight forward and has been provided for in many European countries. However it is more difficult to see how the spirit of constitutional or human rights doctrine can be worked into this scheme, particularly as data protection law may prove to be inappropriate. There is nothing new in technology challenging the law. Nor in the modernisation of legal concepts to fit the times. If we are not only to witness an ever increasing proliferation of CCTV, the authorities permitting installation must not only have the right to dismantle on the grounds that the cameras are no longer necessary to achieve the aim for which they were installed but also because the area in which they are installed now has so many cameras that issues of consent and possibly the nature of the privacy rights of those under surveillance has changed. This of course requires the political will to define and confer such powers.

Concluding Comments

Many European states explicitly acknowledge that CCTV surveillance in public space creates a conflict with the right to privacy – and thus regulation is both necessary and desirable. A permit system appears to be fairly common for private users wishing to surveil a public space. The police are frequently granted a wider ambit in which to use CCTV surveillance but this does not necessarily mean that they feel free to install a large number of cameras. The law can effectively limit CCTV use. This can of course only be true where it is effectively enforced in word and spirit.

There can be no doubt that law will reflect public opinion and the pressure and desire politicians feel to 'do' something about crime. The wave of panic unleashed by the 11th of September 2001 saw several states in Germany broaden the permissive nature of their video surveillance police laws.

Whether regulation in the European sense, would have made any difference to the British development of CCTV use is a question which will always remain unanswered. Would any legal

argument have stood steady to the pressure perceived and generated after the Bulger case? It might have done. It could have given critics a better forum in which to argue their case. The fact is that legal regulation provides an opportunity. It provides a forum in which legitimate criticism and concern about CCTV in general, but also about use in a particular case, can be stated. Simply having to seriously address privacy issues when applying for permission to install CCTV may influence the way operators use the technology later. A legislative and, particularly, a licensing procedure (with the potential to reject an installation after taking a wide range of factors into consideration) can provide a bulwark against panic reactions. This of course all depends on there being persons willing to and in a position to present the arguments against CCTV. Therefore, a well established data protection network (such as that of state and Federal Data Protection Commissioners in Germany) will, for example, be necessary to provide the substance within a legal framework. But argument is also necessary beyond the issues of data protection.

Effective regulation can only be achieved if it is in place before CCTV has spread widely. In other words, it is more likely to be achieved in countries where there is fundamental recognition of privacy issues such as systems constitutionally requiring legislative authority before police can use them.

The efficacy of regulation will depend not only on its quality, but far more on a country's long term commitment to privacy and the institutional safeguards it has already installed to protect it. CCTV surveillance also raises problems as to the definition of privacy and will continue to be a legal challenge long after the keenest issues of regulation have been solved.

Additionally, real, perceived or generated pressures on crime policy, and how far they are allowed to erode legal safeguards, will be elemental. Ultimately, the question remains in how far a population will be prepared to choose freedom from surveillance over the security it believes CCTV can give it. Given the tendency in Europe to accept a great deal in order to combat crime, the apparent pressure for CCTV will have to be combated by reasoned argument. Above all this needs time and a forum which, as this paper argues, legal regulation can help to provide. Legal regulation is only a first step. But it may be a key one.

References

- Alexander, L. (1996) The Moral Magic of Consent (II), *Legal Theory*, 2: 165-174.
- Bäumler, H. (2000) Datenschutzrechtliche Grenzen der Videoüberwachung. In *Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern, Grenzen und Risiken der Videoüberwachung*, Schwerin
- Beulke, W. (2002) *Strafprozeßrecht*. 6th ed. Heidelberg: Müller
- Coleman, C. and C. Norris (2000) *Introducing Criminology*. Cullompton & Portland, Willan Publishing
- Gras, M. (2003) *Kriminalprävention durch Videoüberwachung - Gegenwart in Großbritannien, Zukunft in Deutschland?* Baden-Baden, Nomos.
- Hårdh, R. (2001) The Use of Public Video Surveillance in Sweden. Paper given at: Public Video Surveillance as a crime prevention instrument - a European Comparison. Göttingen, Germany 22-24 February.

- Henderson, R. (2001) Public Video Surveillance in the United Kingdom. Paper given at: Public Video Surveillance as a crime prevention instrument - a European Comparison. Göttingen, Germany 22-24 February.
- Holzer, K. and M. Krischer, (2000) Im Land der 1000 Augen, *Focus*, 33/2000: 51-.
- McCahill, M. and C. Norris, (2002) Urban Eye, Working Paper No. 6, CCTV in London, <http://www.urbaneve.net/results/results.htm>
- McCahill, M. and C. Norris (2004) From cameras to control rooms: The mediation of the image by CCTV operatives. Paper given at: CCTV and Social Control: The Politics and Practice of Video-surveillance - European and Global Perspectives, University of Sheffield, 8 -9 January.
- Norris, C. and G. Armstrong (1999) *The Maximum Surveillance Society. The Rise of CCTV*. Oxford, Berg.
- Ocqueteau, F. (2001) Video Surveillance in France – Regulation and Impact on Crime. Paper given at: Public Video Surveillance as a crime prevention instrument - a European Comparison. Göttingen, Germany 22-24 February.
- Offens, H. (2001) Public Video Surveillance in the Netherlands. Paper given at: Public Video Surveillance as a crime prevention instrument - a European Comparison. Göttingen, Germany 22-24 February.
- Sanders, A. and R. Young (2000) *Criminal Justice*. 2nd ed. London, Butterworths
- Simon, S. (200) Polizei will Videokameras mit Augenmaß einsetzen, *Süddeutsche Zeitung*, 9 February.
- Squires, P. and L. Measor (1996) Closed Circuit TV Surveillance and Crime Prevention in Brighton: half yearly report, Health and Social Policy Research Centre, Brighton
- Stalder, F. (2002) Opinion. Privacy is not the antidote to surveillance. *Surveillance & Society* 1(1): 120-
<http://www.surveillance-and-society.org/articles1/opinion.pdf>
- Taylor, N. (2002) State Surveillance and the Right to Privacy. *Surveillance & Society* 1(1): 66-
<http://www.surveillance-and-society.org/articles1/statesurv.pdf>
- Töpfer, E., Hempel, L. & Cameron, H. (2003) Urban Eye, Working Paper No. 8, Watching the Bear, <http://www.urbaneve.net/results/results.htm>
- Weichert, T. (2001) Öffentliche Videoüberwachung aus der Sicht der Europäischen Datenschutzrichtlinie und des deutschen Datenschutzrechts. Paper given at: Public Video Surveillance as a crime prevention instrument - a European Comparison. Göttingen, Germany 22-24 February.
- Weinbrenner, U. (2001) Videoüberwachung in Deutschland. Paper given at: Public Video Surveillance as a crime prevention instrument - a European Comparison. Göttingen, Germany 22-24 February.