Croatian Model of Telecommunication Information Requests Management (TIRM)

Damir Osterman
National Police Office for Suppression of Corruption and Organised Crime, Ministry of the Interior

Damir Maračić
Police College Zagreb, Ministry of the Interior, Croatia[1]

Abstract
TIRM is an acronym for the Croatian model of Telecommunication Information Requests Management. It is an electronic application designed for the systematic requesting and issuing of electronic communication data, as well as the handling, processing, storage and use of data. TIRM application was developed and designed during the last three years of a process including the needs analysis, preparation, test, and implementation phases. It helps in the processes of authorisation and approval of requests, transferring and storage of data, and in the analytical processing. The paper presents and explains:
– Importance and values of the systematic requesting, issuing and managing of electronic communication information;
– Grounds for electronic communication information requests;
– Possible threats and possibilities of abuse;
– Advantages of using the electronic format of telecommunication information requests management.

Keywords: telecommunication information, electronic information, information requests management, electronic communication, data requesting

Introduction

The possession of electronic communication data by police officers and public prosecutors is a very powerful tool for combating crime. At the same time, it is a big responsibility to collect and keep the information properly, without any abuse in the context of human rights.

All police officers in the Republic of Croatia would agree with the conclusion that a police job is unimaginable without the usage of electronic information requests and analyses (Kralj, 2009).

1 Seconded National Expert at CEPOL in Budapest, Hungary. Corresponding author's email: damir.maracic@cepol.europa.eu

Public prosecutors would agree with the before mentioned conclusion as well, having in mind the value of evidence collected by special evidence collection actions.

Usage of a number of special evidence collection actions at the same time with requesting the telecommunication information is really important. In that sense, requesting the telecommunication information is the controlling and supporting action for all other actions (Maračić, 2015).

The term "electronic communication data" refers to data about the contact(s) between electronic addresses during a certain period (duration, frequency) or at the exact time, location of the device, the identification parameters of the device and the identification of the device user(s) location, excluding any information about the content of communication.

Technological improvements and development enable the public to communicate using various types of communication devices. Therefore, since criminals are using modern communication technology, law enforcement officials have to possess an adequate and efficient model of data collection that is in line with both technological requests and the legal framework.

Without going into details, the electronic communication data used for the intelligence purposes or in an evidentiary form helps to identify, locate and arrest the criminal offender(s) and also to investigate and prosecute criminal offences in numerous cases. Furthermore, it helps in situations when persons are lost or missing, when it is necessary to search for some objects or as an evidence collecting tool.

In general, numerous cases were solved thanks to a crucial evidence that originated from the electronic communication information.

On the other hand, a request for electronic communication information represents a temporary limitation of personal rights, protected by European Convention on Human Rights and its Protocols (Council of Europe 1950), national constitutions and other related laws, and it always comes under the scrutiny of the public eye.

Taking into consideration all the above reasons, law enforcement officers have to follow the very precisely prescribed procedure of: the requesting and issuing of electronic communication data, as well as the handling, processing, storage and use of data.

In terms of the use of electronic telecommunication tracing or interception, each EU member state has its own specific rules and regulations, but what all EU member states have in common is the need to act in accordance with the rules of European Convention on Human Rights and its Protocols. The information on different legal systems of the EU member states and details on the status of the implementation and ratification of regulations can be found on the European Judicial Network website (2018). This website, or, more specifically, the sections of Atlas, Compendium or/and Fiches Belges describe, among other things, all possibilities of electronic telecommunication tracing or interception in the EU member states. The European Judicial Network website thus gives an opportunity to explore and compare the possibilities and ways for a successful judicial cooperation (Maračić, 2016).

Croatian legal framework on electronic communication information requests

In accordance with the Croatian legislature, electronic communication data can be extracted in an intelligence or evidentiary form. The difference between the two forms depends on the used legal ground, since it can be used either in accordance with the Police Powers and Duties Act (Republic of Croatia, 2014) or with the Criminal Procedure Act (Republic of Croatia, 2017).

According to Article 68 of the Croatian Police Powers and Duties Act, electronic communication data verification is one of the police powers. It's allowed in the investigation and suppression of ex officio criminal offences; in the suppression of danger and violence; and also when searching for persons and objects.

Persons authorised for the electronic communication check approvals are the Head of Criminal Police Directorate, the Head of Police National Office for the Suppression of Corruption and Organised Crime and Heads of Police Districts. In the case of their absence, Deputy Heads are authorised for the mentioned approval.

Furthermore, the Croatian Regulation of the Police Proceedings (Republic of Croatia, 2015) regulates in more detail police powers and refers to the Croatian Police Powers and Duties Act. Article 103 of the Regu-

lation stipulates that electronic communication checks should be requested through Information Technology (IT) application of electronic communication information management.

On the other hand, the Croatian Criminal Procedure Act, Article 339a prescribes the verification of the establishment of telecommunication contact as an evidence collection action. It is allowed in the case of the investigation of criminal offences specified in the criminal offences catalogue for the special evidence collection actions and for the criminal offences with prescribed imprisonment of more than five years. The investigation judge is authorised to issue a warrant for requested telecommunication checks at the request of a public prosecutor, but in specific and very urgent cases, a warrant can be issued by a public prosecutor and later validated by a judge. If the registered owner or user of telecommunication devices gives his written approval, the warrant is not needed.

In both cases of requesting telecommunication information, either in a cognitive or evidentiary form, the operational technical procedure is almost the same. For the purpose of the coordination and control of all relevant bodies involved in requesting and conducting this process according to the Law on a Security Intelligence System (Republic of Croatia, 2006) and Criminal Procedure Act, the Operational Technical Centre has been established. The role of the Operational Technical Centre is to provide a flow of the requested telecommunication information between telecommunication providers and investigation authorities. The Operational Technical Centre provides a support to the Intelligence service as well.

The legal ground for requesting electronic information in the Republic of Croatia is regulated in accordance with the directions of the European Court, abiding by the rights of privacy and personal data protection (Juras & Vulas, 2016).

Monitoring of the implemented electronical communication information requests

When we speak about electronic information requests managed in accordance with the police powers, the Croatian Police Powers and Duties Act predicts possibilities for monitoring. For that purpose, in accordance with the Act, the Council for Civilian Supervision of police powers should be established. The Council is composed of 5 members and 5 deputy members. They can act after criminal investigation has been finalised and are authorised to ask for the relevant information from all bodies involved in the process. At the end of the supervision, the Council must submit a report to the President of the Croatian Parliament, the President of the Committees for Internal Politics and National Security, the Committee for Human Rights and Rights of National Minorities, the Minister of the Interior and the General Director of the General Police Directorate. At the same time, the applicant for monitoring should be informed.

When electronic data are collected in an evidentiary way in accordance with the Criminal Procedure Act, the monitoring and control mechanism is arranged through judicial system. A request for electronic (telecommunication) data could be initiated by the police toward the public prosecutor, or the public prosecutor himself can initiate a request. In both cases, the public prosecutor has to pass the request to the investigation judge who considers the request and makes a decision within 4 hours. If the investigation judge approves the request, he/she issues a warrant and sends it to the police authorities for action. As was mentioned earlier, in specific urgent cases the public prosecutor is authorised to approve and issue a warrant by himself but he/she has to inform the investigation judge within 24 hours and the judge has to decide whether to verify it or not. The described protocol is a guarantee for the protection of human rights, so the terms prescribed in the Criminal Procedure Act do not allow any abuse of this evidence action since otherwise all collected data is considered illegal and not usable in criminal proceedings.

It should also be mentioned that all the described actions regarding electronic telecommunication data requests and all results and reports of the requests are part of the chain of evidence used in the ensuing criminal proceeding. During that time, there is another way of monitoring conducted by trial judge or court council.

Statistics as a trigger for action

By adopting the amendments to the 2002 Criminal Procedure Act, the Republic of Croatia has for the first time clearly defined the possibility of access to retained data on electronic communications, or more specifically telephone calls and messages records, while the content of communication still remains in the domain of the gathering of evidence by using special evidence actions and depending on the possession of a court order.

In order to prevent uncontrolled access to retained data and to provide for the use of this power to be monitored, the prescribed way of accessing this information within the Ministry of the Interior implied a centralized approach to telecommunications operators. Such access is ensured through the Criminal Police Directorate, or the Special Investigation Service, which collects and verifies the technical validity of the request centrally and provides technical support to users, while the legality of requests to access the data is checked by the head officers of the criminal police line within the Police Directorates.

At the beginning, all the work was done by filling the forms manually and by delivering them physically to the Special Investigation Service, which recorded all the requests, collected the requested data and submitted them to the claimants.

The problems that dogged the work were the slowness of the entire process of data acquisition and analysis, insufficiently structured data and different data supplied by different telecommunication operators, insufficient explanations of service marks within the submitted records, the lack of data including the lack of infrastructure data for the transmission of communications etc.

Signs of additional problems emerged in 2003 when the first Law on the Liberalization of the Telecommunications Market was adopted, and the police began to notice these problems for the first time in 2005, when new telecommunications operators started providing services. All of this has led the police to face new data formats, new types of data, problems with communicating with operators, and a strong need for establishing new protocols. Rules of the game have been identified to prevent possible abuse without causing public safety erosion and inability to conduct criminal investigations.

The Ministry of the Interior launched an initiative to establish an independent agency that would represent a technical body between the law enforcement authorities and providers of telecommunication services in the field of legal interception of communications and access to retained data.

This initiative came to life in 2007, when the new Law on the Security Intelligence System of the Republic of Croatia entered into force, which was a major change considering that it foresaw the establishment of the Operational and Technical Center for Telecommunication Surveillance (hereinafter OTC). OTC gained an important role in the system when it comes to controlling lawful interception measures. OTC managed to arrange the standardization of procedures in accordance with the ETSI standards and the same format of call data, especially for mobile and landline telecommunications operators.

At the same time, the situation was out of control with the increased number of users of telecommunications services in the conditions of a growing economy in the pre-crisis period. At one point, the number of users exceeded 8 million in landline and mobile telephony services without users of Internet access.

Table 1. Indicators of the number of requests for access to retained data compared to the number of criminal offenses and the number of mobile and landline telephone network users without internet access users (Kralj 2009)

Year	Criminal offences (without traffic offences)	Requests	Phone numbers	Landline subscribers	Mobile subscribers
2001	75 730	1 182	2 466	No data	No data
2002	75 363	2 576	5 646	1 825 157	2 312 653
2003	77 653	4 099	8 867	1 871 347	2 537 332
2004	82 950	6 710	12 021	1 887 637	2 835 508
2005	77 587	11 790	18 648	1 882 500	3 649 700
2006	78 664	16 267	25 218	1 826 800	4 395 150
2007	73 319	18 823	28 915	No data	No data

According to the records of the Ministry of the Interior of the Republic of Croatia, during the years 2014 and 2015 a total of 48 460 requests for verification of telecommunication contacts were filed pursuant to Article 68 of the Police Powers and Duties Act (25 263 requests in 2014 and 23 197 requests in 2015), approved by authorized persons in accordance with the legal regulations, after which the requested information was verified by the telecommunications service provider (Juras & Vulas, 2016).

According to the "Annual comparative data of the electronic communications market in the Republic of Croatia" by the Croatian Regulatory Agency for Network Activities HAKOM, the number of users of services in the landline and mobile network for 2010, 2011, 2013, 2014 and 2015 was as follows:

Table 2. Indicators of the number of landline and mobile network subscribers

Year	Landline subscribers	Mobile subscribers	Sum of subscribers
2010	1 865 729	6 362 106	8 227 835
2011	1 606 090	5 115 140	6 721 230
2012	1 454 133	4 971 351	6 425 484
2013	1 430 644	4 912 134	6 342 778
2014	1 355 421	4 461 352	5 816 733
2015	1 315 654	4 415 660	5 731 314

By reviewing the above indicators, it is clear that the telecommunications market had an uncontrolled growth that stabilized by 2015 and returned roughly to the 2005 indicators.

As access to electronic communications is made available to all police officers working in criminal police lines from the smallest organizational units (police stations) to the units in the Police Directorate, the amount of work and time spent has reached a critical level in 2009. Encouraged by this development of the situation, the Police Directorate of the Ministry of the Interior has launched a comprehensive recording of the state, processes, procedures, data categories and the legislative and organizational framework in order to come up with concrete proposals in 2011 to change the model of work and to move to a solution based on the information and communication technology.

During 2014, an implemented solution based on Internet technology was completed, thus enabling the creation, approval, delivery, data visualization and process monitoring for the purpose of detecting potential misuse of data, called TIRM (Telecommunication Information Request Management hereinafter referred to as TIRM).

TIRM is available to every police officer in the line of criminal police work and is linked to the OTC, which enables a fully computerized process of accessing the retained telecommunication data and auditing them.

This solution has been recognized and accepted by police officers as easy, reliable and user-friendly since the very beginning of the application. The average time of the whole process compared to the previous state is reduced from 3 days to 2-6 hours, whereas in

urgent cases of rescue or search for persons, this process takes only a few minutes, with the level of protection of the data and the legality of using police powers duly secured.

Not less importantly, the whole process is practically paperless, with high savings in paper, ink, delivery costs and working hours. A significant number of police officers who worked on these jobs was returned to crime investigation jobs instead of being engaged with filling in and submitting requests and records and allowing managers to automate the creation of reports for their organizational units and to conduct a faster and more effective supervision over the use of the police powers.

Conclusions

In accordance with the previously explained facts, TIRM is a user-friendly application arranged by the needs of end users. It helps in daily work and is making the process faster. At the same time, the monitoring system is giving the best guarantees for the protection of citizens and their human rights.

As with any IT system, there is a constant need for improvement and upgrading TIRM, and this may be caused by external influences, such as changes in legal acts or new telecommunications services, and internal influences, such as organizational changes, additional requests from users etc. The TIRM system, due to its design, can easily be upgraded to new functionalities or adapted to new needs or additional protection measures.

References

- European Judicial Network website (2018).
  Available from: https://www.ejn-crimjust.europa.eu/ejn/ [Accessed 13th February 2018].
- Council of Europe (1950) European Convention on Human Rights and its protocols.
  Available from: http://www.echr.coe.int/Documents/Convention_ENG.pdf [Accessed 13th February 2018].
- Juras, D. & Vulas, A. (2016) Legal Framework for Checking of Telecommunication Contacts. Policija i sigurnost, Zagreb, Croatia, 1, 69-81.
- Kralj, T. (2009) Examination of the Identity of Telecommunication Addresses in Criminal Practice, Policija i sigurnost, Zagreb, Croatia, 2, 166-179.
- Maračić, D. (2015) Special Collection of Evidence, Simulated Sales: Assessment of Risks in Choice of Sale Objects and Impact of Sale Objects on the Start of Final Action. Proceedings of the 4th International Scientific and Professional Conference "Police College Research Days in Zagreb", Zagreb, Croatia, 620-628.
- Maračić, D., (2016) Webpage European Judicial Network (EJN) as Help for Establishing International Judicial Cooperation. Proceedings of the 5th International scientific and professional conference "The Police College Research Days, "New Technologies and Methods Used for Improvement of the Police Role in Security Matters", Zagreb, Croatia, 398-409.
- Republic of Croatia (2006) Law on a Security Intelligence System, Official Gazette of the Republic of Croatia "Narodne novine", 79/2006, 105/2006.
- Republic of Croatia (2014) Police Powers and Duties Act. Official Gazette of the Republic of Croatia "Narodne novine", 76/2009, 92/2014.
- Republic of Croatia (2015) Regulation of the Police Proceedings, Official Gazette of the Republic of Croatia "Narodne novine", 89/2010, 78/2014, 76/2015.
- Republic of Croatia (2017) Criminal Procedure Act. Official Gazette of the Republic of Croatia "Narodne novine". 152/2008, 76/2009, 80/2011, 121/2011, 91/2012, 143/2012, 56/2013, 145/2013, 152/2014, 70/2017.