Introduction create a culture of transparency regarding bulk

IntroductionToday we often rely on modern investigation techniques to fight against serious crimes such as terrorism and drug dealing, however this good objectives does not always justify the means. Data retention has always been a subject of dispute.

So on 21 December 2016, the Court of Justice released a judgment in cases Tele2 and Tom Watson concerning the ability of EU States to make electronic communications service providers to retain traffic and location data for all providers' users. The cases appeared after the ePrivacy Directive, which gave permissions to restrict the rights on the confidentiality of communications, for instance for reasons of national security. Controversial is also the matter regarding the role of companies and government in the conversation about how privacy rights should develop. There is a concern that corporate interests would be contrary to protection of individual privacy protection.

There is no need in putting too much faith in government, as their interests in combatting crime may also lead to infringing of privacy. We are facing government reluctance to create a culture of transparency regarding bulk data collection and access, including the limitation of end-to-end encryption on social media services like WhatsApp, which was also shows the government's view on the human right. The aim of current research is to find the ways of implementing data retentions without violating fundamental human rights for privacy. The implementation is a lot more complicated then may seem on the first view as it encountered with several problems such as that the content of telecommunications is often very private, and therefore calls for a high level of privacy protection, also while analyzing,

communications metadata can result in very personal insights about individual persons – such analysis may for example reveal the political or sexual preferences, the habits of everyday life.

So it should be approached with great caution and respect to privacy. 1. BackgroundThe Data Retention and Investigatory Powers Act 2014 made an obligation for public telecommunications operators to retain communications data for a period of 12 months. This created a condition when all communications data but not the content was routinely retained by operators and stored within a data archive.

Using the Regulation of Investigatory Powers Act 2000 (RIPA 2000), law enforcement agencies then accessed these archives, for example if necessary in the interests of national security or for the purpose of preventing or detecting crime. However liberty activists were unhappy with this state, saying that it violate citizens' privacy, having their every communications activities logged and stored away. They argued about the DRIPA 2014 statements as being incompatible with EU law by way of a judicial review and were successful in the High Court. Besides, the retention of data in order to transmit it to the competent authorities correspond with the general interest, for example fighting against serious crime and, correspondingly, public security. However, by adopting the Data Retention Directive, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality.

Although the retention of data required by the directive may be considered to be appropriate for attaining the objective pursued by it, the wide-ranging

and particularly serious interference of the directive with the fundamental rights at issue is not sufficiently circumscribed to ensure that interference is actually limited to what is strictly necessary. The retention and access to data is interconnected with the fundamental rights to respect of private life and personal data. The retention of data required by the directive should not negatively affect on the concept of the fundamental rights to respect for private life and to the protection of personal data. The directive does not allow to know the content of the message and ISPs must respect certain principles of data confidentiality and integrity. So directive is incompatible with Fundamental Rights of the European Union as it should correspond with the rights to respect for private life and protection of personal data.

2. Current stateCurrently the Lawful Interception Act is developing and it is expected that it will enter into force on 1 January 2018. According to it all service providers will have to provide authorities with:-identification data, -content data in real time-traffic data in real time, retroactively for a period up to 6 months. However that warrants could be too broad in the context of Tele2 case, so the Act definitely needs some further refinement. The current Court’s answer is that EU law precludes national legislation that prescribes general and indiscriminate retention of data. The Court confirms first that the national measures at issue fall within the scope of the directive. The protection of the confidentiality of electronic communications and related traffic data guaranteed by the directive, applies to the measures taken by all persons other than users, whether by private persons or bodies, or by State bodies.

So it was determined that these retention provisions are not compatible with EU law, the government needs to change the law significantly to make it compliant. This will require the implementation of further cases in which data retention circumstances will be lawful. All in all, progress on the issue since the CJEU's invalidation of the Data Retention Directive remains limited. This may partly be because of the absence of standardized rules across EU.

Eurojust, the EU agency for judicial cooperation in criminal matters, has stated: while data retention schemes are considered necessary tools in the fight against serious crime, there is a need to create an EU regime on data retention that complies with the safeguards laid down by the CJEU. In any event, regardless of whether at European or national level: as long as data retention measures continue to be deployed, adequate protection measures must soon be implemented to prevent fundamental rights violations. In order to show current political mass retention risks associated with metadata, the Advocate General in the Tele2 case stated: « Let us suppose, first of all, that a person who has access to retained data wishes to identify all the individuals in the Member State who have a psychological disorder. Analyzing the content of all communications effected within the national territory for that purpose would require considerable resources. On the other hand, by using databases of communications data, it would be possible instantly to identify all the individuals who have contacted a psychologist during the data retention period. I might add that that technique could be extended to any of the fields of specialist medicine registered in a Member State. Now let us suppose that that same person wished to identify individuals opposed to the policies of the incumbent government.

Again, analysing the content of communications for that purpose would require considerable resources, whereas, by communications data it would be possible to identify all individuals on the distribution list of emails criticising government policy. Furthermore, such data would make it possible to identify individuals taking part in any public demonstration against the government." Targeted surveillance is focused on persons who have already been identified as criminal. Targeted surveillance gives to authorities the access data relating to communications effected by individuals thus identified, even if accessing the content of their communications.

However, the key point is that access is limited to communications made after person have been identified in connection with serious crime. In contrast, general data retention relate to all users communications without any connection with serious crime. Moreover, these obligations give authorities access to the communications history of persons who have not yet been connected with serious crime or terrorism. In this case general data retention obligations give law enforcement access to the past, allowing them to access communications made by users before committing any crime. The role of ISPs is very important to the security and integrity of a data retention system. Even in a system would be reduced to correspond Tele2 ruling, ISPs will continue retaining data in connection with the prevention and prosecution of serious crimes. In the result, they will continue to play an important part in the process where retained data may be accessed for some purposes by authorities.

That is why, it is essential that their powers and duties should be regulated and monitored. As Joe McNamee, Executive Director of European Digital

Rights mentioned: « It is time for EU Member States to start respecting the law. It is time for the European Commission to do its job to ensure that the law is respected. How many times does the Court need to be asked the same question before EU Member States start listening? Data retention is an extreme measure which can only be implemented if the criteria repeatedly laid down by the Court are respected.» 3. Other countries implementation exampleWhile the surveillance of communication traffic is a global phenomena, the legal and technological framework of its operation is different for each country.

In order to make a parallel to EU data retention, I would like to review current surveillance system in post soviet countries. According to statistics published by a NGO on the Russian Supreme Court, the number of legal telephone and email intercepts in Russia have doubled, from about 266, 000 intercepts in 2006 to almost 540, 000 in 2012. In the “ Tele2-countries”, SORM and corresponding devices are used in Croatia, Kazakhstan and the Baltics (but without actually calling it SORM). The systems and regulations varies from country to country, but they are built on the same Russian principle.

SORM (literally “ System for Operative Investigative Activities”) is the technical specification for lawful interception interfaces of telecommunications and telephone networks operating in Russia. The current form of the specification enables the targeted surveillance of both telephone and Internet communications. Initially implemented in 1995 to allow access to surveillance data for the FSB, in subsequent years the access has been widened to other law enforcement agencies. In July 2016, President

Vladimir Putin signed into law two sets of legislative amendments commonly referred to as the “ Yarovaya Law,», which by many Russian activists was describes as unacceptable and incompetent, as it make literally no distinction between Lawful Interception and mass surveillance by state intelligence authorities without court orders. The new regulations however will take effect on July 1, 2018. According to the amendments, Internet and telecom companies are required to disclose communications and metadata, as well as “ all other information necessary,” to authorities, on request and without a court order. Thomas J.

Reese, the chair of the U. S. Commission on International Religious Freedom, said that “ Neither these measures nor the currently existing anti-extremism law meet international human rights and religious freedom standards” and that the Yarovaya Law “ will make it easier for Russian authorities to repress religious communities, stifle peaceful dissent, and detain and imprison people. U. S. State Department spokeswoman Nicole Thompson wrote that: “ We believe that these new amendments will not better protect Russia’s citizens, but are rather part of a troubling Russian trend of intimidation and harassment of civil society and political activists.” The recent releases of Wikileaks revealed that the SORM infrastructure is developed and deployed in Russia with close cooperation between the FSB, the Interior Ministry of Russia and Russian surveillance contractors such as PETER-SERVICE with their « Deep Packet Inspection» systems.

In December 2015, The European Court of Human Rights ruled on a case on the legality of Russian SORM legislation. In a unanimous Grand Chamber decision, the Court ruled that Russian legal provisions “ do not provide for

adequate and effective guarantees against arbitrariness and the risk of abuse which is inherent in any system of secret surveillance.” It noted that this risk “ is particularly high in a system where the secret services and the police have direct access, by technical means, to all mobile telephone communications.» It ruled that therefore, the legislation violated Article 8 of the European Convention on Human Rights. 4.

Practical implicationsSo in order not to descend to Nineteen Eighty-Four « Big Brother» concept, EU authorities should develop data retention law with personal privacy in mind. The European Commission has already proposed a revised version of the law, which is currently being debated by EU member states. The proposals already seek to address some of the issues pointed out by the court, such as giving more precise instructions on what the retained data can be used for and when authorities are allowed to access it. The main idea is to make a law which will correspond with the public view on privacy, and absence of constant surveillance sense. To make an adequate bill both ISPs, law enforcement and cilil right fighters should conclude a dialogue, in which all stakeholders would be satisfied. Firstly all serious criminal offenses which could be a reason for surveillance should be reviewed and redetermined: A reference to serious crime was included in the draft, the 32 offenses listed in the EU legislation on the European Arrest Warrant. The Council compromise specifies that member states “ shall have due regard” to that list and crime involving telecommunication. Secondly Service Providers’ volume of the obligations to retain the communications data of subscribers without their consent should be reduced.

The existing forms of automatic retention of private communications data cannot be implemented with European law. The retention can only occur, exceptionally. Advocate General stated: « I would emphasize that the risks associated with access to communications data (or ‘ metadata’) may be as great or even greater than those arising from access to the content of communications ..

. In particular, as the examples I have given demonstrate, ‘ metadata’ facilitate the almost instantaneous cataloguing of entire populations something which the storage of the content of communications does not» So the content of captured data should be explicitly defined. Also the EU officials should not abuse their authorities to spy on some professional minorities such as journalists, in order to control investigative journalism.

As already stated, from the Tele2 case conclusions, EU law now requires the application of a whole range of safe measures which govern access by State authorities to any system for the general retention of communications data. While these measures are designed to protect the rights of all citizens including journalists, some of them might be considered of particular significance for the protection of journalistic sources etc. Finally, it should be noted that the Tele2 decisions has important implications for the data storage and disclosure system, whose liability has been reduced with a direct ban on general and non-selective retention.

Even a system that has been redesigned to take into account a complete ban must have a number of guarantees to ensure that its disclosure mechanisms correspond to the basic rights to achieve legitimate aims. That

apply to data storage, the criteria for accessing data and independent control of the data storage and disclosure systems. ConclusionSo the indiscriminate collection of data by telecom operators still remains incompatible with the EU law, and needs some further research to find balance between combating crime and obligation to retain data. The new directive should contain clear and precise rules governing the allowed extent of interference with the fundamental rights for privacy and other Fundamental Rights of the EU to ensure that such interference is limited only to what is strictly necessary.

Such data retention requirements not only interfere with fundamental rights, but also are very costly as requires data centers maintenance.” National laws regulating what would constitute the necessary, legitimate and proportional State involvement in communications surveillance are often inadequate or non-existent. Inadequate national legal frameworks create a fertile ground for arbitrary and unlawful infringements of the right to privacy in communications and, consequently, also threaten the protection of the right to freedom of opinion and expression.” Communications Act 2011 is already irrelevant, so currently there is no legal power to force ISP to collect their customers data. The Tele2 case judgment, took into account international best practices and standards, when setting the criteria, safeguards and practices which should be observed by a Member State. However it also should be notable the decision in Tele2 does not keeps EU states from fighting against serious crime and terrorism. As we have seen, the effect of the Tele2 apart from limiting the abilities of the system, the

force also applies to all national systems of communications data retention and disclosure.

With this decision, the Court makes specific requirements for national data retention laws. The requirements show how seriously data retention practices interfere with EU fundamental rights and the need to establish adequate protection. These ptotection means need to be clearly stated in national law, and must govern the access of authorities to the retained data. We should also takes every opportunity to strengthen the rights to privacy and protection of personal data.