



Warsaw, 30 March 2014

**Ms Navanethem Pillay
UN High Commissioner for Human
Rights**

Dear Ms Pillay,

In response to your invitation to submit our input regarding General Assembly resolution 68/167, Panoptykon Foundation would like to present a short brief on the surveillance practice in Poland and general recommendations concerning this issue. Should you have any further questions, please, do not hesitate to contact us.

BACKGROUND

Digital technologies can be used both as a tool of empowerment and as a tool of oppression or surveillance. We witness rapid development of all types of security-oriented technology, such as CCTV, body scanners, geolocalisation, specialised software used for profiling etc. On the other side, the state shows a tendency to gather and process more and more personal data with the view of managing the needs of its citizens better. Thus we face the creation of integrated data bases, including in such sensitive areas as medical care and criminal records. We believe that both these general tendencies and particular projects pursued within the state administration or law enforcement deserve thorough analysis and intervention in order to ensure the right balance between digital freedoms and surveillance.

For several years now a discussion has been underway in Europe concerning the use of telecommunications data (billings, location data) for the purpose of combating crime. The Europe-wide retention regime was introduced by the Data Retention Directive in order to increase availability of telecommunication data for the purposes of investigating and prosecuting serious crimes.

This problem is particularly visible in Poland, which not only opted for the most privacy-intrusive solutions when implementing the Directive but also allowed itself for over-implementation in some respects, in particular with regard to the purpose of data retention. The police and secret services are empowered to access billing and location data once retained without any control (e.g. judicial control, prosecutor's oversight or ex post control exercised by the citizens themselves). Law enforcement agencies have no obligation to inform the person in question that operational measures had ever been applied once the proceedings are completed. Because of this flawed legal framework, the official number of requests for telecommunication data in Poland is staggering: almost 2 million per year (versus hundreds of thousands in other EU member states).

Regarding Internet users data, our recent research gives reason to think that in Poland we are not facing mass surveillance of Internet service users from the Polish law enforcement and intelligence agencies. On the other hand, we have to stress that legal procedure regarding requests for Internet users data is vague and should be clarified.

Recommendations

- Human rights requirements

Surveillance practice should meet all appropriate criteria for human rights limitations. According to international law restrictions to human rights can be provided only by the law and aimed at achieving a legitimate objective and also be reasonable, necessary and proportionate. Thus legally binding instruments should precisely lay down criteria how and when personal data could be used by LEAs and secret services.

- Strong data protection legal framework

We need strong data protection legal framework, both on the national and global level. Those instruments should be legally binding and give citizens adequate safeguards against privacy violations. In particular, it should address such issues as: legal grounds for data processing, definition of consent for data processing, right to object to processing, right to be informed about processing. This instrument should cover activities of both private companies and public authorities. A good point of reference for global privacy standards could be the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe of 1981.

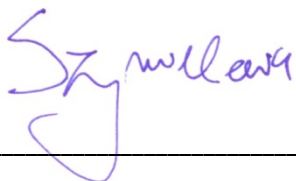
- Independent oversight

Countries must introduce external and independent supervisory mechanisms for verifying whether law enforcement agencies and intelligence services carry out their surveillance activity in accordance with the binding law. Where personal data are involved, the problem of a lack of supervision over the operation of the LEA is deepened by the fact that citizens themselves have no possibility to verify whether public authorities have requested their data from private companies.

- Transparency and auditing

Citizens should have the right to know how many user data requests have been made by public authorities, what they specifically refer to, who files them, and how many of them have been processed. Moreover, public authorities should evaluate whether the possibility to access e.g. mobile phone user data has had any influence on their ability to combat crime or other operations.

Sincerely,



Katarzyna Szymielewicz

President of the Panoptykon Foundation