# Pros & Cons of Smart ICT in Some Governmental Applications

**Dusan SOLTES**
**Faculty of Management, Comenius University in Bratislava**
**Bratislava, 820 05, Slovakia**

## ABSTRACT

The paper is dealing and presenting results of our ongoing research under the framework of our EU/7FP/Sec./SMART that has been focus on application of the latest smart ICT in five selected problem areas viz. e-Government, Border control, Counter-terrorism, Consumer protection and Smart surveillance in cyberspace. At this time the most important problem areas among these five selected application areas have been the protection of the protection of the Schengen external borders of the EU and closely related problems of the fight against terrorism. In difference to the existing critical situation with the illegal immigration and thus also the growing thread of terrorism in the EU, the paper is clearly demonstrating that the existing system of application and proper utilization of the latest smart ICT in addition to be supported by the strong and demanding EU "aquis communautaire" for the Schengen external border system is able fully and completely protect the territory of the EU against any threads of terrorism. In the following parts of this paper we are presenting some more details on the issues of the smart ICT not only in the case of protection of the Schengen external borders of the EU and in the fight against the terrorism but also in remaining other three application areas of our above mentioned SMART EU funded project.

**Keywords**: Smart ICT, Schengen External Borders, e-Government, Consumer Protection, Counter-terrorism.

## 1. INTRODUCTION

Under the framework of the EU funded project EU/7FP/Sec./SMART we have been researching application of the latest smart ICT in five selected problem or application areas viz.:

- e-Government
- Border control
- Counter-terrorism
- Consumer protection
- Smart surveillance in cyberspace.

In the following parts of this extended abstract we are going to present some basic results and experiences as being achieved from our still ongoing research in the above five selected problem areas. The results are quite a mixed one as in addition to some expected potential positives and benefits we have identified also a serious negatives and misuse in many cases even threatening some of the fundamental not only human but also other rights as guaranteed by the basic treaties to all citizens of the EU.

## 2. e-GOVERNMENT

In this – to some extent - the key, leading and coordinating application area from which all other application areas on the national level as well as the EU are somehow depended in their development is unfortunately one of the most disappointing regarding their overall performance in respect of the smart ICT utilization and application. Although it has been one of the main and most prioritized application areas also regarding investments into the latest smart ICT, its services to selected users in many EU member states are less than satisfactory. It is basically regarding all main kinds of functions like e.g. G2C, G2B, G2G, G2EU, etc. As the main vehicle for these kind of services has been developed e.g. in Slovakia the web at http:www.slovensko.sk where the citizens but also all other groups of users may find some basic information according to individual categories of users. But it is still prevailing more just as an information providing portal than as a portal for directly giving an opportunity to arrange directly some necessary actions like e.g. to establish a private company under the functions of G2B, or to arrange for a citizen its new modern e-ID card, e-EU passport, a driving licence, etc. As for the G2G the main problem is that individual governmental agencies and ministries have been preferring rather their own ministerial portals or data bases with own data than to have and share one common governmental data base. And that is also the problem of the communication between the individual governmental agencies and their partners among the EU institutions as functions of the G2EU. The same problem still exists also regarding the communications and cooperation, data sharing with and between the partner agencies in the individual EU member states. One of the main problems in this communication on the G2EU communications is the problem of language as according to the national legislations in many EU member states, all governmental tenders are only in the national languages so practically useless for their utilization on the entire common market of the EU. In addition to the problems with the insufficiencies of the above main governmental portals regarding their content and types of services, the problem is also with a rather user unfriendly mode of communication as it has been characterized recently e.g. also by the Deputy Prime Minister in charge for Information society in Slovakia. He has considered the system of communication with that governmental portal as a rather too complicated and difficult to access and using not only for ordinary citizens but also the people with some solid background in the utilization of the modern smart ICT like e.g. Internet, mobile applications, GPS, etc.. It should be a system for all citizens including those who are not right computer gurus but who are nowadays quite well ready for practical utilization and use of many kinds of the above mentioned consumers smart ICT appliances and applications.

## 3. SCHENGEN BORDER CONTROLS

This application area of the massive application and utilization of the latest smart and surveillance ICT is currently one of the most controversial problem areas in the EU. For example Bulgaria, Romania and Croatia as a latest entrants to the EU as yet cannot be a part of the Schengen system for protection of the external borders of the EU because they are not yet “ready and sufficiently reliable” partners in this protection. But at the same time over more than 1.5 million illegal immigrants have entered the EU territory just in the last two years under the absolutely unacceptable violation of any even the minimal principles of this border protection system as it is required by the EU Schengen legislation [1]. This legislation is consisting of not only a special Protocol to the Amsterdam Treaty and thus being an integral part of the so-called primary – constitutional - legislation EU but also it is represented by numerous regulations and directives. Just in a very brief overview of this legislation requirements it is necessary to mention that for the entry into the EU Schengen area it is necessary to have a valid passport with the Schengen visa that cannot be obtain just at the Schengen border but it must be obtain in advance, everybody has to have enough finances for the whole length of stay in the EU that normally is for 90 days as a maximum, those arriving from the outside of Europe have to have required immunizations certificates, etc. But most of these illegal immigrants are arriving to the EU without any of the above requirements and are even refusing to give their finger prints for their at least some identification, etc. That all has been happening in spite of the border control system that by its technological standard belong among the most advanced and perfect border protection system with the application of the latest smart ICT especially at the sea border of the EU. What is even worse it is the fact that most of these illegal immigrants are coming to the EU shores by boats of human traffickers and smugglers whose boats are very easily detected and recognized on the open seas but instead of capturing and confiscating their boats according to the requirement of the UN Convention on the fight against the international crime they are let to disembark their illegal immigrants and are allowed return back for another group of illegal immigrants to the places from where they will bring another contingent of illegal immigrants who have to pay horrible sums of money for their smuggling into the EU. There remains still some unanswered question from where those poor illegal immigrants have acquired those amount of foreign currencies especially in case of relatively large families where those fees are on the level of several thousands of USD or Euro, etc. In general this is a typical example of an evident difference between the theory and practice in application and utilization of the smart ICT and corresponding legislation for the protection of the Schengen area of the EU.

## 4. COUNTER-TERRORISM

This problem area is again a typical example of the paradoxical situation on application of the latest most advanced smart surveillance ICT in the prevention and fight against any potential terrorism e.g. as it is nowadays at airports but also more and more at various public places [2]. For example at the at airports in addition to several times repeated controls of all necessary valid travel documents, every passenger has also to pass through a very careful and in many cases even disgraceful, dishonest and humiliating body and hand luggage controls and screening. In some cases the security staff is more preferring their person to person body control by their hands than to rely on the results of the surveillance and controls by the latest smart ICT. That all happening at the same time when potential terrorists are illegally through the so called “green borders” or even more often by smuggling boats entering the territory of the EU without any identification, refusing even the finger printing or any other control of their identity as we have [presented it in the previous part of this paper. Although it is estimated that at least one percent of this illegal immigrants are potential terrorists or at least supporters of them what according even the very conservative estimates represents more than 15 thousand potential terrorists if we calculate them from the total of more than 1.5 mil. illegal immigrants who arrived to the EU in the last two years 2015-6.. It is also an undeniable fact that most of these illegal immigrants especially those young ones are army deserters or those who are by declaring themselves just poor victims of wars. But at the same time they are dressed in the latest sport outfits, with the latest smart phones men who thanks to those smart phones are well organized and well informed. They are fully and efficiently using their smartphones for fighting against any counterterrorism measures taken against them by the member states of the EU. By the GPS they are able to communicate among themselves or with smugglers in order to find the best routes how to cross illegally the internal borders within the Schengen area and/or to avoid any newly installed installation to protect internal borders between the member states in the EU that could prevent them on their way to the countries of their final destinations in the EU that are mostly Austria, Germany, Sweden, the UK, etc. Hence, again also in this case the smart ICT is more used or better misused for supporting potential terrorists than otherwise supporting fight against that. The problem is again more legislative or of the poor governance as the smart ICT in the hands of police and authorities concerned are dis-functioned by various human rights aspects cannot be fully used in the fight against the potential terrorism.

## 5. CONSUMER PROTECTION

It is a reality that all public places including shopping malls, offices, banks, streets, vehicles of the public transport and all various other places where it is “necessary” to control and monitor crowds and people moving around are under a permanent monitoring and surveillance by various latest smart and surveillance ICT including everywhere present CCTV cameras and other similar technology. But it is also unfortunately true that the results of this permanent 24 hours monitoring and surveillance are not preventing any crime or robbery and/ or any other criminal activities. But when it comes to the situation that people e.g. have been robbed by pickpocketing in the shopping malls or other similar places, the cameras recordings are not available for ordinary citizens as consumers or customers as all recordings belong to the particular owners or operators of those facilities. Those recordings could be obtain only if the police requests for them but it is quite a rare case as it has to be really some larger amount of money in order the police would consider it as a sufficient reason for their direct action. In view of all these monitoring and surveillance smart ICT, they are in fact not so much for the protection of consumers but more for their illegal monitoring and violation of their fundamental human rights regarding their right to protection of their privacy, personal data, property, etc. For example the personal data according to the particular EU legislation and thus also by the national laws of the EU member states is possible to collect and record only with an explicit consent of the particular person. But it is unfortunately a quite common practice that in order of the so called "improving of services to consumers" all communications with vendors are thanks to the availability of this smart ICT recorded and if a person has any objections against that unlawful recoding then the communication is interrupted by the vendor. Similar situation is also in the city transport vehicles e.g. in the City of Bratislava where it is a notice that the vehicle is monitored by CCTVs mainly of course for providing more security for the passengers [3]. But in fact in many cases there are not at all any CCTV cameras for surveillance the space but it is an official excuse for the tickets controllers in order they could record the communications with passengers who do not have a necessary ticket or like that. Hence again, the smart ICT is used not for the consumer protection but m principle against them and against their fundamental human rights regarding protection of their personal data, their privacy, etc.

## 6. SMART SURVEILLANCE IN CYBERSPACE

The absolute top misuse and a real haven and paradise for the misusing the latest smart ICT has been the cyberspace regarding all kinds of communications through Internet, mobile phones, GPS, smart housing, WIFI areas and all various other application areas of the smart communication systems. All these and various other communication channels in the cyberspace are not only permanently monitored but also recorded, stored, used and unlawfully shared also for and among various other often illegal purposes. They all are thus also a clear violation of any even most elementary principles on the protection of personal data privacy, personal integrity etc. as it is e.g. guaranteed to all citizens of the EU by the particular EU legislation [4]. According to the particular legislation the use of such data collected in the cyberspace could be only for the specific reason they were recorded for and such data could be stored only for a very limited time. But as we are witnessing it in practice, all these rules and regulations on the protection of personal data are regularly violated not only by various criminal gangs and hackers for whom it is often only a part of their professional perfection and techie skills in hacking. But as we have found out it has been unfortunately performed and quite widely also by those who have to be the guarantors of the respect for rules and laws for protection of citizens' rights [5]. Among those violators are unfortunately very often also national governments or their agencies, etc. as we have learnt from such cases like Snowden and like that

## 7. CONCLUSIONS

Also from this a rather short overview on application and utilization of the latest smart surveillance and monitoring ICT in the selected five application areas it is clear that in addition to many potential benefits that these technologies are bringing to the wellbeing, comfort and last but not least to security of ordinary citizens, at the same time they are also misused as smart tools for violation of any even the most elementary and fundamental human rights of the citizens i.e. people to whom by the particular laws all these smart technologies have to be first of all serving and helping. Of course it is not the problem that would be caused by this smart ICT itself. Unfortunately, it is the problem mainly of those institutions and/or individuals who have to be responsible for the proper application and utilization of this latest smart ICT.

## 9. REFERENCES

[1] D. Soltes, **Schengen e-Border Wall Supported by the latest Smart ICT, But …**, The 20th World Multi-Conference on Systemics, Cybernetics and Informatics Proceedings, Volume I, Orlando, Fl., USA pp 189-193, 2016

[2] **EU/7FP/Sec./SMART Project Final Report for the SR**, FM UK Bratislava 2015.

[3] **EU/7FP/Sec./SMART Project, WP 10** – Country Report Slovakia, Final Version FM UK Bratislava 2014.

[4] **Directive 96/46 EC on the Protection of Personal Data**, European Parliament & European Council, Brussels, 1995

[5] **Regulation (EC) No. 1882/2003 on Protection of Personal Data**, European parliament & European Council, Brussels, 2003