Helsińska Fundacja Praw Człowieka
ul. Zgoda 11, 00-018 Warszawa
tel.: +48 22 556 44 40; fax: 556 44 50
www.prawaczlowieka.pl

FUNDACJA PANOPTYKON
ul. Królewska 2, 00-065 Warszawa
tel: +48 692 404 096
www.panoptykon.org

5th November 2010

JOINT STATEMENT REGARDING THE EVALUATION OF DIRECTIVE 2006/24/EC

On behalf of two Polish non-governmental organisations: the Panoptykon Foundation (a member of European Digital Rights Coalition) and the Helsinki Foundation for Human Rights, and having consulted the National Chamber of Commerce for Electronics and Telecommunications, we would like to express our opinion on the data retention regime as implemented in Poland in connection with the process of evaluation of Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC ("**the Directive**") that is currently being carried out by the European Commission. We have been monitoring the functioning of the data retention regime in Poland and we remain deeply concerned about the impact of this regime on the rule of law and observance of fundamental human rights in our country. We hope that the Commission will take the facts and arguments stated below into account when preparing its evaluation report.

In this statement we will:

(1) recall general arguments questioning the necessity and proportionality of the Directive which have already been formulated on the grounds of the European Convention on Human Rights and *acquis communitaire*;

(2) describe the functioning of the data retention regime in Poland, stressing the risks it involves from the human rights and the rule of law perspective;

(3) formulate key recommendations regarding the amendment of the Directive.

1. Fundamental criticism of the Directive on the grounds of European legal order

It is important to recall that the retention of traffic and location data in accordance with the provisions of the Directive constitutes a major interference with the right to privacy and secrecy of correspondence as guaranteed in Article 8 of the European Convention on Human Rights. Therefore, both the Directive itself and the national legislation implementing it must meet the conditions laid down in Article 8 for a lawful restriction of that right: any such restriction must be "in accordance with the law" and "necessary in a democratic society" for a legitimate purpose.

In 2008, the European Court on Human Rights found "that the blanket and indiscriminate nature of the powers of retention of fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to

strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard"[1]. This finding must, *a fortiori*, apply to the blanket and indiscriminate nature of the powers of communications data retention, which (i) relates to persons not even suspected of offences and (ii) concerns communications data, which is far more revealing than biometric identification data.

In 2009, the Constitutional Court of Romania found that the principle of blanket data retention violates the European Convention on Human Rights[2]. The High Court of Ireland decided in 2010 that it will refer to the European Court of Justice the question of whether the data retention directive is compatible with fundamental rights[3].

Finally, at the time the data retention regime was debated and adopted, the most widely recognised European data protection authorities – namely the Article 29 Working Party and European Data Protection Commissioners – pointed out the incompatibility of blanket communications data retention with fundamental human rights and *acquis communitaire*.

We will recall only a couple of statements, which seem particularly relevant at the point of evaluating the Directive:

"The European Data Protection Commissioners have noted with concern that in the third pillar of the EU, proposals are considered, which would result in the mandatory systematic retention of traffic data concerning all kinds of telecommunication for a period of one year or more, in order to permit possible access by law enforcement and security bodies. (...) The European Data Protection Commissioners have repeatedly emphasised that such retention would be an improper invasion of the fundamental rights guaranteed to individuals by Article 8 of the European Convention on Human Rights, as further elaborated by the European Court of Human Rights (see Opinion 4/2001 of the Article 29 Working Party established by Directive 95/46/EC, and the Declaration of Stockholm, April 2000)."[4]

"The routine comprehensive storage of all traffic data, and user and participant data, proposed in the draft decision would make surveillance that is authorised in exceptional circumstances the rule. This would clearly be disproportionate."[5]

"The decision to retain communication data for the purpose of combating serious crime is an unprecedented one with a historical dimension. It encroaches into the daily life of every citizen and may endanger the fundamental values and freedoms all European citizens enjoy and cherish."[6]

All of the above arguments formulated by data protection authorities remain adequate today, since the Directive, in the shape it was finally adopted, fully accounts for this legitimate criticism.

---

[1] ECtHR, S. and Marper v. The United Kingdom, application nos. 30562/04 and 30566/04, 4 December 2008.

[2] Constitutional Court of Romania, decision no. 1258, 8 October 2009, http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html.

[3] High Court of Ireland, record no. 2006/ 3785P, 5 May 2010, http://www.scribd.com/doc/30950035/Data-Retention-Challenge-Judgment-re-Preliminary-Reference-Standing-Security-for-Costs.

[4] Working Party, Opinion 5/2002 on the Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9-11 September 2002) on mandatory systematic retention of telecommunications traffic data.

[5] Working Party, Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism.

[6] Working Party, Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

2. Concerns with the (mis-)use of the data retention regime in Poland

In the scope of our statutory tasks, we have been monitoring the functioning of the data retention regime in Poland in the shape it was adopted as a result of implementing the Directive. There are numerous concerns that deserve to be expressed in the context of evaluating the Directive. Polish case study proves that the Directive failed to set firm and unequivocal limits to the scope and use of data retention.

The Directive was transposed in a semi-secret way, without adequate public debate. Firstly, in the statement of reasons for the amendment of the Telecommunications Act, no calculation as to the costs of the transposition of the Directive was provided. Secondly, the very draft amendment of the Telecommunications Act that was formally subject to public consultation, did not include the material changes implemented to the national legal system, since these were subsequently adopted within a one-month period in the form of an ordinance of the Minister of Infrastructure[7] that entered into force within the next couple of days. This draft ordinance was consulted on solely with the telecommunications industry, and lacked the consultation of other interested parties, such as human rights watchdog organisations.

As a main result of the lack of proper public discussion over the transposition, the very scope of data retention in the field of mobile telephony was broadened; in particular it was extended with regard to location data[8]. According to the above mentioned ordinance implementing certain provisions of the data retention directive[9], the necessary location data for both pieces of telecommunications terminal equipment is not limited solely to the information on the Base Transceiver Station ("BTS") covering the area in which the device initiated/received the call; the necessary information also covers every other (than primary) BTS to which the telecommunications terminal equipment (calling or receiving the call) is switched during the call.

Secondly, Polish law[10] allows for very permissive use of traffic data; namely, this data can be used for general crime prevention purposes (and not only the prosecution of most serious crimes as intended in the Directive), thus allowing law enforcement agencies the indiscriminate acquisition of data, which reveals the social network and place of residence of a given person. The law does not specify the prosecution of what kind of crimes shall justify the use of traffic data, neither is the access to such data conditioned by the gravity of charges. As a result, data

---

[7] The Minister's of Infrastructure Ordinance of December 28, 2009 on the detailed list of data and types of public telecommunications network operators or providers of publicly available telecommunications services required to retain and store data (Polish Official Journal of 31st December 2009 [Dz.U.09.226.1828].

[8] Information for the European Commission on the statistics on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or a public communications network in connection with Article 10 of Directive 2006/24/EC and the Article 180g (2) of the Polish Telecommunications Act (Polish Official Journal of 3rd August 2004 [Dz.U.04.171.1800] with further amendments).

[9] Namely sections 5a and 6a of paragraph 4 of the ordinance.

[10] Competences permitting the use of retention data are contained in the specific laws regarding particular services (see also the footnote 13 below for the list of the authorized services). For example, Art. 18.1 of the Law on Central Anticorruption Bureau states that:

1.The obligation to obtain a Court warrant does not concern information necessary to fulfill tasks of the CAB prescribed by law that consist of data regulated by Art. 180 c and 180 d of the Telecommunications Law (so called 'retention data');

2. The telecommunications operator is obliged to make the retention data accessible to the CAB with no charges:

1) on a written motion from the Head of the CAB or a person authorised by them;

2) on oral request of the CAB agent, possessing a written authorisation issued by the Head of the CAB or a person authorised by them;

3) through the telecommunications net to the CAB agent, possessing a written authorisation issued by the above mentioned persons.

retention is frequently used by the police in all sorts of cases, including those as minor as enforcement of alimentary obligations. Also, more and more often traffic data is requested by the parties in civil disputes such as divorce cases.

Thirdly, the existing law empowers the police and secret services to access billing and location data once retained without any control (e.g. judicial control or *ex post* control exercised by the invigilated person – at present secret services have no obligation to inform the person in question that operational measures had ever been applied once the proceedings are completed). Moreover, the actual procedure used by policemen and other security agents does not fulfil proper security and control standards. Operators report that the retained data is accessed through simple interfaces established on telecommunications networks lacking any registration procedures in the network provider's systems. The draft law containing the technical specification of the interface is yet to be adopted. Overall, existing legal provisions are vague and all they require from telecommunications operators is that they be in cooperation with secret services. In fact, the transposition of the Directive only gave the secret services democratic legitimacy to require the retained data in the prosecution of an unlimited array of crimes, as well as broadened the scope of retained data.

Finally, the rudimentary official data stored and available to the public (e.g. under law on access to information) is not sufficient to assess how often, for what purposes and with what results for crime investigations the traffic data is being used by the secret services[11]. Relevant data both from network operators and competent enforcement authorities should be collected in order to provide a broad and thorough picture of the mode and effectiveness of the use of the retained data. The scope of statistical data to be submitted on a yearly basis to the Office for Electronic Communications ("OEC") by the telecommunications undertakings pursuant to Article 10 of the Directive is far too narrow to provide exhaustive information for the purposes of controlling whether the right to privacy is adequately protected. Taking into account the uncontrolled and unlimited interface access of the competent agencies to the stored data, it may well be possible that a given operator may not possess all the data necessary to provide adequate numbers. Moreover, so far the data in question are collected by the OEC in order to report it to the European Commission, which evokes serious doubts as to whether all these data will ever be publicly available.

Notwithstanding the above mentioned drawbacks of the obligation to submit statistical data to the OEC, the scarce information that was made available to the public still allows for certain conclusions to be drawn. The statistical data provided by the OEC[12] (in accordance with Article 10 of the Directive) for 2009 shows that Polish law enforcement agencies, including secret services, requested access to traffic data as many as 1.06 million times. This number is very telling as far as the approach to data collection and the prevailing mentality among law enforcement agencies in Poland is concerned.

Taking into account the range of authorities that are given access to the retained data in Poland, the lack of adequate data showing the use of data and its effectiveness in crime investigations seems even more evident. As a result, there is no democratic control over the use and

[11] The Panoptykon Foundation has asked various governmental agencies to provide such information, with no material result.

[12] Information for the European Commission on the statistics on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or a public communications network in connection with Article 10 of Directive 2006/24/EC and Article 180g (2) of the Polish Telecommunications Act (Polish Official Journal of 3 August 2004 [Dz.U.04.171.1800] with further amendments).

effectiveness of this very invasive tool. The Helsinki Foundation for Human Rights has for several years been fighting with the Internal Security Agency and the Central Anti-Corruption Bureau to disclose the statistical number of wiretaps, but both agencies consistently refuse to disclose this data claiming state secrecy. Both cases were brought to administrative courts. In the case against the Central Anti-Corruption Bureau, the Supreme Administrative Court concluded that "statistical data on the use of the measures of operational control should be considered public information"[13].

Recent developments in Poland, in particular a series of political and media affairs involving surveillance of journalists and important public figures, shows some of practical threats posed by the data retention regime in its current shape. Police and secret services have been notorious in invigilating several well-known journalists, aiming to identify their journalistic sources of information. This practice undermines the foundation of a democratic society, i.e. the protection of free and independent media and the principle of freedom of expression. Retention of telecommunications data was among the key tools misused by the secret services in these investigations.

Concrete examples of how traffic data and location data tends to be used in practice can be found in numerous journalistic reports and press interviews with former security agents and prosecutors, which were published in connection with recent affairs[14]. On the basis of this journalistic material, it is clear that numerous agencies[15] are allowed to request traffic data records in a rather informal manner, without the need to justify such request or undergo any transparent legal procedure.

The chain of affairs involving uncontrolled surveillance of journalists and public figures evoked a great deal of criticism from both media and human rights defenders. The Helsinki Foundation for Human Rights has recently published their open letter to the prime minister calling for legislative measures to limit secret services' powers in the scope of surveillance[16]. Among many critical statements in this letter, we read:

“As long as the problem of excessive police and secret services' powers – resulting from loopholes and abuse of power – continues to exist, Polish law in this respect will not correspond to constitutional and international standards, and individual rights and freedoms will not be properly respected. (…) Under Polish law there is a range of provisions that allow the police and special services to carry out surveillance of various people. Disclosures of abuse prove that these special powers meant for the fight against international terrorism and organised crime are in practice used to gain information about political opponents or journalists who try to control political decision makers. Such practices undermine the foundations of democracy, the core

[13] NSA (1.10.2010) sygn. I OSK 1149/10

[14] Gazeta Wyborcza, Ewa Siedlecka, „Władza staje na straży swojego interesu”
[http://wyborcza.pl/Polityka/1,103836,8506779,Inwigilacja_dziennikarzy___wladza_staje_na_strazy.html]
Gazeta Wyborcza, Wojciech Czuchnowski „Speckomisja: można inwigilować dziennikarzy”
[http://wyborcza.pl/1,75478,8506756,Speckomisja__mozna_inwigilowac_dziennikarzy.html]
Gazeta Wyborcza, Wojciech Czuchnowski, „Dziennikarze na celowniku służb specjalnych”
[http://wyborcza.pl/1,75478,8480752,Dziennikarze_na_celowniku_sluzb_specjalnych.html]
Wiadomości 24, Monika Olejnik, "Podsłuchiwano mnie i dziewięciu innych dziennikarzy"
[http://www.wiadomosci24.pl/artykul/monika_olejnik_podsluchiwano_mnie_i_dziewieciu_innych_163217.html]; Gazeta Wyborcza, Monika Olejnik, Agnieszka Kublik„10 mln. Za wojnę bogów”;
[http://wyborcza.pl/1,75480,8542355,10_mln_za_wojne_bogow.html?as=7&startsz=x]

[15] There are nine different agencies in Poland entitled to use data retention for investigation purposes, namely: [Police, Border Guard, Internal Security Agency, Intelligence Agency, Military Intelligence Service, Military Counter-Intelligence Service, Military Gendarmerie, Central Anti-Corruption Bureau and Treasury Intelligence.

[16] The letter is enclosed.

values of which are pluralism and freedom of expression, including the protection of journalistic sources of information".

Furthermore the Helsinki Foundation for Human Rights claims in its statement that there is a legal gap in the existing law which does not regulate the terms and limits of the use of modern technological measures by secret services (e.g. billings, BTS, GPS). These rules should be defined very precisely, as the measures generate the risk of a profound invasion of citizens' privacy. It is postulated, therefore, that the Telecommunications Law be changed.

We conclude that the data retention regime as designed by the Directive and subsequently implemented in Poland amounts to invasive surveillance of the entire population, which cannot be accepted in a democratic society. Blanket data retention undermines professional confidentiality, the protection of confidential journalistic sources and the right to privacy in general, thereby deterring citizens from using electronic communications networks for the purpose of private or confidential communication.

Because of the lack of appropriate legal safeguards and taking into account how easily enforcement officers can access the traffic data of all citizens, it seems that the data retention regime as shaped by the Directive and implemented in Poland violates fundamental human rights as well as the principles of necessity and proportionality, and consequently paves the way for an ever increasing mass accumulation of information about the entire population.

3. Key recommendations regarding the amendment of the Directive

We welcome the fact that Commissioner Cecilia Malmström has publicly declared on several occasions that one of the major purposes of the current evaluation process is to assess whether the data retention directive meets EU obligations under the Charter of Fundamental Rights, in particular whether it meets the "necessity and proportionality test", which needs to be applied to every limitation of the right to privacy as well as any other fundamental freedom.

In this context, we would like to suggest that the following key amendments to the Directive be considered in the evaluation process:

(i) **"Serious crimes" should be enumerated**

Serious crimes the prosecution of which can justify the use of traffic data should be enumerated in the Directive. Without such measure it is not possible to meet the aim of harmonising the data retention regime across the EU. In order to prevent traffic and location data from being systematically misused, the Commission will need to propose to the Parliament and Member States a clearly defined limit on its permitted use.

(ii) **Definitions of "serious crimes" should be harmonised**

It is not only necessary that "serious crimes" be enumerated, it is also essential to harmonise their legal definition, i.e. define what "computer-related crimes" or "terrorism" mean. Otherwise Member States will always tend to stretch these definitions in order to pursue their own political priorities, e.g. treating the prosecution of soft drugs trafficking on the same grounds as the fight against international terrorism.

(iii) **Access to retained data must be limited**

It is necessary to subject the agencies that have access to retained data to external,

preferably judicial control, in order to safeguard citizens' rights. Access to sensitive data should have an even higher standard of control. The European Commission should, therefore, lay down the rules for access to privacy-sensitive data instead of leaving this crucial task to Member States. One of the key issues to be harmonised in this respect is the definition of "competent enforcement authorities" entitled to access retained data. At present it is entirely for the Member States to decide on this, which leads to systemic problems such as the misuse of retained data, as reported from Poland.

(iv) **Retention period should be shortened and harmonised**

The data retention period should be harmonised and shortened to the minimum (e.g. six months). On the basis of the Article 29 Data Protection Working Group's report on the second joint enforcement, action , one has to conclude that the approach based on the limited harmonisation in the field of data retention failed. In practice, Member States applied a very different approach to key issues such as data retention periods and the terms upon which law enforcement agencies may obtain access. As a result, Poland used this legal opportunity to extend the data retention period as much as possible, beyond what can be deemed necessary and proportionate in a democratic society.

(v) **Data protection and data security must be ensured**

As recommended by the European Data Protection Supervisor, rules on access and data protection should be included in the Directive in order to prevent the misuse of retained data. It is necessary to ensure that general principles of data protection continue to apply and affect the terms and limitations of the data retention regime. The right to privacy needs to be maintained in the sense that data retention should only be allowed when necessary (and not only beneficial) for the prevention of serious crimes. European law, including Article 15 of Directive 2002/58/EC, requires that access to data be necessary, proportionate, and appropriate within a democratic society before it is granted. It is worth considering whether the Directive could impose on Member States the obligation to create a specialised, independent body (resembling an Ombudsman) empowered to control the use of surveillance measures by law enforcement agencies.

(vi) **An independent evaluation of data retention regime should be performed**

The Directive should provide for an independent and external mechanism of evaluation of how the data retention regime functions in all Member States. Such mechanism should involve review by more than one external institution, for example: the European Commission, the European Data Protection Supervisor and the Article 29 Working Party.

(vii) **Collecting statistics from Member States**

In order to fulfil the above objectives it is necessary that Member States collect detailed statistics. For the purposes of subsequent evaluation it should be required that all data regarding individual cases be retained in a special register. Moreover, it is essential that Member States collect information about all cases of abuse of data retention schemes and records of all cases, where data was requested but no legal case was instigated against the individual in question. Finally, Member States should be requested to

provide data that justify the use of data retention as the only and necessary measure of prosecuting serious crime, i.e. proving that no other (less intrusive) measure could have been used to reach the same effect.

The statistics should be sent yearly to the European Commission in order to enable independent evaluation of how the data retention regime functions in practice. This statistical data should also be published to enable society to exert control over the government through media and watchdog organisations.

(viii) **Reimbursement**

Costs of data retention schemes must not be put on consumers. This is particularly so as Member States have been insisting on their right to retain traffic data for extended periods of time; these Member States must be required to cover the costs of retention and provision of traffic data to law enforcement agencies. The Directive should provide for harmonised rules of cost reimbursement to the effect that this burden be shifted from consumers of telecommunication services to law enforcement agencies. Otherwise we will face the challenge of discriminating against consumers in those Members States that generate higher costs related to their law enforcement agencies' preserving and accessing traffic data.

4. Concluding remarks

In light of the above facts and concerns, we conclude that the implementation of the Directive has led to a systemic problem with ensuring safeguards for fundamental rights and the rule of law. This is not only due to the shortcomings of the Polish legal system and the abuse of power but also to the shortcomings of the Directive itself. In our opinion these shortcomings undermine the sensibility and effectiveness of this regulatory measure. In light of our concerns, the European Commission should either make sure that all of the suggested amendments are introduced in the Directive or consider abandoning this regulatory measure altogether. Maintaining an ineffective and selective regulatory measure, such as the Directive in its present shape, may lead to further abuses and misinterpretations of its underlying rationale, such as those reported in our statement above.

We urge the Commission to give this problem their utmost attention since it affects both the fundamentals of European democracy and the principles of the single European market. The Directive not only imposes a number of limitations affecting traditional civil freedoms but also generates considerable financial costs, which effectively will always be borne by the same citizens who suffer from the limitations in question. This double effect in itself should be a more than sufficient argument to carry out the evaluation process with all the diligence it requires.