The Guantanamisation of Data

"A society that will trade a little liberty for a little order will lose both, and deserve neither" Thomas Jefferson

Published in Slovenian daily newspaper Dnevnik, Saturday Edtition Objektiv, November 2008

Barack Obama has promised that the US will close down the detention camp at its Guantanamo Bay base on Cuba, the inmates of which have been waiting (and waiting) for someone to finally tell them what evidence there might be against them, as well as when and on what basis they might receive a fair trail. In the meantime, and given the delay, it might be insinuated by others - rightly or wrongly - that these men are incarcerated because they have the wrong surname, believe in the 'wrong' God, or because their skin is not the right colour, or maybe even solely because they had a suspected Arab as a friend? In any event, this prison represents one of the biggest slaps in the face for basic human rights in the modern age. When those who are aware, see the Guantanamo inmates and listen to their stories, most condemn its very existence.

So just why was the Guantanamo camp established? In order to increase the security of the public in the war against terrorism; well, that's what the Bush administration used to reply. Concurrent with this unwarranted situation of detention without trial, a very different story is developing as to the collection and processing of enormous quantities of data - not only on US citizens, but indeed everyone - by America's *National Security Agency.* In actual fact EU member states are also collecting information on their citizens and, increasingly often, on others too. To most, such collection and compilation is neither questionable nor objectionable and the mentality prevails that *'if I have nothing to hide, nothing will happen to me, so I really don't mind.'* A retention center that stores our personal data doesn't hurt us, and in most cases we don't even know about it. So why do a growingly number of countries want to collect ever-increasing amounts of our personal data? One undoubted reason is to fight terrorism more efficiently. In relation to this I think that we should all be aware that the real value of freedom is revealed in times of crisis, and that democracy which is not able to function on the basis of those values which form the very foundation of our social development and respect for the individual, is not worth a penny.

Unfortunately we are living in an era in which we are all potential suspects, and hence society is under surveillance and - consequently - control; for some former communist countries the word "*again*" could also be added to the end of that last thought. The guiding principle of 'only impinging upon human rights when there exists a valid reason' has lost its erstwhile meaning. In the USA, as well as in Europe, the state collects data on everyone, just like that; such a resource is then stored in case it may someday be needed. Europe places emphasis on the supervision of personal data collections, and legal issues must be considered in relation to their processing. In the USA, the story is very different, and a lot of information on Europeans (for example all data on SWIFT bank transactions, while 39 elements of personal data pertaining to every air passenger travelling to the USA) ends up in the US domain without the consent of the EU. At the same time, a lot of data is collected without us being aware of it (such as within the context of the ECHELON satellite communications interception system).

There is absolutely no independent supervision of a great deal of data storages over which the NSA (National Security Agency) presides, and it is also possible to mine data without resort to a court order. The EDPS (European Data-Protection Supervisor) has long endeavoured for data exchange to be better supervised, and that the individual in particular - regardless of their nationality - would be able to check what elements of data pertaining to them is stored in collections, and furthermore that they would be entitled to the correction of any erroneous records, as well as enjoy court protection in disputes pertaining to the processing of their personal data.

Such a standpoint is not shared by the USA. American law governing the protection of privacy only allows the initiation of lawsuits by American citizens and individuals who have permanent residence in the USA. So, is there a similar Guantanamisation of data in Europe? In recognition of government and private sector organizations which have done the most to threaten personal privacy, NGO's in Germany awarded its *2008 Big Brother Award* to the EU's Council of Ministers, because it introduced and maintains records on alleged terrorists that bypass all democratic procedures. Many organizations and individuals who have been thus denounced have been stigmatised, and their human rights have been severely violated.

Last June, Sweden's parliament adopted some controversial legislation – the so called FRA[1] law, which sanctions the expansion of the supervision of society; it is an eavesdropping law which allows the state to track data exchanged among citizens via the Internet, telephone and telefax. This

[1] FRA is the Swedish government agency for the supervision of telecommunications

legislation actually facilitates complete control over a huge number of citizens, and should be precluded as it is incompatible with human rights legislation.

The digital revolution has had an immense impact on our privacy. Today we leave electronic tracks in many places and at all times. The collection and analysis of these trails leads to the creation of sociograms, which are, in themselves, supposed to be the final product in the analysis of information traffic. Such sociograms can, however, be marked with regard to the flow of information between senders and recipients. Indeed, on the basis of analyses of sociograms one can create a psychological profile of individuals, by means of which typical members of deviant social groups can be identified.

The idea behind the adoption of the disputable Swedish law is that those individuals who could possibly represent a danger to society may be identified through analysis of the huge quantity of data thus acquired. Such a system thus detects - surprise, surprise - potential terrorists, as well as hostile activities in other countries, ethnic and religious conflict, and even impending economic crises.

Many experts are - thank God - still shouting the warning that claims that we will be successful in preventing terrorist acts by using such techniques, are exaggerated. It is indeed the terrorists themselves, who, as a group of individuals, can most conscientiously and efficiently screen themselves against the possibility of supervision; the common citizen, however, does not; and can hence be placed in a an awkward position if their personal data should ever fall into the wrong hands.

The FRA law is a slap into the face to both democracy and human rights as it enables the state complete insight into the lives of individuals, something which Swedish advocates of privacy find a most scary prospect. Certain methods could, quite rightly of course, be applied in the case of military matters as well as in instances where terrorism or some other palpable threat is suspected. It is, however, quite unacceptable that everyone - including entirely innocent Swedish citizens - is included within such a system of surveillance.

Governments across Europe appear evermore eager to collect biometric data, fingerprints and DNA, in order to pursue the righteous struggle against terrorism and other crime. America's president is obviously already aware that even a fingerprint is very sensitive data - George Bush's security officers apparently wipe his fingerprints away from any surface he touches outside the Whitehouse. As a keen advocate of biometrics, which is supposedly quite harmless for the honest hard working citizen

who has nothing to hide, Germany's Minister of the Interior, Wolfgang Schäuble, has also of late been made more aware as to such sensibilities. Some activists stole Schäuble's fingerprint from a glass at a party in order to show him 'in a graphic way", what one can do with a fingerprint; namely, they posted it on the Internet, together with instructions as to how fingerprints may be misused. Since then, Herr Dr. Schäuble's statements have been a tad more reticent.

When we talk about the society of surveillance, the critical question arises as to how far we should go? What are we going to find acceptable in order to prevent crime, increase security and employ all those exceptional possibilities afforded by modern technology? In relation to this issue The EU has undertaken a major step towards the surveillance society through the adoption of the *Directive on Data Retention in Telecommunications*. And although this Directive has yet to be implemented in all member states, additional steps are already under discussion. As it happens Slovenia has generously and completely non-critically adopted the longest period of the retention of data foreseen by the said Directive, namely two years, whereas most countries opted for a period of one year or even six months. It was really just a matter of time as to when those exercising this power would realize that all this data retention is of little use if in some European countries - Slovenia included - one can anonymously buy a pre-paid SIM card, and hence anonymously use a mobile phone. I suspect that very few criminal masterminds care to undertake subscription agreements for those phones intended for aiding or abetting the perpetration of evil deeds or criminal activities; this for the very fact they would have to entrust a mobile operator with a deal of their personal information, whereby data on their calls would be duly retained for the statutory two years. No, indeed they would most likely buy a pre-aid package from their nearest newsagent, calmly carry out their business and then throw the phone away.

The possibility of anonymously purchased SIM cards should, accordingly, be prohibited, and judging by the EU's latest excellent idea this is only a matter of time. By compelling all villains to sign up for their mobile phones, the forces of law and order will now be able to breath right down their collars; those few whinging NGOs who don't care for the idea will be easily pacified. Henceforth, all will be well and good in the world …or will it? Are we going to prohibit the lending of mobile phones to other people? Will phone calls have to be reported to the authorities, and will we kindly have to ask them to allow us to make a call - as was the case in Ceauşescu's Romania? When will the same destiny meet the instant messaging programmes, email, data transfer and modes of communication currently not yet covered by legal requirements regarding compulsory data retention? Is it not better to concentrate on content? And better still - if we really want to stop terrorists, criminals and other

ne'er-do-wells – why take such limited measures, why not control everything? That way will we be able to prevent bad things from happening before they actually occur! Such a brave new world is envisaged in Steven Spielberg's 2000 film *Minority Report*, in which - on the basis of foreknowledge - the "*pre-crime*" police department apprehends criminals ahead of the crime being committed. Indeed, if the technology is there, why not use it? Well, there's the rub.

You have to accustom the public gradually. If we make one small step towards a surveillance society every day, then people won't even notice the control. Moreover, when presented appropriately, the *vox populi* will even demand it; after all, they want security. Yesterday it was data on electronic communication, and tomorrow - because criminals might abuse the system - we will have to give the lady at the newsagents our ID if we want to purchase a pre-paid mobile package. And what is in store for the day after tomorrow? …No, I do not like being followed at every step, even though I've got nothing to hide.

There is another aspect I would like to warn about, and it too concerns security. We often hear that we have to relinquish a degree of privacy to ensure our security; such is a game with a negative score, in which no benefits may be accrued without some loss being incurred. My colleagues and I deal with the protection of personal data and privacy on a daily basis, and do not want to play by such rules. In our opinion, it is not a matter of choice between security and privacy, but rather one between freedom and control. When new technologies are employed, we have to ask ourselves whether or not we want greater control or more freedom; this is the essential question.

We do not have to sacrifice our privacy in order to achieve better security; technology can be employed in such a way to ensure a win-win situation. Biometrics, for example, can significantly increase security using any solution in which retained biometrical data remains in the possession and thus under the under control of the individual to which it pertains. By way of such methodology, the individual holds their own biometric data, thus it does not need to be stored or encrypted in any system which may be abused. Accordingly, the privacy of the individual also becomes far more secure. Electronic toll collection, for example, can also be carried out efficiently without resort to processing personal data, the charge being made on the basis of data pertaining to the vehicle – namely a device which records the number of kilometres driven, as opposed to systems which necessitate reference to vehicle location together with unwarranted personal information pertaining to its driver. Indeed, only those schemes which are ill-conceived, poorly thought-out, or in which security issues are exaggerated, exert a negative impact on the freedoms and privacy of the individual.

Microenvironments, especially the working environment, are becoming an important battleground in the struggle between control over and the exercise of basic human rights. As has been demonstrated in several cases in which the Information Commissioner intervened, this is a somewhat grey area which yearns for more precise statutory regulation. Is it appropriate for employees in the workplace to be treated differently from movie stars or royalty? Princess Margaret, scrutinised at every step along the way by the paparazzi, once remarked that she had as much privacy as a goldfish in a bowl.

So, what are the acceptable boundaries in the surveillance of employees? How far should the rights and interests of employers or third parties extend? Today technology enables almost perfect surveillance of employees – control of access to the Internet, electronic mail, video surveillance of premises, and GPS management of company vehicles… For a mere hundred bucks per user, an employer can install undetectable spyware which every Friday afternoon will send him an email containing a report on how much time an employee has spent surfing non-work-related websites, the number of video clips sent and the most frequently called telephone numbers. The fact remains that in this age of electronic communications each workplace generates a wealth of personal data, such is the nature of this technology. Telephone calls are recorded, as are the websites accessed and electronic mail sent. Where do the limits of data collection lie? Who should be allowed to use such information and for what purposes? The jury is still out on the jurisprudence of surveillance, and recent cases in Slovenia reveal the need for legislation - predicated on constitutional provisions as to the privacy of information and communication - which would more precisely define the admissible limits of intervention into the private lives of employees.

The answer to one question underlies the answer to all the others iterated herein: Are we able to purge the evil and wrongdoing in this world through the introduction of a surveillance society?

In accordance with a Gaussian function, the probability density distribution of any given phenomenon or population will resemble a bell-shaped curve when displayed graphically. At the tapering margins, to the left and right of the central body of the curve - i.e. on either side of the bulging apex that marks the middle - are those who are particularly malevolent or benevolent, honest or deceitful, clever or stupid, beautiful or ugly, industrious or lazy, short or tall. However, we will not - by means of any measure of surveillance or control over the entire population - eliminate the ugly, dirty or evil people who exist to one side of the Gaussian curve; we may, however, curtail the endeavours - at least to a certain extent - of those at the margins who are a driving force in the development of society: the innovative and inventive, those who make this world more beautiful, or

dare to shout out loud when society is on the wrong path, together with those who love democracy and hate dictatorship.

Unchecked surveillance and control leads us towards a dystopian future, a *Truman Show*, in which the life and independence of the individual is subordinated by others who are not overseen or controlled by anyone. In any such society, those who exercise control over the data, shall be able to wield control over the individual; such superintendents will be able to exert power, immense power. Does a surveillance society lead towards totalitarianism and the curtailing of social diversity, which is itself the pre-condition for our development? If people become paranoid and afraid of everything, because they are controlled at every step, then they will become automatons.

Let us reflect on Goethe's words: "*Talents are best nurtured in solitude*."

Do we possess sufficient knowledge and ability to close down the Guantanamo of data? Am I exaggerating? I don't know. Maybe. I hope I am.

Nataša Pirc Musar,
Information Commissioner of the Republic of Slovenia