The Relation between Privacy and Security in Data Retention – An Overview of Certain Percentage of Croatian Citizens' Opinion

J. Levak[1, 2], and D. Osterman[2]
[1]*Faculty of Law, University of Zagreb.*
[2]*University of Applied Sciences Velika Gorica.*
jelena@rinigard.com

***Abstract*—The aim of this paper is to define citizens' views on the use of telephone call lists and location (without content), i.e. the retention of, and access to retained data about, telecommunications traffic by the police for the purpose of preventing and detecting offenders, and searching for missing persons and objects. The research aimed to answer the question of whether the ruling of the Court of Justice of the European Union (CJEU), by placing the right to privacy before the right to security, took into account the rights of victims of crime and the humanitarian aspect of saving people and property; and to identify acceptable data protection measures, transparency, and control mechanisms to access the data. The data were collected through an online questionnaire between September 25, 2018 and November 13, 2018 on a sample of 252 subjects, and then processed using the PASW Statistics 18.0 statistical package. The results show that both security and privacy are equally important to citizen. The results also showed that under clearly defined conditions, citizens find it acceptable to restrict privacy in order to maintain a satisfactory level of security. It was also evident that citizens do not see police as someone potentially misusing the retained data, but they think that the problem lies in the protection of data by telecommunications service providers and the transparency of checking access to retained data.**

***Index Terms*—Court of Justice of the European Union; Retention of Electronic Communications Data; Right to Privacy; Security.**

I. INTRODUCTION

It has been a common understanding among the police of all EU countries that data retention of electronic communication and access to this information are of great importance for the purposes of investigation and prosecution, and thus for effectively combating crime [1]. Furthermore, it is important to note that, consequently, the Court of Justice of the European Union (CJEU) rulings took into account only the human rights protection segment and not the protection of victims of serious crimes such as abduction, human trafficking or murder, detection of perpetrators, humanitarian aspect of searching for missing persons, and breaching of national security.

The numerous terrorist attacks in recent years have directed proper attention to data retention of electronic communications by providers of telecommunications services as a tool for protecting national security and solving crimes. Possession of data on electronic communication is a very powerful tool in fighting against crime, but at the same time it represents a great responsibility in terms of the collecting and safeguarding information, without interfering with the fundamental rights guaranteed by the Charter of Fundamental Rights of the European Union (CFR) [2].

The judgement of the Court of Justice of the EU in Joined Cases C-203/15 and C-698/15 (Tele2 and Watson) [3] substantially disrupts the security system of the EU and its Member States, as well as individuals, by restricting the work-space of law enforcement bodies to prevent and investigate crimes, and humanitarian work in the field of search and rescue. At the same time, the ruling does not provide any realistic guidance to ensure the continuing efficient work of the law enforcement, but rather indicates that they should anticipate execution of a crime or disappearance of a person. This approach by the Court of Justice indicates a fundamental lack of understanding of ways to protect the lives and property of citizens, as well as a great deal of mistrust and even the presumption of misuse of such information by law enforcement authorities.

II. DATA RETENTION – HISTORICAL DEVELOPMENT

The directive 97/66/EC on the processing of personal data and the protection of privacy in the telecommunications field was adopted in 1997. Subsequently, it had to be adapted to the developments in the markets and technologies of electronic communications services to provide an equal level of protection of personal data and privacy to users of publicly available electronic communications services. Regardless of the technologies used, it was replaced by the Directive 2002/58/EC on processing personal data and the protection of privacy in the field of electronic communications on July 12, 2002 [4].

It forms part of a package of telecommunications regulations, known as the Privacy and Electronic Communications Directive. Primarily, it relates to processing of personal data when delivering a communication service. In its introductory part, it states that new advanced digital technologies are being introduced into public communications networks, leading to specific requirements regarding the protection of personal data and user privacy. The development of the information society is characterized by the introduction of new electronic communications services, and access to digital mobile networks has become available and acceptable to the general public.

The Directive states that Member States must, according to their national legislation as well, ensure the confidentiality of communications transmitted over a public electronic

communications network. Listening, recording and storage of communication data must be expressly prohibited to non-users without the consent of the said users. The Directive stipulates that traffic data and location data must be deleted or made anonymous after they are no longer needed for communication or billing purposes (business purposes), unless the subscriber has given his or her consent for another use. Among other things, Article 15 (1) states: "Member States may adopt legislative measures to restrict the scope of the rights and obligations... when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defense, public security, prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system, as referred to in Article 13 (1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6 (1) and (2) of the Treaty on European Union."

Subsequently, in 2006, the Directive 2006/24/EC, on the withholding of information obtained or processed in connection with the provision of publicly available electronic communications services or public communications networks (the Data Retention Directive [5]), was adopted with the main objective of harmonizing the provisions of the Member States related to obligations to retain certain information collected or processed by providers of publicly available electronic communications services or public communications networks. In doing so, it ensures the availability of such data for the purposes of prevention, investigation, detection and prosecution of serious criminal offenses, such as criminal offenses related to organized crime and terrorism. The Directive thus stipulates that these providers must retain traffic and location information as well as related data necessary to identify subscribers or users. However, it does not allow the retention of communications content and information accessed. The key provisions of the Directive are: the obligation to retain data (Article 3) and access to data (Article 4) and the categories of data to be retained, the duration of the retention and the scope.

Following its adoption, the Directive has been constantly criticized by various stakeholders (service providers, the European Data Protection Supervisor, and various civil society organizations), leading to a series of lawsuits raising the question of the lawfulness of data retention measures before national courts [6].

In 2014, the EU Court of Justice ruled in joined Cases C-293/12 and C-594/12 (Digital Rights Ireland and Seitlinger et al. [7]), that the Data Retention Directive was invalid because it disproportionately restricts the rights guaranteed by the EU Charter of Fundamental Rights - the right to respect private and family life, home and communication (Article 7), and the right to personal data protection (Article 8). The CJEU considers that EU law prevents general and indiscriminate withholding of traffic and location data. The Court, however, provides that Member States are free to regulate retention of information in a targeted manner for the purpose of combating serious crime. However, such retention should be limited to what is strictly necessary, with regard to the categories of information to be retained, the means of communication to which it relates, the persons concerned and the duration of detention chosen. Access by national authorities to the retained data must be subject to constraints, including prior review by an independent body and that the data be stored within the EU.

Furthermore, the judgments stipulate that national legislation must be clear and precise and provide sufficient guarantees to protect the data against the risk of misuse. Legislation must indicate under what circumstances and under what conditions a data retention measure can be adopted as a preventive measure, ensuring that the extent of that measure in practice is limited to what is strictly necessary. Such legislation must be based on objective evidence that enables the identification of persons whose information may reveal a link to possible serious crime, thereby contributing to the fight against serious crime or to preventing a serious risk to public safety.

In a ruling of December 2016, the CJEU, in its two joined cases C-203/15 and C-698/15 (Tele2 and Watson) interpreted that any national regulation which, in order to combat crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users with respect to all electronic communications, contradicts the directive on privacy and electronic communications, i.e. that it is opposed by any national regulation governing the protection and security of traffic and location data, and in particular the access of the national authorities to the retained information where the purpose of that approach in the fight against crime is not limited to the fight against serious crime, and where that approach is not subject to the prior scrutiny of a court or an independent governing body.

Annulment of the Data Retention Directive by the Court of Justice has created a state of legal uncertainty, in particular with regard to the legal statuses of the national legislations through which the directive and the very availability of such information was transposed to law enforcement authorities and their use as evidence in criminal proceedings. In a number of judgments (C-362/14, C-582/14, C-203/15 and C-698/15, C-293/12 and C-594/12), the Court of Justice has accentuated a proactive stance on ensuring data protection. The Court found that the Directive had achieved a legitimate aim in the fight against serious crime and the protection of national security, but that safeguards to protect privacy and a sufficient level of data protection were not sufficiently provided.

EU Member States that are no longer obliged by such a decision of the EU Court of Justice, under the specific legal instrument of the Union to introduce or maintain a national data retention regime, have approached the ruling differently. Some maintained the current state of affairs, while others moved to amend, replace or repeal the legislation transposing the directive, or repealing it by national courts. The EUROJUST [8] reports following the aforementioned judgments of the Court of Justice showed that, while some countries do not have specific legislation on mandatory data retention, the vast majority of countries do have one. Furthermore, no country has legislation containing all the specific criteria laid down by the Court of Justice of the European Union (the requirement that retention of information be permitted only in a targeted manner for the purpose of combating serious crime, with respect to the categories of data to be retained, the means of communication to which it applies, the persons to whom it relates and the length of the retention period). All states have provisioned

some form of access restriction, which seeks to balance the need for access in the interests of criminal investigations and prosecutions against citizens' rights.

Following the case-law of the EU Court of Justice, it is no longer possible for general and indiscriminate retention of data, both at EU and national levels. With such an interpretation, we can conclude that certain national legislations which retain such arrangements are contrary to EU law and the EU Charter of Fundamental Rights, as consequently confirmed by the subsequent rulings of their national courts (https://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention. For example, BE- June 11 2015, (https://www.const-court.be/public/f/2015/2015-084f.pdf), NL- March 11 2015 (https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2015:2498).

One of the main concerns raised by law enforcement agencies regarding the collection of evidence is the unavailability of data (not stored or secured by telecommunication service providers and Internet service providers). All of this could lead to the cessation of ongoing investigations and prosecutions, as well as contesting the admissibility of evidence at a later stage. Data retention is an essential investigative/prosecutorial tool in the fight against serious crime and terrorism, however, the ruling of the EU Court of Justice, sets before the law enforcement authorities the impossible task of identifying or targeting certain electronic data that may become evidence in criminal prosecution, because it presupposes measures of crime prediction before they occur.

III. Working At The Level Of EU Working Bodies Regarding Data Retention After The Judgment Of The EU Court Of Justice In The Case Of Digital Rights And Tele2

Joint work at EU level on data retention issues began during the Maltese presidency [9] with the aim of assisting Member States in analyzing the requirements arising from the case-law of the EU Court of Justice. Following the initial idea, the Estonian Presidency decided to move the deadlock and raise the issue to the level of the Ministries of Justice at the informal meeting of justice and home affairs ministers in Tallinn on 6th-7th of July 2017, who decided to entrust this task to the Working Party on Information Exchange and Data Protection (DAPIX), but in the informal composition of Friends of Presidency.

It was then decided that the focus of the work group should be: 1. ensuring the availability of data (in line with the draft of the e-Privacy Regulation [10]), 2. establishing safeguards regarding access to retained data based on strict verification of necessity and proportionality and 3. limiting the scope of the retention framework to recent case law [11].

Also on this occasion, the EU Counter-Terrorism Coordinator and EUROPOL introduced additional elements through concepts of restricted data retention and targeted access. Although some Member States on this occasion called for the European Commission to design and propose a new EU data retention legal instrument to ensure a common EU-wide reference framework, i.e. legal certainty and predictability of the legal framework, most delegations nevertheless supported the continuation of joint efforts in examining general principles and special elements for a simple reason - lengthy legislative procedures that do not help Member States, which currently do not have data retention legislation in place, adopt measures at the national level concerning data retention in relation to prevention and prosecution of criminal offenses. Work continued at the same intervals (3 to 4 meetings per presidency) during the Bulgarian, Austrian and Romanian Presidencies.

Due to the fact that many Member States are currently reviewing their domestic legislation to design retention regimes that meet the requirements of the court rulings, and due to the large number of different variables that emerge, there is a strong potential for continued legislative inconsistency within the European Union on this issue. Therefore, further consideration of a common understanding of the requirements arising from the judgment of the EU Court of Justice at EU level is needed, with consideration to what extent a common data retention framework would be useful for preventing and combating crime.

IV. Legislation Of The Republic Of Croatia

Following the repeal of the Directive, the Republic of Croatia has maintained the existing legislation in this field. With amendments made to the Code of Criminal Procedure in 2002, in Art. 177 (2), a precisely defined authority emerges for the first time, whereby law enforcement may request the legal entity of a telecommunications service provider to verify the equivalence of telecommunication addresses that have established a connection during a specified period, while before that, access to retained information was exercised pursuant to the same article of the Code of Criminal Procedure from 1997, that is, the part relating to other necessary measures and actions. In the coming years, data retention and telecommunications surveillance were defined by a series of legal regulations up until 2014. These regulations fully ensure data retention, data access policies, and control of the application of this power, which is the basis for the interpretation that the Republic of Croatia, in the regulations and procedures of access and protection below, is fully in line with the judgment of the Court of Justice.

The legal acts defining this issue in the Republic of Croatia are as follows:

- Code of Criminal Procedure (NN 110/97, 58/02, 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13 and 152/14),
- Law on police duties and powers (NN 76/09 and 92/14),
- Law on Security and Intelligence System of the Republic of Croatia (NN 79/06 and 105/06),
- Law on electronic communications (NN 73/08, 90/11, 133/12, 80/13 and 71/14),
- Regulation on obligations in the area of national security for the Croatian legal and natural persons in telecommunications (NN 83/03, 64/08 and 76/2013),
- Telecommunications Law (NN 122/03),
- Law on Security and Intelligence System of the Republic of Croatia (NN 79/06 and 105/06),
- Defense Law (NN 73/13),
- Rules on military and police affairs and the implementation powers of authorized officers of the Military Police (NN 44/2014).

An important factor in the changes was the establishment of the Operational-Technical Center for Telecommunications Surveillance (OTC) described in the Law on Security and

Intelligence System of the Republic of Croatia [12], which was defined as a technical body that activates and manages the measure of covert surveillance of telecommunications services, activities and traffic, and acts as a coordinating body between public telecommunications operators and law enforcement authorities. The establishment of this body made it possible to harmonize the rights and obligations regarding the storage, access, transfer and security of retained information.

V. Research Of Citizens' Attitudes On The Need Of Data Retention And Access To Retention Data

A. Research Goal

The aim of this research was to investigate citizens' views on the use of telephone listings and location (without content) by the police in order to prevent and detect offenders and to search for persons and cases, without analyzing legislation.

In this sense, the citizens were asked their opinion about the need to retain electronic communications data, about the legal access to this data, ways of safeguarding the procedure and its transparency, and trusting the bodies involved in the process of data retention and accessing the retained data.

B. Methodology

Although the judgment applies to the entire EU, the intention is to examine the opinions of the citizens of the Republic of Croatia, not with regard to the judgment itself, but only with regard to the retention of data to which the judgment relates, access to that information by law enforcement authorities, and safeguarding and transparency of the data access procedure. Data were collected by using snowball sampling method, and access was given to respondents by sending an e-mail with a link to the questionnaire, targeted at non-judicial and law enforcement contacts. The questionnaire was also posted on a Facebook group, "Questionnaires for papers and research", which has over five hundred members from all over the Republic of Croatia.

C. The Sample

Online data collection was conducted between September 25, 2018 and November 13, 2018. Participation in the survey was voluntary and anonymous, and respondents were able to opt out of the survey at any time. Of the total number of participants (N = 252), 175 (69.4%) were men and 77 (30.6%) women. The largest number of participants, 135 (53%), resided in a major city, 72 (28.6%) participants in a smaller city, and 45 (17.9%) in a village/settlement. The largest number of participants, 96 (38.1%) have a university degree, 74 (29.4%) have a college degree, 80 have a high school diploma, and 2 (0.8%) have completed primary school. In regards to the amount of monthly income, 51 (20.2%) participants stated that they had no income, 14 (5.6%) participants were in the range of up to 2.000 HRK, 13 (5.2%) in the range of 2.000,00 – 4.000,00 HRK, 52 (20.6%) participants in the range of 4.000,00 – 6.000,00 HRK, 61 (24.2%) participants in the range of 6.000,00 – 8.000,00 HRK, 41 (16.3%) participants in the range of 8.000,00 – 10.000,00 HRK, and 20 (7. 9%) of participants in the range of more than 10.000,00 HRK.

Particular attention was paid to the affiliation of the respondents to law enforcement bodies in the Republic of Croatia, which include police, public prosecutor's office, judicial bodies, and an additional category made up of attorneys dealing with the issue of retaining electronic communications data in private practice. The results show that majority of participants, 193 (76.6%), are not members of judicial or other law enforcement bodies (including lawyers), while 59 (23.4%) belong to the mentioned category, which is also important for the research itself. This ratio among respondents was targeted because the survey itself was focused on the general population, with intention of acquiring objective answers, while on the other hand, there should be a sample of members of the judiciary and law enforcement bodies to compare the overall results when asked about the reasons for withholding data in relation to the results of the respondents who are not members of this group, that is, only the main target population. A specific analysis of the comparison of the results between the two groups is not foreseen for this paper and will be further elaborated in the second stage of data processing.

D. The Questionnaire

The questionnaire was designed specifically for the purposes of this research. The questionnaire consisted of two parts. The first part of the questionnaire consisted of seven socio-demographic questions, and the second part of the questionnaire contained eight questions on attitudes related to the retention of communications data for the purpose of preventing and detecting perpetrators of criminal offenses, and search for persons and objects. Five questions were closed-ended (multiple-choice questions), while two questions assessed respondents' degree of agreement on a Likert-type scale, ranging from 1 = strongly agree, to 7 = completely disagree. In addition to questions about attitudes toward withholding communication information, respondents were also asked whether or not they were members of judicial or other law enforcement agencies, including attorneys. The questionnaire also contained informed consent to participate in the research, and a brief text on the legal regulations on data retention by the communication service providers and the relevant provisions of the Code of Criminal Procedure and the Law on Police Affairs and Powers. Also, in order to ensure a proper understanding of all questions asked, the questionnaire contained shorter definitions of some terms such as encryption and pseudonymization of data.

VI. The Results

Table 1 shows the participants' answers to the question whether there is a reason for communication providers to retain communication data so that the police can access them, if necessary, for the purpose of detecting offenders or searching for persons and objects. Out of the total number of participants, 48% believe that such reasons exist, 16.3% think that such reasons do not exist, while 34.9% think that such reasons could exist.

Table 1
Distribution of Participants with Regard to Their Attitude About Reasons for Communications Service Providers to Retain Data on Communication

Answer	Frequency	Percentage	Cumulative Percentage
Yes	123	48.8	48.8
Could	88	34.9	83.7
No	41	16.3	100.0
Sum	252	100.0	

Question: "Do you consider that there are reasons for communications providers to retain communication data (call list, location ...) so that the police can access them, if necessary, for the purpose of identifying the perpetrators of crime or when searching for persons and objects?"

Table 2
Distribution of Participants, Who Are Not Members of the Judiciary and Other Law Enforcement Bodies, Including Lawyers, with Regard to Their Attitude About Reasons for Communications Service Providers to Retain Data on Communication

Answer	Frequency	Percentage	Cumulative Percentage
Yes	75	38.9	48.8
Could	80	41.5	83.7
No	38	19.7	100.0
Sum	193	100.0	

Table 2 shows the participants' answers, who do not belong to law enforcement authorities in the Republic of Croatia, which includes the police, prosecutors, judicial authorities and private practice lawyers dealing with the issue of data retention of electronic communications, to the question whether there is a reason for communication providers to retain communication data so that the police can access them, if necessary, for the purpose of detecting offenders or searching for persons and objects. Of the total number of participants, 38.9% felt that such reasons existed, 19.7% thought that such reasons did not exist, while 41.5% believed that such reasons could exist. It can be seen that the percentage of 'Yes' to this question is 38.9%, compared to 48.8% in Table 1, which shows the distribution of the whole sample, suggesting that law enforcement officials are more inclined to give a positive answer on justification of the retention of communication data by the communications service provider. However, for any general conclusions, it is necessary to carry out additional data analysis and comparisons of these groups of participants.

Question: "Do you consider that there are reasons for communications providers to retain communication data (call list, location ...) so that the police can access them, if necessary, for the purpose of identifying the perpetrators of crime or when searching for persons and objects?"

Table 3
Allocation of Participants with Regard to Reasons for Not Having Reasons to Withhold Communication Information by the Communication Service Provider

Answer	Frequency	Percentage	Valid Percentage	Cumulative Percentage
I believe that the police is misusing that information	5	2.0	13.2	13.2
The information provided by the service providers is not sufficiently protected	14	5.6	36.8	50.0
Access to police data is not controlled by an independent body	3	1.2	7.9	57.9
There is no transparent way to verify access to data	4	1.6	10.5	68.4
Sum	12	4.8	31.6	100.0
No Answer	38	23.8	100.0	
Sum	192	76.2		

Table 3 shows the frequencies of participants' responses to the question why they believe that communication providers should not withhold communication information. Of these, 14 (36.8%) felt that data was not sufficiently protected by service providers, 12 (31.6%) of participants believed that there was no transparent way of verifying access to the data, 5 (13.2%) of participants believed that the data was misused by the police, 3 (7.9%) believe that access to police data is not controlled by an independent body, and 4 (10.5%) participants believe that access to police data is not authorized by an independent body.

Question: "If the answer to the previous question is NO (question in Table 1) - the data should NOT be withheld because:"

Table 4
Allocation of Participants with Regard to the Possibility of Changing Their Opinion on the Acceptability of Communication Data Retention by the Communication Service Provider

Answer	Frequency	Percentage	Valid Percentage	Cumulative Percentage
Strong yes	8	3.2	19.5	19.5
Yes	7	2.8	17.1	36.6
Undecided	15	6.0	36.6	73.2
No	4	1.6	9.8	82.9
Strong no	7	2.8	17.1	100.0
Sum	41	16.3	100.0	
No Answer	183	72.6		

It is interesting to note in Table 4 that 36.6% of participants stated that they would change their minds (19.5% - Strong yes, 17.1% - Yes) under the terms of data protection guarantee, access control and transparency of access verification, while 26.9% of participants stated they would not change their minds (9.8% - No, 17.1% - Strong no). A neutral response (undecided) was given by 36.6% of participants.

Question: "If the answer to question 9 is NO - would you change your mind about giving the police access to the information, provided they have sufficient guarantees for data protection, access control and transparency of access verification?"

Regarding the frequency of response to the preferred data retention time by the communication service provider, Table 5 shows the response frequency to the preferred data retention time by the communication service provider. The largest number of participants (45%) felt that this time should be 12 months, 30.6% stated a longer period of time (23.8% -18 months, 5.2% - 24 months, 1.2% - 36 months). 0.4% - 60 months), while 24.2% of participants reported a shorter time period (0.4% - 9 months, 10.7% - 6 months, 10.3% - 3 months, 0.4% - 1 month, 2.4% - 0 months).

Question: "Croatia has a statutory retention period of 12 months for all communication data of all service users. Do you think this period should be:"

Table 5
Frequencies of Response to Preferred Data Retention Time by Communications Service Providers

Months	Frequency	Percentage	Cumulative Percentage
0	6	2.4	2,.4
1	1	0.4	2.8
3	26	10.3	13.1
6	27	10.7	23.8
9	1	0.4	24.2
12	114	45.2	69.4
18	60	23.8	93.3
24	13	5.2	98.4
36	3	1.2	99.6
60	1	0.4	100.0
Sum	252	100.0	

Table 6
Frequencies of Response to Preferred Data Retention Time by Communications Service Providers

Answer	Frequency	Percentage	Cumulative Percentage
Access via username and password	40	15.9	15.9
Coding/Database Encryption	40	15.9	31.7
Pseudonymization of data	15	6.0	37.7
A combination of at least two of the above methods	157	62.3	100.0
Sum	252	100.0	

With respect to the distribution of participants according to the type of minimum acceptable level of protection of personal data from Table 6, it is evident that the majority of participants (62.3%) chose the option of combining the minimum of the two mentioned methods of data protection, 15.9% of participants chose the method of using the username and password, 15.9% of the participants chose the coding/database encryption, and 6% of the participants chose the pseudonymization method of the data. In order to ensure the respondents' understanding of these terms, they were briefly explained in the questionnaire.

Question: "Police access to communications data stored with telecommunications service providers is statutory, and operator data is protected by various physical and software protections. What minimum level of service provider protection would be acceptable to you?"

Table 7
Distribution of Participants According to Their Level of Agreement About the Ability to Check Whether the Police Accessed Their Personal Data

Answer	Frequency	Percentage	Cumulative Percentage
Strong yes	102	40.5	40.5
Yes	39	15.5	56.0
Undecided	61	24.2	80.2
No	17	6.7	86.9
Strong no	33	13.1	100.0
Sum	252	100.0	

The distribution of participants according to the level of agreement with the ability to verify access to their own data by the police in Table 7 shows that 56% of participants believe that users of telecommunications services should be able to verify access to their own data by the police through an independent body using an Internet platform where access can be verified (Strong yes - 40.5%, Yes - 15.5%), 19.8% of them believe that users should not have access to this data (No - 6.7%, Strong no – 13.1%), while 24.2% of participants gave a neutral response.

Question: "Do you think that as a user of telecommunications services you should be able to verify access to your data by the police through an independent body using an Internet platform where access can be verified?"

Table 8
Distribution of Participants According to the Time Period of the Ability to Verify Access to Their Own Data

Answer	Frequency	Percentage	Valid Percentage	Cumulative Percentage
At any moment	134	53.2	55.8	55.8
Immediately upon completion of the investigation	64	25.4	26.7	82.5
One year after the access if the investigation has already been completed	29	11.5	12.1	94.6
Two years after the access, regardless of the course of the investigation	13	5.2	5.4	100.0
Sum	240	95.2	100.0	
No answer	12	4.8		
Sum	252	100.0		

Regarding the distribution of participants according to the time period of the ability to verify access to their own data from Table 8, it can be seen that the largest percentage of participants (55.8%) felt that users should be able to check access to their own data at any moment, 26.7% considers that this possibility should be available immediately upon completion of the criminal investigation, 12.1% of them believe that this possibility should be available one year after the completion of the criminal investigation, and 5.4% believe that this possibility should be available two years after the check has been carried out regardless of the course of the criminal investigation.

Question: "If you had the ability to perform this verification of access to your data, when do you think you should be able to perform this verification?"

Based on the results obtained, it can be argued that the majority of participants consider that there are justifiable reasons for communication service providers to retain communication data, while insufficient level of data protection by service providers and the lack of transparency in how to check access to data are most commonly cited by the opposing opinions.

VII. DISCUSSION

The relatively high proportion of 83.7% of participants, seen from Table 1 above, who believe that reasons for withholding information may or may not exist, indicates a greater propensity for privacy by the citizens of the Republic of Croatia. These results suggest that solutions need to be found that will enable law enforcement authorities to carry out these types of checks, with sufficient elements of privacy protection and the prevention of abuse. The data in this table is further confirmed by the data in Table 2, which excludes members of the judicial authorities, law enforcement bodies in the territory of the Republic of Croatia and lawyers, since members of these groups may be subjective to this information, but could not be completely avoided during conducting a survey.

Based on these results, we can conclude that the judgments of the EU Court of Justice have not sufficiently taken into account the desired level of security, especially at a time of increased terrorist activity in the EU. There certainly are reasons to be concerned about privacy, but privacy should not deprive or substantially restrict the right to security. The guidelines that the judges followed in reaching the verdict could have repercussions on other security systems, especially those related to public infrastructure surveillance, all for the pursuit of a greater right to privacy. The complete abolition of data retention could give offenders 'open hands' to use the public information and communication infrastructure for the purpose of committing, preparing or organizing any criminal offense, which can result in a significant increase in insecurity.

In all Member States, national authorities have the power to review the safeguards of electronic communications providers regarding data retention. This could even support the claim that such monitoring of guarantees by an independent body could be used as an argument to defend national data retention legislation. The retention regime, in order to be in line with EU law, should therefore contain a provision on the review of compliance with safeguards by an independent national body. This is explicitly stated by the EU Court of Justice in the Tele2 ruling [13].

Furthermore, in both rulings (Digital Rights and Tele2), the Court of Justice criticized the lack of rules governing the procedural criteria under which retained information can be accessed. In its judgment, the EU Court calls on Member States that "national legislation must first set out clear and precise rules governing the reach and application of such a retention measure, and prescribe minimum conditions so that persons whose data are retained have sufficient safeguards to enable effective protecting of their personal information against the risk of misuse" [14].

According to the Court of Justice, "it is essential that access to the retained data by national competent authorities is in principle, except in duly justified urgent cases, subject to prior scrutiny by a court or an independent administrative authority, and that the decision of that court or authority is made following a reasoned request from the national authorities, submitted in particular under procedures for the prevention, detection or prosecution of criminal offenses" [15].

The vast majority of Member States have such safeguards in place that are in accordance with the prerequisites established by the EU Court of Justice, either through prior court surveillance or prosecutorial supervision. For emergency situations, special conditions apply, where notification or ex post approval by the aforementioned bodies is considered sufficient. Therefore, the distribution of survey participants with regard to reasons for not having reasons to withhold communication data by the communication service provider, in Table 2, is not surprising because it shows that citizens consider that, as the leading reason for opposing data retention (36.8%), data provided by the service providers is not sufficiently protected.

Regarding the prior judicial approval or approval of an independent governing body, when it comes to the non-urgent research phase, there should be no adverse effect on the conduct of the law enforcement authority. Moreover, such approval can only add to the greater responsibility in the exercise of this authority.

However, the prior authorization procedure must respect the urgency of conducting the research and should in no way adversely affect the retention of retained information, especially in the case of data retained temporarily by providers due to the large amount of the same or technological limitations.

Any authority that assumes the responsibility of prior authorization should in any case acknowledge and adapt to the way law enforcement authorities act. This additional step must slow down the process of accessing retained data.

Regarding the frequency of responses to the preferred data retention time by the communication service provider, the largest number of participants (45%) felt that this time should be twelve months, which is in line with the current regime of data retention and access to retained data in the Republic of Croatia, as is in most other Member States with effective data retention regime. When examining the situation in this regard in other Member States, it can be observed that the length of the retention period was not a central issue in the consideration of their national courts or was not at all questionable. The Court of Justice's considerations in the Tele2 judgment are scarce on this point, since they are limited to the claim that the adopted retention period should be limited to what is "strictly necessary" [16].

The proposal to store retained information in encrypted form or to protect it through pseudonymization does not come directly from the Digital Rights or Tele2 judgments, but emerged as one of the Estonian Presidency's debating motions to meet the EU Court's request for minimum safeguards [17]. Only a small number of Member States have such practices, while national legislations of other Member States do not provide for detailed or descriptive security measures.

At present, there is no obligation to report to the person who was the subject of access to his or her retained information. Such a reporting obligation would not be a useful approach, but using the benefits and capabilities of information and communication technologies, it would be possible to implement a solution that would allow for easy and rapid verification in situations where there is no risk to criminal investigations under well-defined conditions. Such an option would not have a direct impact on the work of law enforcement authorities or endanger criminal investigations in progress, while on the other hand it would allow transparency and increase citizens' confidence in law enforcement authorities.

Although the majority of research participants, 55.8% of them believe that access to retained data should be done at any time, from the point of view of the law enforcement

authorities as well as the legislation, this would not be possible so we can transfer this percentage of replies to the answer category "Immediately upon completion of the criminal investigation", which would total 82.5% of participants, or 198 of them. These results, when viewed from the privacy perspective, are completely understandable and this type of verification certainly contributes to the transparency and legality of the verification.

VIII. Conclusion

Considering that the legislature in the Republic of Croatia did not consider it necessary to start amendments or repeal of the Law from the moment of the rendering of the judgments, we can conclude that the retention of the data and access to the retained data in the Republic of Croatia is completely in accordance with the judgments of the EU Court of Justice, especially when organized crime, terrorism and threats to public and national security are in question. This research into citizens' interest in incorporating additional safeguards and greater transparency confirms that citizens are interested in certain shifts in transparency and additional safeguards that are possible, and would be well received.

The research results also clearly show that, in its judgments, the EU Court did not take into account the safety of citizens, and their appetites in terms of safety with respect to privacy, the right of victims to find the perpetrators and serve justice, nor the humanitarian aspect of search and rescue operations for missing persons. The Court also limits the possibilities of investigating and preventing criminal offenses without providing clear guidance on how to strike a balance between security and privacy, that is, we can freely state that it has been easier and simpler for the Court to ban access to the data. Instead of finding a satisfactory solution or guidance, it set an impossible task of anticipating the commitment of criminal offenses. Such crime prediction would require law enforcement authorities to have tools in place that would anticipate the conduct of persons, the preparation or organization of criminal offenses or terrorist acts.

Driven by discussions and opinions expressed during the work of the Friends of the Presidency Working Party within the Council of the European Union and the European Commission's [18] inertia regarding the retention of electronic communications data after the repeal of the Data Retention Directive, the authors concluded that even the proponents of European legislation themselves are not ready to overcome the current status quo in the approach "Privacy vs. security", and they let national legislatures test it, which they had several times already, in their own courts, by using the method of trial and error. We are of the opinion that the shift will only happen when both approaches are equally satisfied and begin to act collectively as "privacy and security", with both rights being regarded as "rights that enable rather than end" [19].

This research, although limited to the territory of the Republic of Croatia, is in the wake of the most recent views expressed at the Justice and Home Affairs Council on December 6 and 7, 2018 [20]. Specifically, one Member State called on the European Commission to assist its national legislations and to carry out a comprehensive study on data retention from which possible solutions to this important issue could be derived, with the support of other Member States. In addition to emphasizing that work on this matter should continue, the European Commission listens and waits for the completion of several preliminary proceedings before the Court of Justice (Case C-511/18 and Case C-520/18).

In the meantime, it is also interesting to refer to Case C-207/16 on the request for a preliminary ruling from the Audiencia Provincial de Tarragona (Provincial Court of Tarragona, Spain). The said request for a preliminary ruling essentially concerned the interpretation of Article 15 (1) of Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002 on the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) communications) in connection with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. The request was lodged as part of an appeal initiated by Ministerio Fiscal (Attorney General, Spain), by lodging an appeal against the decision of the Juzgad de Instrucción n ° 3 de Tarragona (Investigation Court No 3 in Tarragona) denying police access to personal data held by electronic communications providers. On 2 October 2018, the Court of Justice (Grand Chamber) ruled that Article 15 (1) of Directive 2002/58/EC, as amended by Directive 2009/136/EC, in conjunction with Articles 7 and 8 of the Charter of the European Union on fundamental rights should be interpreted as meaning that access by national authorities to the identity information of SIM card holders activated by a stolen mobile phone, such as their first and last name and, where appropriate, the address of those holders, constitutes an encroachment on their fundamental rights recognized by the said articles of the Charter of Fundamental Rights, which is not so serious that this approach, in the context of the prevention, investigation, detection and prosecution of criminal offenses, should only be granted when it comes to combating serious crime. Such a ruling confirms the interpretation of law enforcement members that the ECJ judgement does not relate to the identification data of service users and thus should not even be discussed within the problem of access to retained telecommunication activity data.

In conclusion, it is important to emphasize additional security measures for databases that store such retained data using various security methods such as searchable encryption, pseudonymization/depersonalization, dual authentication, encryption or a combination of these methods. An innovative method of data protection would be to use software protection to force privacy and security settings regardless of who the data is being delivered to, or impose data owner policies on any other computer system, which would allow complete control over access and use of retained data.

References

[1] Council of the European Union, 9663/19 (OR. en), 27 May 2019, Conclusions of the Council of the European Union on Retention of Data for the purpose of Fighting Crime - adoption

[2] Charter of Fundamental Rights of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri= CELEX:12012P/TXT (accessed January 7, 2019)

[3] Judgment of the Court (Grand Chamber) of 21st of December 2016. Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others. Requests for a preliminary ruling from the Kammarrätten i Stockholm and the Court of Appeal (England & Wales) (Civil Division). Reference for a preliminary ruling — Electronic communications — Processing of personal data — Confidentiality of electronic communications — Protection — Directive 2002/58/EC — Articles 5, 6 and 9 and Article

15(1) — Charter of Fundamental Rights of the European Union — Articles 7, 8 and 11 and Article 52(1) — National legislation — Providers of electronic communications services — Obligation relating to the general and indiscriminate retention of traffic and location data — National authorities — Access to data — No prior review by a court or independent administrative authority — Compatibility with EU law. Joined Cases C-203/15 and C-698/15., available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62015CJ0203, (accessed on January 1, 2019)

[4] DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of July 12, 2002 on the processing of personal data and the protection of privacy in the field of electronic communications (Directive on privacy and electronic communications)

[5] Official Journal of the European Union, L 105/54, April 14, 2004, DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of March 15, 2006, on the withholding of information obtained or processed in connection with the provision of publicly available electronic communications services or public communications network and amending Directive 2002/58/EC

[6] Levak J., Osterman D., Protection, Retention and Exchange of Information Used by Law Enforcement Authorities and Possible Technical Solutions on Data Retention Following the Revocation of the Data Retention Directive by the Court of Justice of the European Union, Police and Security (Zagreb), year 26. (2017), issue 4, p. 342-364

[7] Official Journal of the European Union, C 175/6, June 10, 2014, Judgment of the Court (Grand Chamber) of April 8, 2014 (reference for a preliminary ruling from the High Court of Ireland, Verfassungsgerichtshof - Ireland, Austria) - Digital Rights Ireland Ltd (C-293/12), Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl et al (C-594/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General (Joined Cases C-293/12 and C-594/12)

[8] Council of the European Union, ST 10098/17 LIMITE, Brussels, 6 November 2017, Data retention regimes in Europe in light of the CJEU ruling of 21 December 2016 in Joined Cases C-203/15 and C-698/15-Report

[9] Council of the European Union, ST 6713/17 LIMITE, Brussels, 1 March 2017, Retention of electronic communication data - next steps

[10] FoP DAPIX Joint Meeting on Data Retention Formation and TELE (Working Group on Telecommunications and Information Society) in October 2017, opinions were exchanged concerning a new proposal for a draft of the e-Privacy Regulation. During 2018, two additional joint meetings were held to address the need to maintain flexibility under the new e-Privacy Regulation. Flexibility is recognized as a key element for future developments, either on the basis of the case-law of the Court of Justice or through legislative reforms at national or European level.

[11] Council of European Union document 14480/1/17

[12] Article 18 of the Law on Security and Intelligence System states: "In order to activate and manage the measure of covert surveillance of telecommunications services, activities and traffic, and to achieve operational and technical coordination between legal and natural persons who have a public telecommunications network and provide public telecommunications services and access services in the Republic of Croatia, and bodies authorized to apply telecommunications surveillance measures in accordance with this Act and the Criminal Procedure Code, shall establish an Operational and Technical Center for Telecommunications Surveillance (hereinafter: OTC)."

[13] Tele2 judgment, paragraph 123

[14] Ibid, para. 109

[15] Ibid, paragraph 120 (see by analogy, in relation to Directive 2006/24, judgment of Digital Rights, paragraph 62; see also by analogy, in relation to Article 8 of the ECHR, ECtHR judgment of January 122016; Szabó and Vissy v. Hungary, CE: ECHR: 2016: 0112JUD003713814, paragraphs 77 and 80.)

[16] Ibid, para. 108

[17] Council of the European Union, ST 14319/18 LIMITE, Brussels, 23 November 2018, Data retention-State of play

[18] It should be mentioned that the European Commission was already obliged in its COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL, in its Fourth Progress Report on the Establishment of an Effective and True Security Union (COM (2017) 41 final) of January 25, 2017, to draw up guidelines for the adoption of national laws on data retention that would comply with the judgment.

[19] United Nations (UN), Human Rights Council, Cannataci, J. (2016), Report on the Special Rapporteur on Right to Privacy, A / HRC / 31/64, 8 March 2016, p.9, paragraph 23., available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/262/26/PDF/G1626226.pdf?OpenElement, (accessed December 3, 2017)

[20] Council of the European Union, 15252/18 (OR. en), OUTCOME OF THE COUNCIL MEETING, 3661st Council meeting, Justice and Home Affairs, Brussels, 6 and 7 December 2018 https://www.consilium.europa.eu/media/37953/st15252-en18.pdf, (accessed March 17, 2019.