Council of the
European Union

Brussels, 1 September 2014
(OR. en)

11746/1/08
REV 1 EXT 2

ENFOPOL 138

PARTIAL DECLASSIFICATION

of document:	11746/1/08 REV 1
dated:	15 October 2008
new status:	Public
Subject:	Close Circuit Television (CCTV) - Main findings of questionnaires

Delegations will find attached the partially declassified version of the above-mentioned document.

COUNCIL OF THE EUROPEAN UNION

Brussels, 15 October 2008

11746/1/08 REV 1

RESTREINT UE

ENFOPOL 138

NOTE

From :	General Secretariat
To :	Working Party on Terrorism
Subject :	Close Circuit Television (CCTV) - Main findings of questionnaires

I. Introduction

1. One of the most important contributions to the technical improvement of surveillance methods in recent years has been the development of CCTV.

   The contribution of CCTV to the fight against terrorism was sufficiently obvious in the aftermath of the London bombings in July 2005 as to make further demonstration unnecessary.

   CCTV is perfectly in keeping with the measures recommended by the EU Action Plan on combating terrorism[1], and in particular paragraph 2.6.1[2].

[1] 11882/1/06/REV 1 of 7 September 2006.

[2] 2.6.1. "Improve protection of other potential targets of terrorist attack, other than critical infrastructures (i.e. soft targets, crowded places, public transport) on the basis of relevant research".

2. At the Working Party on Terrorism meeting on 16 October 2006, the GSC and the Presidency proposed that a study be conducted on the development of CCTV in the European Union and its compatibility with respect for individual rights.

   The results of that study, as presented today, are based on the replies to two questionnaires, (15702/06 of 23 November 2006 and 2954/07 of 5 June 2007), circulated to the Member States after the Working Party on Terrorism meetings on 21 November 2006 and 4 July 2007.

   The replies to the first questionnaire[3] revealed that the situation varies considerably from one Member State to another. Bearing that in mind, a second, more specific and comprehensive questionnaire[4] was circulated.

3. The replies to the second questionnaire, which were more difficult to obtain because they fell within the remit of a variety of national authorities, required a series of consultations with Member States in order to remove all the ambiguities and avoid any risk of confusion. The consultations took place alongside the Working Party on Terrorism meetings between October 2007 and April 2008.

   The resulting combination of all the replies provides a fairly precise overview of this issue within the EU (cf. point II of this note). The replies from the various countries are contained in an addendum.

II. Best practices and recommendations

1. While some Member States make a clear distinction between the use of CCTV by the private sector and by public authorities, others adopt a less clear-cut approach to this fundamental difference.

[3] 15702/06 of 23 November 2006.
[4] 2954/07 of 5 June 2007.

2. Prior legal control and legal control "a posteriori" of CCTV use, whatever the authority with responsibility therefor (independent authority, law-enforcement agency, judicial authority, central, regional or local government) is a condition which is indispensable for the respect of individual freedoms. It is, furthermore, also a condition for the efficient use of CCTV in the fight against terrorism.

3. The difference in legal arrangements between areas open to the public and those accessible to employees only must be made more distinct.

- The public, who are warned in clear terms in accordance with statutory requirements, can always choose not to enter a shopping area placed under CCTV surveillance.
- This is not the case for staff working in these areas who, by definition, are under obligation to stay in them.
- Also, we must anticipate the not insignificant risk of intrusive technologies designed to combat terrorism being misused for staff management purposes or in the context of industrial disputes.
- If we failed to do so, a negative reaction from the public would be likely to interfere with public authority use of CCTV to protect European nationals against terrorism and crime.

4. Particular attention needs to be paid to the development of technical resources. Image transmission capacities already allow the images obtained to be transmitted to and processed at offshore centres. The centres involved could be undertakings' registered offices, or their establishments, in countries whose legislation provides fewer guarantees for individual freedoms.

   It would therefore be paradoxical for exchanges of CCTV images between Member States' official institutions in the context of the fight against terrorism to be more tightly controlled than exchanges of images of the same type between private individuals in the course of commercial activities (both between Member States and with third countries).

- Offshore processing - even within the EU - of CCTV images makes it more difficult, if not impossible, to provide information and legal remedies for the nationals of the countries in which they were collected.
- At the same time, transmission to third countries or even EU Member States, of images obtained by CCTV, in the context of the fight against terrorism or crime, is endowed with robust safeguards to protect individual rights.

- Offshore processing - even within the EU - of images obtained from CCTV operated by private individuals or companies must therefore be prohibited.

5. A common logo warning of the use of CCTV should be devised, to be used by all the Member States in order to give citizens the best possible protection.

6. Prohibit commercial use of images taken by CCTV in places open to the public (for example, sale of images to the media or market research).

7. Most Member States authorise the public authorities to gather evidence by means of covert CCTV, so as to establish before the courts that crimes have been committed or are in the process of being committed.

   In the answers to the questionnaires, Member States made few comments and referred to little in the way of good practice, whereas this means of evidence gathering is particularly important for the fight against terrorism. Given its intrusive aspect, it requires a high level of legal supervision, but it seems to be an indispensable weapon in the judicial arsenal.

   Covert CCTV may also make it easier for special forces to intervene, thus protecting the lives of any hostages and of criminals and members of those special forces.

8. Legal supervision of the use of CCTV is divided into two main types: prior control and control a posteriori. In each case, the questionnaires sought to determine the most appropriate procedures and authorities to guarantee both respect for individual freedoms and efficiency.

The original division of CCTV into categories (by employers inside premises closed to the public, by employers inside commercial premises open to the public, by public authorities for the purpose of prevention, by public authorities for "overt" crime detection and by public authorities for "covert" crime detection) has been reproduced within these two distinctions. We also find the same five categories in the survey on the choice of authority (independent authority, law-enforcement agency, judicial authority, central, regional or local government) responsible for legal supervision of CCTV.

It would be useful if this essential legal supervision could comply with certain broad guidelines. The more the use of CCTV is likely to be intrusive or prejudicial to civil liberties (e.g. when used by public authorities for "covert" crime detection)), the closer that supervision should be. The same applies when CCTV operation is not in the interests of the public as a whole, but only or mainly in the interests of the users (e.g. when used by employers inside premises closed to the public).

The broad guidelines for the legal supervision of CCTV use might be constructed around these two points. Once that general structure has been accepted, it should be possible to organise the choice of methods and authorities consistently, something which would be very difficult to do today, given the current state of legislation in the various countries.

9. Regarding a posteriori control over the use of CCTV by private individuals

- The three possibilities envisaged here (control by an independent authority, by a law-enforcement agency or by a judicial authority) do not set aside any legal proceedings by a national who considers his individual rights to have been infringed by a CCTV.
- Countries which stipulate no a posteriori control over the use of CCTV by a legal or natural person under private law are few and far between[5].

[5] **NOT DECLASSIFIED**

- The use of such intrusive methods by the private sector, more so than by a public authority for a purpose in the general interest, must be subject to strict a posteriori regulation.

10. Regarding a posteriori control over the use of CCTV by a public authority

- The three possibilities envisaged here (control by an independant authority, by a law-enforcement agency or by a judicial authority) do not set aside any legal proceedings by a national who considers his individual rights to have been infringed by a CCTV. These three possibilities are also envisaged outside situations where the public authority operating the CCTV puts the images before a court as evidence of a crime or offence.

- The control options at issue here therefore fall outside the scope both of any prior legal procedure and of the usual hierarchical supervision of the administration's activities.

- Countries which stipulate no a posteriori control over the use of CCTV by a public authority are few and far between[6].

11. Regarding persons authorised to view CCTV images:

⇨ Conclusions on access to CCTV images in the case of systems installed by private persons (by employers inside premises closed to the general public or by employers inside commercial or industrial premises - areas open to the public)

- Access by managers of the premises or individuals appointed by them does not raise any problems since this is the reason for the existence of these systems. However, it highlights the importance of prior scrutiny of the lawfulness of such systems .

[6] **NOT DECLASSIFIED**

- The differences in the treatment of systems installed by employers inside premises closed to the general public or by employers inside commercial or industrial premises - areas open to the public - are not significant.

- Most of the Member States allow police services access to this type of CCTV image.

- The possibilities of access available in this framework do not endanger individual liberties in any way as such access is justified by those services' administrative or judicial tasks.

- With regard to access by police services, the Belgian Law of 21 March 2007 is a perfect illustration of what is possible in this precise area.

- The same applies to Hungarian legislation with regard to the access granted to intelligence services (Act CXXV of 1995 on the national security services).

- **NOT DECLASSIFIED**

- **NOT DECLASSIFIED**

- With regard to access by other law-enforcement agencies, many examples of good practice were noted (see above). In certain cases, however, the possibility afforded does not seem to be linked to the imperatives of combating terrorism[7]. In other cases, by restricting access to police and intelligence services[8], a number of countries (**NOT DECLASSIFIED**) deprive themselves of the assistance that could be given by other departments such as the Tax and Customs Board, Border Guard, Unit for Combating Money Laundering and VIP Protection Department.

- Finally, it is particularly important for respecting individual liberties that each person may have access to the images on which he/she appears[9].

⇨ Conclusions on access to CCTV images in the case of systems installed by public authorities for the purpose of prevention

- Access by local or municipal authorities does not raise any problems in the cases mentioned in particular by **NOT DECLASSIFIED** legislation. However, these access authorisations highlight the importance of prior scrutiny of the lawfulness of these systems and the clearance of the persons who must implement them.

- Access by police forces is granted unanimously as it is the reason for the existence of such systems. It also highlights the importance of prior scrutiny of their lawfulness.

- Most Member States allow intelligence services access to this type of CCTV image. **NOT DECLASSIFIED**

7 **NOT DECLASSIFIED**
8 **NOT DECLASSIFIED**
9 **NOT DECLASSIFIED**

- With regard to access by other law-enforcement agencies, many examples of good practice were noted (see above). In certain cases, however, the possibility afforded does not seem to be linked to the imperatives of combating terrorism[10]. In other cases, by restricting access to police and intelligence services, a number of countries (**NOT DECLASSIFIED**) deprive themselves of the assistance that could be given by other departments such as the Tax and Customs Board, Border Guard, Unit for Combating Money Laundering and VIP Protection Department[11].

- Finally, it is particularly important for respecting individual liberties that each person may have access to the images on which he/she appears[12].

- Conclusions on access to CCTV images in the case of systems installed by public authorities for crime detection (overt and covert CCTV).

- Access by police forces is granted unanimously as it is the reason for the existence of such systems. However, it highlights the importance of prior scrutiny of the lawfulness of such systems.

- Most Member States allow intelligence services access to overt CCTV images. **NOT DECLASSIFIED**

- Access to covert CCTV images is also restricted by certain countries (**NOT DECLASSIFIED**)[13]. This restriction is also likely to hamper unnecessarily the fight against terrorism.

10 **NOT DECLASSIFIED**
11 **NOT DECLASSIFIED**
12 **NOT DECLASSIFIED**
13 **NOT DECLASSIFIED**

- **NOT DECLASSIFIED** are the only countries that grant access to commercial security agencies or private detectives if they are the official users of the CCTV or mandated by the official user or owner. As they are CCTV systems installed by a public authority in a judicial framework, this type of authorisation seems justifiable only if the commercial agencies are required by the judicial authority to give an expert opinion. The protection of individual liberties and their safeguards do not allow judicial tasks to be "privatised". The Member States have, moreover, taken this requirement into account by not allowing private or commercial companies any access in the case of covert CCTV.

- A majority of Member States allow police forces and/or intelligence services of third countries access to images produced by this type of CCTV.

  However, the ban "in principle" on access to such images by the intelligence services of partner countries (**NOT DECLASSIFIED** for overt CCTV and **NOT DECLASSIFIED** for covert CCTV)[14] is likely to hamper unnecessarily the combat against terrorism. A legal framework can probably be found to allow this type of cooperation while guaranteeing that individual liberties are protected.

- Finally, with regard to the other categories which may be authorised to view CCTV images, and failing fuller information, only the practices of **NOT DECLASSIFIED** [15] and **NOT DECLASSIFIED** seem to be justified.

17. Retention period

- A superficial, black-and-white approach might lead one to believe that the longer images are retained the more useful they may be for the fight against terrorism and the less individual freedoms are protected. That rudimentary analysis is contradicted by one essential fact: the capacity to transmit and analyse the images.

[14] **NOT DECLASSIFIED**
[15] **NOT DECLASSIFIED**

- Thus, too big a stock of outdated images, far from contributing to the fight against terrorism, is likely to hamper the work of the investigation services by leaving them saturated with largely irrelevant information. And, especially if the images come from CCTV installed by private individuals, over-long retention periods are likely to have the direct effect of pointlessly infringing individual freedoms.

- Everything is a question of proportion in this area, as is often the case. It is therefore particularly difficult to define best practice. Moreover, it must always be possible to update practice in line with technological developments.

  Harmonisation between Member States can be carried out only by taking account of special national characteristics. However, one of the rules that could be adopted is that the retention periods granted to private individuals may under no circumstances be equal to or longer than the shortest periods granted to the public authorities.

- Moreover, it emerged during the study that, although attention had been devoted only to the maximum period for retention of images, the minimum period should also be considered. Economic constraints linked to recording and conservation methods may in fact lead to a very rapid turnover of rerecordable or rewriteable media, without any concern for effectiveness. True, in that case, individual freedoms are perfectly protected but this is due only to the full effectiveness of the system.

- Thought should therefore be given to minimum as well as maximum retention periods.

⇨ Regarding periods for retention of CCTV images relating to systems installed by private individuals

- Period of useful retention of CCTV images relating to systems installed by employers inside premises closed to the general public:

By definition, staff working in such areas are obliged to remain there. Their individual rights must therefore be the subject of special protection as there is a significant risk of this intrusive technology aimed at combating terrorism being misused for staff management purposes or in the context of industrial disputes. This risk must therefore be anticipated by protective legislation.

The maximum period of one month (it is preferable that it be shorter than the retention period for CCTV images from systems installed by employers in commercial premises open to the public) therefore seems to be best practice.

This is the case today in a minority of countries: **NOT DECLASSIFIED**.

- Period of useful retention of CCTV images relating to systems installed by employers inside premises open to the public:

Unlike staff working in such areas who are, by definition, obliged to remain there, the public, who are warned in clear terms in accordance with statutory requirements, can always choose not to enter the commercial premises or public area placed under CCTV surveillance. Furthermore, the risk of attacks - hence the need for more protection - is greater in areas accessible to the public.
However, individual freedoms must be protected effectively. The maximum period of two months therefore seems to be a good measure.

A minority of countries currently apply a maximum image retention period of two months or less: **NOT DECLASSIFIED**.

- To date, few countries seem to have gauged the risks to which individual freedoms are exposed by excessively long retention of such images.

- Progress must be made in this connection since, in addition to infringing individual freedoms, excessive and poorly controlled use of CCTV systems by private individuals would be a political error[16] and would prove ineffective in combating terrorism.

[16] All the experts observe that sympathy with terrorism - which is often provoked by inappropriate repression - is more dangerous than terrorism itself because it offers it opportunities for recruitment and therefore expansion.

-

⇨ Regarding periods for retention of CCTV images relating to systems installed by public authorities for the purpose of prevention

- This is therefore monitoring of public thoroughfares (favourite areas for the commission of terrorist acts) in the public interest (prevention), by a public authority or in specific instances by bodies to which it has entrusted this task. Although this context provides certain safeguards for civil liberties, image retention must not, however, be unlimited.

- Moreover, taking account of the constraints of using and analysing such images, an excessive retention period would put individual freedoms at risk without bringing any notable benefits in combating terrorism.

- Harmonisation between Member States can be carried out only by taking account of special national characteristics. However, one of the rules that could be adopted is that the retention periods granted to public authorities may under no circumstances be shorter than those granted to private individuals.

- While a maximum of three months seems a good compromise, the question of a minimum retention period is important. Even though the issue is not within the scope of this study, a minimum of two weeks also seems a reasonable compromise.

⇨ Regarding retention periods for CCTV images in the case of systems installed by public authorities for crime detection (overt and covert CCTV). Countries which do not permit the use of covert CCTV systems (**NOT DECLASSIFIED**) are, of course, only partly concerned. The images referred to are those obtained from CCTV intended to record evidence which can be used in court. They are thus part of the judicial procedure.

Here there are two competing scenarios:

- either those images are regarded as being an integral part of the judicial procedure and therefore must be subject to the same judicial rules as other items of evidence in court. In that case, it is not necessary to set a specific maximum retention period.

- or those images, although an integral part of the judicial procedure, are regarded as constituting a serious threat to individual freedoms in view of the particularly intrusive manner in which they were obtained. In that case, consideration needs to be given to the maximum retention period for those images. We should not, however, lose sight of the fact that too short a period may pose a threat to the rights of defence. Hence retention until all avenues of appeal have been exhausted would appear to be the minimum. The following countries are currently in that position: **NOT DECLASSIFIED**.

18. Possibility of using CCTV images as evidence in court

- It is difficult to identify best practice on this point. Member States' legislation converges fairly closely and there are only a few marginal exceptions of a kind likely to interfere with the fight against terrorism without adding any substantial gain in the defence of individual freedoms.

- Almost all the Member States[17] consider that images obtained from CCTV may be used as evidence in court. They are governed either by the general rules on admissibility of evidence (**NOT DECLASSIFIED**) or, in the case of some Member States, by specific legislative provisions relating to CCTV (**NOT DECLASSIFIED**).

[17] **NOT DECLASSIFIED**

Sometimes the admissibility of CCTV footage as evidence is governed by a specific system (**NOT DECLASSIFIED**). It is in that connection that certain difficulties may arise. Those specific systems appear to make only a minor contribution to the defence of individual freedoms and may constitute a hindrance in the fight against terrorism.

19. Cooperation between police and intelligence services

In the final report on the evaluation of National Anti-Terrorist arrangements[18], the fourth recommendation under the need to improve the cooperation between services[19]. That recommendation also applies to the use of CCTV.

- Cooperation and exchanges between police services and intelligence services therefore need to be improved. They may be organised through legislative or regulatory provisions (**NOT DECLASSIFIED**) or they may be managed more informally on a case-by-case basis (**NOT DECLASSIFIED**).

- The provisions laid down by **NOT DECLASSIFIED** [20] are the only ones which do not seem of a kind to facilitate such cooperation and yet do not appear to offer any greater protection of individual rights.

20. International cooperation (Part VIII)

Cooperation between Member States is one of the keys to the fight against terrorism.

---

18 12168/05.

19 Recommendation 4: "Member States should consider putting in place national coordination arrangements to ensure strong inter-agency cooperation, and to ensure that all competent national authorities have access to the information and intelligence that are needed. One possibility would be for Member States to set up a national coordination arrangement for the day to day exchange of information in the field of prevention, disruption and investigation, involving all security and intelligence services and law-enforcement agencies engaged in counter-terrorism.
In addition to this, Member States are recommended to facilitate exchanges of staff with a view to enhancing coordination and cooperation, especially where formal structures are not available".

20 **NOT DECLASSIFIED**

- For CCTV exchanges between Member States, cooperation is organised on the basis of legislative or regulatory provisions (**NOT DECLASSIFIED**) or is managed informally on a case-by-case basis (**NOT DECLASSIFIED**).

- However, **NOT DECLASSIFIED** restrict such cooperation to judicial proceedings only[21], thus giving the defence of individual freedoms priority over the effectiveness of the fight against terrorism.

- **NOT DECLASSIFIED** does not have a legislative framework cooperation between member states on CCTV-issues

21. Improving the effectiveness of the fight against terrorism

21.1. Prior legal control

- Prior legal control, which operates mainly on the basis of a registration system, an authorisation system or a mixed system, undeniably constitutes a guarantee of individual rights. It is also likely to improve the effectiveness of the fight against terrorism.

- Prior legal control procedures may enable, or help, an authority to keep a centralised inventory of all existing CCTV in a given geographical area. That is an extremely useful possibility for the services both in terms of prevention - following a local threat - and in terms of ability to react after an attack has been committed[22].

[21] **NOT DECLASSIFIED**

[22] In this instance, the use of CCTV images may make it possible to interrupt a series of attacks from very early on.

- Without prior legal control, the services, working under pressure of a serious threat or facing a series of attacks, would be obliged to make an empirical inventory of CCTV in the geographical areas concerned. In addition to the risk of not arriving at an exhaustive inventory of potential sources of intelligence, which is inherent in operations carried out under pressure of events, a "heat of the moment" inventory of this kind takes a great deal of time and resources and occupies staff at a time when they are badly needed elsewhere.

➢ **Prior legal control, in the form of registration or authorisation, is therefore a measure to protect individual rights which also contributes to the effectiveness of the fight against terrorism.**[23]

21.2. Legal control a posteriori

- Contributes essentially to the defence of individual freedoms. Its impact on the effectiveness of the fight against terrorism is relatively neutral from the operational standpoint.

- However, by legitimising the use of CCTV and reassuring the public about the penalties which any abuses would trigger, such control makes the use of these intrusive devices more acceptable to the public.

- One of the most useful aspects of legal control a posteriori is that it prevents abuse of process or resources both by the public authorities and by private sector operators.

[23] A centralised inventory could be created on the national or regional level. For operational purposes, confidentiality of the inventory needs to be ensured. The important investment in legal and administrative terms to create a system of registration or authorization also have to be taken into account.

➢ **Legal control a posteriori protects individual rights without interfering with the effectiveness of the fight against terrorism, and even makes it possible to legitimise the intrusive tools used in that connection.**

21.3 Use of images

This aspect of CCTV can be divided into two main questions:

- Who is authorised to view the images?
- How long can the images be stored?

21.3.1. Access to images

- Prior legal control of CCTV, as already stated, makes it possible to make an exhaustive map of CCTV over a given geographical area. That means that six categories of people are likely to have access to the various types of CCTV in service in that zone:
  - managers of the premises or individuals appointed by them
  - police forces
  - intelligence services
  - other law-enforcement agencies
  - commercial security agencies or private detectives if they are the official users of the CCTV or mandated by the official user or owner
  - other categories.

- While it is logical that those who have installed CCTV or their employees should have access to the images recorded, the effectiveness of the fight against terrorism means that the police services[24]and the intelligence services[25] must be able to access the product of all the devices (affirmative answers to questions 1.2, 1.3, 2.2, 2.3, 3.2, 3.3, 4.1, 4.2, 5.1 and 5.2 of Part IV of the second questionnaire).

- Nevertheless, access by private individuals to the images produced by CCTV installed by the public authorities for the purpose of prevention or to obtain evidence[26] (affirmative answers to questions 3.5, 4.4 and 5.4) offers no significant added value for the fight against terrorism. That possibility might instead serve to discredit the use of intrusive detection tools such as CCTV by the public authorities.

➢ **Defining the abuse of images from CCTV installed by the public authorities for the purpose of prevention or to obtain evidence as a specific criminal offence may be a useful way of defending individual freedoms without interfering with the effectiveness of the fight against terrorism.**

21.3.2. Deadlines for retention of images:

A superficial, black-and-white approach might lead one to believe that the longer images are retained the more useful they may be for the fight against terrorism and the less individual freedoms are protected. That rudimentary analysis is contradicted by one essential fact: the capacity to transmit and analyse the images.

- Thus, too big a stock of outdated images, far from contributing to the fight against terrorism, is likely to hamper the work of the investigation services by leaving them saturated with largely irrelevant information. And, especially if the images come from CCTV installed by private individuals, over-long retention periods are likely to have the direct effect of pointlessly infringing individual freedoms.

[24] This is the case in most countries, except in certain cases in: **NOT DECLASSIFIED**.
[25] This is the case in most countries, except in certain cases in: **NOT DECLASSIFIED**.
[26] This is the case in certain countries: **NOT DECLASSIFIED**.

-

➢ **A time-limit for the retention of CCTV images guarantees individual freedoms and is at the same time a factor in the effectiveness of the fight against terrorism.**

22. Quantitative inventory

- One of the consequences of the absence of prior legal control is that it is impossible to estimate the exact number of devices in service in the EU Member States, whether in public or in private places.

- It is thus also impossible to estimate their levels of performance, which may range from the most obsolete technology to state-of-the-art innovations.

22.2. Operational inventory

- The contribution of CCTV to the fight against terrorism was sufficiently obvious in the aftermath of the London bombings in July 2005 as to make further demonstration unnecessary.

- It is, however, necessary to point out that CCTV contributes more to identifying the perpetrators of an attack committed than to preventing the first attack in a series[27]. Yet by making it possible to dismantle networks quickly, such devices may reduce the risk of a wave of attacks. The efficiency of the authorities is thus demonstrated and prevents panic and fear among the population, which is the main object of terrorist action targeting the EU.

- To achieve such results, certain basic principles need to be respected:

[27] Except where suspect behaviour is identified when terrorists are staking out the location.

- CCTV is one element in the arsenal for fighting terrorism, a potentially effective element but one which cannot be viewed independently of the rest of the tools available. Its development must therefore be integrated into an overall strategy on fighting terrorism.

- **With regard to the preventive dimension in particular**

  - It must be possible to view (and thus to transmit) the images recorded in a period as close to real time as possible.
  - Transmission must be to the relevant operational service.
  - That service must be able to intervene without delay.

- **With regard to the repressive dimension in particular**

  - It is necessary to have a minimum of spatial continuity (between devices). That applies when a person's or, more specifically, a vehicle's movements need to be followed. It requires both an inventory of devices[28] and consideration and consultation between the various public authorities and with private individuals[29].

- **More generally,**

  - It is imperative that the various operators planning to install CCTV take account of the needs of the internal security forces. That means establishing national minimum standards or, better still, European minimum standards for CCTV. These minimum standards should be of functional nature, not technical. To allow large-scale exploitation of data in the event of an attack, the systems put in place by the various operators must offer the following five functions:

  - ability to protect requisitioned data from erasure while continuing to record.

[28] Making it possible to map the zones covered in real time.
[29] For instance in the immediate vicinity of public transport arrival and departure points.

- ability to provide the authorities (via the prior legal control procedure, for instance) with a map showing the location of the cameras and the video area monitored. Dematerialisation of recording requests and authorisation applications should make it easier to meet that condition, which should also be accompanied by an obligation to update.

- setting minimum periods for data retention.

- capacity to export swiftly large quantities of data which may be useful to the enquiry without blocking the operation of the system[30].

- capacity to transmit images of interest to the security services to their crisis centres in real time.

➢ **It emerges from these comments that there is a need to use all resources to facilitate convergence, interoperability and in certain cases sharing of the means offered by all devices.**
Far from being a threat to the defence of individual freedoms, that would also make it possible to facilitate and systematise both prior and a posteriori control of those devices.

➢ **Moreover, the security forces must direct their efforts to the capacity to receive and exploit good-quality images. They must also be involved in the design, and even in the use, of the systems put in place by the various players.**
That would make it possible to limit the installation of their own resources and so keep down costs to the public purse.

22.3. Financial balance

The data set out below are far from exhaustive, nor are they simply an account of the very different realities in the 27 Member States, but they are intended essentially as food for thought.

[30] For example, it currently takes a day to copy 30 000 hours of recording (equivalent to the images recorded by 427 cameras over 72 hours).

The investment cost per camera can generally be estimated at between EUR 30 000 and 70 000 for public thoroughfare surveillance in an urban area[31].
These are very high costs. If CCTV - as seems very likely- is to become an integral part of the security arsenal, it will be necessary either to reduce the cost or (where possible) to share CCTV activity over several beneficiaries.

It is also worth considering the possibility of bringing down the cost of the camera connection at the heart of the network. Various technical connection solutions over a very wide range of costs could be envisaged via:

- optic fibre
- ADSL
- power liner carrier
- WIMAX
- GSM/GPRS

Depending on the type of connection chosen, another item to be taken into account is the cost of camera consultation time[32]. Operational exploitation costs also need to be added (data exploitation team).

Technology developments also have a real, though limited, impact on the cost of equipment. They may result in greater efficiency and a reduction in the cost of the overall system. The top item of cost is not the technology but civil engineering and camera connection costs.

The impact of the falling cost of cameras, bandwidth (improved compression methods) and recording/storage devices will be offset by the increase in the quality of equipment (high-definition digital) and the inherent technical requirements and constraints.

[31] On the basis of a set of 1000 cameras allowing images to be sent and viewed.
[32] For cameras connected via WIMAX, GSM or GPRS, the cost increases with camera consultation time.

- **The convergence and interoperability of all the devices would reduce costs and at the same time facilitate the defence of individual freedoms. Controls would thus be easier and less costly and so could be more numerous and more detailed.**

_____