2014 Hawaii University International Conferences
Science, Technology, Engineering, Math & Education
June 16, 17, & 18 2014
Ala Moana Hotel, Honolulu, Hawaii

Smart Technologies for E-Surveillance: Some Evident Benefits But Also Many Problems Regarding Protection of Personal Data and Disrespect for Fundamental Human Rights

Soltes, Dusan
Faculty of Management
Comenius University,
Bratislava, Slovakia.

Soltes, Dusan
Faculty of Management
Comenius University,
Bratislava, Slovakia.

Smart Technologies for E-Surveillance: Some Evident Benefits But Also Many Problems Regarding Protection of Personal Data and Disrespect for Fundamental Human Rights.

The paper has been dealing with some issues regarding modern smart e-surveillance regarding also the problems of protection of personal data and fundamental human rights

SMART TECHNOLOGIES FOR E-SURVEILLANCE: SOME EVIDENT BENEFITS BUT ALSO MANY PROBLEMS REGARDING PROTECTION OF PERSONAL DATA AND DISRESPECT FOR FUNDAMENTAL HUMAN RIGHTS IN GENERAL

Dusan Soltes
Faculty of Management, Comenius University,
Odbojarov 10, 831 01 Bratislava
Slovakia

Abstract

The paper is dealing with application of the above smart technologies in the area of e-Surveillance and in this respect is presenting the results of our ongoing research under the European Union funded project EU/7FP/Sec./SMART. The more information on this and other of our related EU funded projects viz. CONSENT and RESPECT can be found at our web: //erdc.fm.uniba.sk.The main so far achieved results from our above ongoing research are the following ones. It has been evident that an application of the latest smart ICT in e-surveillance have had a very positive impact on achieving more secure and safe environment not only in the so-called cyberspace but also in many application areas of these ICT. The first such area of a very positive impact has been achieved in the area of the contemporary system of the border controls of the so-called Schengen external borders of the EU that have been protected by the several mutually linked and integrated systems of e-surveillance viz. CCTV cameras, automated border checks, automated targeting systems, biometric matching systems, etc. Very similar systems have been used for the protection of the external borders also in case of all airports in combination with general security controls. The other most widely utilized application areas of these smart ICT have been various areas of public life, various cultural and other social events in the forms of so-called crowd controlling, the same also regarding phone and Internet communications, financial transactions, etc.

Key Words:

e-surveillance, smart technology, monitoring, crowd controlling, CCTV. biometric matching systems, ground sensors, financial transactions.

1.Introduction

It already an integral part of our daily life that practically all the time around all of our activites have been under the permanent 24 hrs. surveillance. I tis just enough if one has been using any of the current achievements in the consumer electronics and using such today its most common applications like e.g. a mobile phone, various banking debit or credit cards, Internet, social networks, GPS systém for orientation while driving a car, visiting any of the public palces, sport or cultural or any other public events, but even such electronic systems lke electronic security systems in peoples‘ homes, etc. and the whole life has been under the permanent all the day 24 hrs. uninterrupted surveillance. survillncesss

In many practical situations it brings to people a lot of potential benefits but on the other hand there is also a growing number of various cases of misuses of such data collected about us by those all various types of e-monitoring, surveillance and recording systems.In the next parts of this paper we will try at least very briefly state and analyse some of the most typical positive but also negative aspects of such permanenet monitoring and surveillance system.

2. The two of the most widely applied areas of smart technologies in e-surveillance

Unfortunately the limited scope and size of this paper does not allow us to deal with all the potential benefits of application of the smart ITC e-surveyllance systems and their utilization hence we focus further at least on two of the most widely and important ones as follows:

The e-surveillance on the external borders of the EU

The e-surveillance by the CCTV cameras and by some related e-surveillance smart technologies

2.1 E-surveillance on the external borders of the EU

It is quite clear that in spite of some evident negative aspects of application of the latest e-surveillance systems there are existing many positives in this respect. In the following parts of this chapter we will try to present some of the most evident benefits achieved in the application of the smart e-surveillance applications that have become an integral part of our daily life. In this respect according to our ongoing reasearch under the particular EU funded SMART Project has been the e-surveillance of the so-called schengen border systém that has consisted of the following main features.

The entire schengen external border of the EU has been protected by an integrated systém that consists of several subsystems that are to the large extent relying also on the application of the smart ICT technonologies:

- ABC - Automated Border Checks that have been applied on all border crossing of the Schengen border systém. The most important advantage of the entire systém in this respect has been that the results of all these checkings have been becoming a part of the schengen information systém (SIS) so any negative aspects in this respect have automatically become a part of the entire systém so there is not left any space for any calculations and/or speculations to use some other entry point to the EU through the checking points in other EU member state and its border control this integrated SIS has been linking all border controls and checkingpoints of the Schengen border what altogether makes the entire systém more consitant and reliable
- ATS The second integral part on the external border of the EU has been an Automated Targeting Systém that is serving as an automatic tool for all persons who arare passing through the particular cheking points. On the basis of the particular personal data collected from the passport as well as from other related sources like e.g. from the recordings of the previous visits it is possible to create a relatively complex and comprehensive „picture“ and/or description of every person and thus to categorize that person. On the basis of that such a person in some cases could be placed into some of the risk categories like e.g. terrorists, smugglers, etc. For example due to the relatively big difference in the price but also salaries levels between the Slovak republic and Ukraine that are sharing the common Shengen border they are creating among others also a very attractive and profitable smuggling business especially regarding car fuels, alcoholic beverages, cigarettes, etc. hence thanks to this systém i tis very easy now to identify, record and then taking any actions against those „travellers“ who are able to cross the border even several times during one day as in case of visa regimes there is existing an assymetric systém i.e. the Slovak citizens do not need visas for entering Ukraine while on opposite te citizens of Ukraine need so-called schengen visas. Thua it used to be quite a wide spreaded business for Slovak „tourists“ to cross even several times a day the border in order to import those commodities and goods we have mentioned above and of course also many more of them. But with introduction and

implementation of the schengen border control systém it meant also the end of these kind of widely used „tourism“ between both countries. After several border crossings the systém has been automatically reporting that this or other person has been too active in the border crossings irrespective if they were conducted only through the Slovak – ukrainian border or some of them tried to minimaize their border crossing in such a way they have been trying to cross the border to Ukraine via neighboring Poland or Hungary

- AVT – Automated Vehicle Tracking is an another smart technology being applied on the Schengen border controls. It substance is based on the utilization of a small electronic unit – chip that has been stowed discreetly somewhere in the bowels of a vehicle. Then through the GPS satellites i tis possible to to monitor a movement of such vehicle even in case if that vehicle has managed to cross the border without any evident suspicious activites and/or features. The advantage of this smart systém has been that the systém is not directly limited just by the area of the border control points but i tis possible to trace such a vehicle also in the wider and more distant areas and/or territories from the biorder area.. In this respect has been already possible to detect and také action against such e.g. smaggling activites where the vehicle has crossed border chceks without any problems but then further from the boreder it has been recorded that the vehicle has been ding some suspicious movements and/or direction in their further moving in the inland of the country being quite far from the particular border controls, etc. Tjhis systém is quite efficinetly applied against such vehicles that have been involved not directly in smuggling only but also in other criminal activites like e.g. bin the case of bogus exports that are used for avoiding the tax duties regarding VAT, etc. It has been quite a common practice that the goods have been declared like destined for an export and then after crossing the border the same vehicle has returned back but with the same marchendise that was as being „exported“ so in such a case having possibility for the return of the VAT as well as to sell the particular merchendise again back in the home country, etc.

- ANPR – Automated Number Plate Reader that is not yet applied on the schengen border checking points e.g. in the Slovak republic but in the very near future i tis supposed to be implemented there. The main advantage is that in difference to the above AVT that requires some kind of special and secret and confidential activites linked to the placement of the particular chips on the vehicle this systém is automatically recording the id number of every vehicle crosing the border chceking points. And again as in the case of the above ABC or ATS systems i tis possible also in this case to achieve the same targeting of the vehicle as in previous cases it was with the persons crossing the bored too frequently or with some suspicious activites like smuggling some goods or commodities, etc.

- UGS – Unattended ground sensors has been also applied on the external borders within the Schengen border. I tis an other smart ICT based technology that is helping in the border areas especially in the harsh mountaineous and for access or movements by vehicles difficult border areas and thus being too difficult for any other possible border control systems. The UGS has been based on the combination of various sensor modalities like e.g. seismic, acoustic, magnetic, pyro=electric, transducers, daylight imageers and/or passive infrared imagers that are enabling to detect and record any presence or ovements of persons, vehicles or other moving objects in the particular area of surveillance. In such a case that any of such objects and/or movements have been detected in the particular area, the particular activites have been reported via radio-frequency or satellite communications to remote PED – Processing, Expolitation and Dissemination stations and the necessary action then by a suitable means and ways e.g by helicopters are carried out directly on the spot and in the real time exactly in the place and location when such an unauthoriszed aktivity has taken place and/or was carried out.

- CCTV – Of course as anywhere also in the border controls are widely used CCTV camers as one of the most efficient and also not so expensive smart ICT based technolgies. The problém is like in all application areas for the CCTV that the particular systém is meeting some of its most desired objectives i.e. such as:
    - The camers have to enable not only to capture the particular object or person but also to enable the necessary recognition either face or number plate and/or any other relevant features of the particular object
    - The camera has to be properly focused or be able to folow the particular object of surveillance
    - The camera has to have a proper angle of surveillance and monitoring i.e. it has to be properly installed in order not to be obscured by some other objects or not being too low and/or too high focused

- One of the most important aspects for efficiency of CCTV cameras is that the entire automated systém is properly and manned and operated by an experienced staff that is trained properly in order be able to immediately utilize and také action on the bases of the recorded images in the real time and not only ex post e..g. some time after the particular images have been recorded when already the momentum of an active and immediate action has already been substantially lower than i fit is carried out on the spot in the real tiemof the particular action, movemnet themselves.

In addition to this most common and also practically applied ICT based smart e-surveuillance technologies there has already been existing a relatively long list of this kind of smart e-surveillance systéms but that have not yet been applied on the external borders of the Schengen border systém we have been researching and analysing like e.g.:

- BMS – a computerized Bio Metric Systém using the comparison of the particualr biometric data from the passport, ID cards etc. with those collected on the spot from the particualr person and also with those stored already in the particular data base
- AFR - again a computerized Automated facial recognition that is able to identify a person on the bases of her/his face and its comparison with its digital image again in a passport, ID card and/or data base from the preious border crossings and controls
- AVR – a Computerized Automated Voice Recognition that is able to make voice recognition through voice as recorded by micropones or other simile equipment e.g. mobile phones that are considered as being able to recording voice and/or any other simile signals even in case if the mobile phoen has been switched off chat is sometimes quite important and benefitial in the border or customs controls areas
- AXRS – Automated X-ray Scanners i.e. devices that are able automatically detect any illicit substances if being imide the body. This e-surveillance technology has been already experimentally teste dat some airports but has been received by a geerally widely negative reactions from x-rayed people as t is too invasive and of course also represnts also some health risks. But it looks like that sooner or later it will become one of the e-surveillance systems especially at airports
- RDD – a Radio Detection Device thatis able to detect automatically a presence of any radioactive substances that are from time to time also a part of the smuggling activites at border crossings, etc.
- GDD – is a simile device like RDD just the object of detection has been gunshot that could be automatically detected on the base sof sound sensors
- Thermo-Camera – it is an automated camera that is able to identify any human or other objels that are emitting any temperture higher than the serounding evironment. Thanks to its functions i tis one of the very promising e-surveillance device that especially at the borders could find a very wide and efficient application
- AMPT - Autmated Mobile Phone Tracing i sone of the most promising e-surveillance systems as more and more people have been using this moder „communication obsession“. It has been based on the same basis as the mobile phones have been functioning i.e. using multilateration of radio signals via GPS and thus enabling not only the particular communication but also localization where from the particular mobile phone has been locate.

In conclusion to this part on e-surveillance technologies being already applied at the border controlling or will be sooner or later applied we could state that allthese latest automated e-surveillance systém cannot protect borders absolutely perfectly.They all are contributing very positively to border protection and security but there is a certain paradox existing not only in case of the EU Schengen border but also in case of other otherwise very much protected borders like between Mexico and the USA, between Palestine territories and Israel, etc. While this e-surveillace is really protecting the particular bordersvery efficiently, there are always ways and means that are almost negating these benefits. For example in case of the schengen border i tis really difficult to become a part of that area mainly due to the problems of all these required aspects of border controls and protection like e.g. itis still in case of Romania or Bulgaria whose applications to join Schengen has been already several times rejected on the grounds that they arenot yet ready to protect that border as required although the numbers of illegal entrants are relativem very low e.g.in comparison with the Schengen area on the southern borders of the EU i.e. its Medditterean shores that have been the main entrnaces for boat peole illegally entering the Schengen area in the so-called PIGS states i.e. Portugal, Italy, Greece and Spain but also Malta and Cyprus thus making of the particular Schengen border nothing more than „ementál chease“ i.e. chease being famous for its big and many holes! And in order not to blame only this southern border, many „holes“ in the Schengen borders are various underground tunnels that are then and again discovered anywhere where there is existing any possible extra profits being large than potential risks, etc.

In view of ths we could conclud this part by stating that even the most sofisticated e-surveillace systems cannot be efficient if they are not supported also the whole range of legal, political, organizational, staffingand other supporting measures and activities. .

2.2 Smart e-surveillance by the CCTV cameras and some other related e-surveillance smart technologies

The second selected application area of ICT based e-surveillace systems but also one of the most contravrsial once has been the application and probably the most widely applied one i.e. the CCTV cameras systems that have alreadybeen almou permanently monitoring not only the public spaces but also priváte ones. In the following part of this paper we are at least briefly characterizing at some of the most typice features of these e-surveillance smart systems:

Our survey and research in general in this respect as carried out under the EU/7FP/SMART and RESPECT projects has clearly demonstrated that the video camera surveillance has become an integral part of our daily lives practically in all its parts. It could be stated in this connection that practically for the whole 24 hour long day period, people have been monitored and recorded by the various kinds of surveillance CCTV cameras systems:

in their houses and their residences during the nights as well as in connection with their leaving and/or arriving from/to their houses, etc. It is just enough to have installed any kind of security system linked directly to some security service and it is then immediately clear when one is switching on or off that security system including its cameras and thus also indirectly reporting when one is home or leaving or arriving, etc.

then during their transport they have been monitored by the camera system currently practically being installed in all means of the public transport, on stations, platforms, etc. Even of course also utilization of own cars has not been totally free from all various kinds of camera or various other e-surveillance systems either on almost every road/street crossings, highways, parking lots, petrol stations, rest places, etc. and of course not to mention if drivers have been using the GPS or any other such devices including hands-free mobile phone, etc. All of them have been monitoring and recording any movements of any car, etc.

in connection with transport it has to be mentioned especially the air but also ship transport that is not only related to extra controls and e-surveillance but we could even say the passengers are directly forced into literally enforced body controls not only by various hands-on or e-monitoring gates but even to the hands touching by the security staff. One has to admit that in many cases for unknown reasons sometimes they prefer their hands for direct touching bodies of passengers than to use those hands-on devices. One then cannot help not to think that many members of that security staff are doing these jobs exactly for the same reasons like various pedophiles are usually working in various areas that are for children e.g.in scout clubs, sport clubs, kids dancing clubs, religious youth clubs, etc.

people during their shopping as well as all their other daily common duties, activities, movements and visits at post offices, banks, various other offices and places of the public services have permanently been monitored and recorded by various camera surveillance systems and in addition of course by various other e-surveillance systems especially if using e.g. credit/debit cards, various customers/clients benefit cards, ID cards, etc.

the same being the case at the people’s working places where also in the most such places there have already been installed various types of CCTV camera system especially and at least at entrances and exit gates, activities areas, parking lots, canteens, etc. as well as again also in connection again with various entry ID cards, passwords, biometric identifications, etc.

any visits of cultural, social and especially sport events where it is possible to expect some higher number of visitors or attendees have been nowadays mandatory under the surveillance by various camera systems.

Without these CCTV camera installations e.g. some sport or other cultural or social events cannot be even organized at all

even during an ordinary strolling, walking along the city streets, parks and/or playing at children playgrounds and being at other places of otherwise commonly free access have been nowadays under the permanent surveillance by various camera or other e-surveillance systems

all galleries, exhibitions but also hotels, restaurants and other similar places of public attendance and visits have been as well under the permanent camera surveillance

especially carefully and under the permanent e-surveillance have been all transport related facilities where as a rule a lot of people have been moving around like it is in the case of airports, bus and train stations, etc. but also again the particular public parking lots, etc.

However, one of the biggest shortcomings of ever growing application areas of all the CCTV and related e-surveillance smart technologies have been the attitude of all their operators towards the objects of their smart e-surveillance i.e. towards the citizens as the objects of all their particular activities. From our research we have found out that if something happens to people like e.g. being customers, clients, etc. and they become victims of some robbery, physical or psychical abuse and they would like to use the particular camera recording to help them in identifying what and how those abuses have happened they as a rule are rejected as the particular recording are not available to them as the objects of that e-surveillance but only for the owners or security staff of the particular company or institution, etc. The only way how to get such help through particular recording s is through approaching the police but in most cases due to the character of such incident it is viewed by police as a minor case and not belonging under their competence. That all in case of victims that are involuntary without their consent recorded and stored, etc. Although the particular legislation on the protection of personal data clearly states that the owner of that data i.e. that person has a primary right to handle own personal data and without his/her consent nobody has the right to handle such data without that.

In conclusion to this part on the e-surveillance by various CCTV cameras and related e-surveillance smart technologies we could state that people have been not only monitored by these various cameras but their faces, bodies, movements, activities sometimes even in the most intimate situations have also been recorded and as such being available for any subsequent analyses, evaluation, searching and of course unfortunately also for a still growing misuse of such recordings for various and not only positive activities regarding the particular persons, etc. Although, the legislation e.g. on the Fundamental human rights of the citizens of the EU is strictly stating that such recorded data can be stored and used only for a time period being absolutely necessary for the reason that such data have been recorded, the practice is completely different. It is quite a common practice that all these various camera recordings are stored for an unlimited time period together also with various other similarly recorded data like e.g.it is in case of telephone conversations especially those through mobile phones but also by various other communication devices related e.g. to social networks, Internet, e-mail communications, etc. And there are almost unlimited numbers of examples how these fundamental human rights have been violated by many stake holder, operators, various security services but also police and governmental services, etc. It is a practical experience of also this author that coming back to certain hotels after several months or even after a year, at the reception he was often told that his name is enough for identification as all other necessary data the hotel has kept in its database of guests from previous visits?!

In view of this we could only state again that all this modern e-surveillance not only by CCTV cameras we have been dealing with in this part, are in a strict violation of any fundamental human rights on protection of personal data, on the protection of integrity of personality, its dignity, etc. However, the main paradox of all these e-surveillance by the CCTV cameras and related other smart e-surveillance technologies has been the fact that the more of these camera installations have been existing it has not at all been accompanied by the more security in such surveillance areas. For example the statistics on the CCTV camera installations in all the banks in the Slovak Republic for last five years are clearly demonstrating that the more camera systems installations have not led towards less bank robberies but on the contrary there has been even some growth not only in the number of such bank robberies but also there has been a growing number of unresolved cases in that respect.. The only benefit of all this by the law mandatory installations has been that in such a case that camera system has been in place, the particular robbed banks can be compensated through their insurance policies as without such policies that is impossible.

3. Main conclusions and recommendations

In conclusion we would like to summarize at least very briefly some main findings of our ongoing research under the EU/7FP/SMART, CONSENT, RESPECT projects. One of the main findings in this respect has been the fact that the modern life is fully and permanently monitored and under a surveillance by the latest e-surveillance technologies like we have some of them identified and described in the previous parts of this paper regarding e-surveillance on the EU Schengen borders and in connection with applications of the CCTV systems

This e-surveillance has definitely brought to some application areas more security, more responsible behavior of people especially due to the fact that if people are aware of being monitored and under a permanent surveillance but on the other hands there are still many questions regarding the potential misuse of such data from these sources

On the other hand all these surveillance has led to a wide spread disrespect towards some of the fundamental human rights especially regarding human dignity, protection of personal data, integrity of personality, protection against any kind of discrimination, right to privacy, etc. Some of these e-surveillance and accompanying activities by the security staff especially at airports could be characterized as totally unacceptable discrimination of people as e.g. in many airports among others are also warnings that any conversation with security staff during controls are strictly prohibited and punishable by law and that all for our money we pay for these “our” security through enormously expensive air tickets. It is then no surprise that some of security staff at the airports are behaving towards passengers i.e. their sponsors and so to say indirectly their employers so arrogantly that it is in breach of not only some fundamental human rights on equality before the law but it is directly humiliation of people in general.

For the future it will be necessary also on the basis of our ongoing research under the EU CONSENT, SMART and RESPECT projects to achieve a more balanced relation between three important concepts of the contemporary life i.e.

- between threads of terrorism or any other criminal activity

- application of the latest e-surveillance technologies

- and last but not least with fundamental human rights, peoples dignity in order they would not be victims of various

bureaucratic or even deviants’ sexually motivated misconducts.

4. References

.

[1] J. Cannataci et al: EU/FP7-SSH-2009-A CONSENT – Collaborative project (small or medium scale focused project on Consumer sentiments regarding privacy on user generated kontent (UGC) services in digital economy, Annex I – Description of Work, University of Central Lanceashire, Preston, UK September 2009

[2]Cannataci, J. et al: EU/FP7/SSH-2009-A CONSENT Project, WP3 – Mapping Privacy Settings, D 3.1. Survey Report, University of Malta, La Valetta, October 2010

[3]//www.smart.law.muni.cz

[4] D. Soltes at al: EU/FP7/SMART Project, Work Packages WP2-8 with thé results as achieved in thé Slovak Republic gradually in years 2011-13, FM UK Bratislava, March 2013

[5] D. Soltes at al: EU/FP7-SMART Project, Work Package 10 – The Group Discussions for Slovakia, Bratislava, April 2013

[6] Fundamental Human Rights of the Citizen of the EU, European Commission Press, Brussels 2 010