CHAPTER 2
LEGAL RELATIONS: FROM THEORY TO PRACTICE

THE RIGHT TO PRIVATE COMMUNICATION USING TELECOMMUNICATIONMEANS: NATIONAL AND INTERNATIONAL LEGAL ASPECTS OF PROTECTION

Mueen Fandi Nhar Alshunnaq[1]

[1]*Doctor of Law, Jadara University, Irbid, Jordan, e-mail*: *abu_alahmadshunnaq@yahoo.com, ORCID: https://orcid.org/0000-0002-4488-1220*

Abstract. *Today's challenges dictate the need to strengthen the national and international legal mechanisms for the protection of personal data and the right to private communication. However, considered rights are not absolute. Legitimate restriction of guaranteed rights is possible, since these means of communication are a powerful tool in the investigation and disclosure of hard/very hard crimes, including transnational ones, especially considering the terrorist threats to Jordan and other countries. The possibility of restricting human rights, arising from the guarantees enshrined in the European Convention on Human Rights and consistently enshrined in the ECHR, demands from the state the least compulsory guarantee while interfering with the rights of individuals – to act "in accordance with the law". Law protection of personal data and right to privacy are researched in the context of peculiarities of conducting investigative (search), secret investigative (search) and other procedural actions in criminal proceedings, which concern access to some telecommunication means (e.g., smart phones). Taking into account different functional purposes of technical means of telecommunication, access and collecting of evidence contained therein, should be carried out on a case- to-case basis, in a different procedural form, considering specifics of telecommunication technologies in each particular case.*

Keywords: *privacy, the secret of communication, telecommunication means, criminal proceedings, covert investigative (search) actions, due process, international law, smart phone.*

JEL Classification: K12, K22, K33,

Formulas: 0; fig.: 0; tabl.: 0; bibl.: 8

Introduction. The protection of personal data in information and telecommunication networks/systems (telecommunication means), including using the Internet, today is one of the main tasks of the states, private institutions and the international community. Legal protection of personal data and privacy rights includes the following: constitutional law, international law, administrative law, and criminal and criminal procedural law.

Consequently, these rights on the national level are guaranteed by constitutions or special legislation. Also, today's challenges dictate the need to strengthen the international legal mechanisms for the protection of personal data and the right to private communication. However, considered rights are not absolute. Legitimate restriction of guaranteed rights is possible, since these means of communication are a powerful tool in the investigation and disclosure of hard/very hard crimes, including transnational ones, especially considering the terrorist threats to Jordan and other countries.

General Data Protection Regulation (GDPR) (EU) 2016/679 (it. 4 of Preamble) states that "the processing of personal data should be designed to serve mankind. The

right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality". At the same time GDPR (it. 19 of Preamble) should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests, including public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. This is relevant, for example, in the framework of anti-money laundering or the activities of forensic laboratories [1].

Aim. The main objective of the research is to identify issues related with the legal regulation of the protection of personal data and the right to private communication, and to put forward suggestions for their solution, which are set out in the results of our study. Law protection of personal data and right to privacy are researched in the context of specifics of conducting investigative (search), covert investigative (search) and other procedural actions in criminal proceedings, which concern access to some telecommunication means.

Methods. The national and international (in EU area) legislatives, case-law of ECHR, judgements of Jordan courts in criminal cases and relevant legal literature are analyzed in the paper. In this research, a complex of general and special scientific methods of legal science (dialectical, comparative legal, analytical, descriptive, systemic-structural, generalizations etc.) is used.

Results. The stated idea of possible wrongful use, in particular of the Internet environment, for improper purposes, is consistently traced in Recommendation CM/Rec (2018) 2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries (Adopted by the Committee of Ministers on 7 March 2018at the 1309th meeting of the Ministers' Deputies). As specified in the Recommendation, inter alia, "the internet has facilitated an increase in privacy-related risks and infringements and has spurred the spread of certain forms of harassment, hatred and incitement to violence, in particular on the basis of gender, race and religion, which remain underreported and are rarely remedied or prosecuted". According to the Committee of Ministers of the Council of Europe, owing to the abuse, serious problems were encountered in connection with maintaining public order, national security, crime prevention, activities of law enforcement bodies, as well as the protection of other persons, including protection of intellectual property rights [2].

For example, Art. 8 Convention for the Protection of Human Rights and Fundamental Freedoms (Rome, 1950), along with the fact that it enshrines the right to respect for the right to private and family life, to own home and correspondence, also provides for the possibility of restricting it to clearly defined cases, such as "in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well- being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the

protection of the rights and freedoms of others". It follows from the practice of the European Court of Human Rights that interference by public authorities is possible not only when it is carried out "in accordance with the law", but also when it has a "legitimate purpose" and is "proportional" [3].

European Court of Human Rights (hereinafter, ECHR or European Court) also asserted that legitimate restriction of guaranteed rights "are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions. Noting, however, that democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order to counter such threats effectively, to undertake the secret surveillance of subversive elements operating within its jurisdiction, the Court considered that the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications was, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime" [4].

All of the foregoing, taking into account the possibility, in exceptional cases, of limiting the right to privacy and private communication (as a part of the right to respect for private and family life), determines our further scientific research and analysis of legislative regulation of the presented set of problems in the criminal procedural context since nowadays, the means of criminal procedural influence and combating crime, including transnational one, are perhaps the only effective way to counteract these challenges of national security and public safety.

As Dita Plepa rightly specified in her paper, "security has been and is one of the most fundamental issues defining relations between the state and the citizen. Development of a contemporary democratic and judicial state is linked to the search for balance between the protection of constitutional values and respect for human rights" [5].

Consequently, as we see, the possibility of restricting human rights arising from the guarantees enshrined in the European Convention on Human Rights and consistently enshrined in the ECHR demands from the state the least compulsory guarantee while interfering in the rights of individuals – to act "in accordance with the law". Nowadays it is an indisputable thesis since the proper legal procedure enshrined in the law is an unconditional guarantee of enforcement of human rights and freedoms. Therefore, in our study, we will try to show that a serious problem, inter alia, for a number of European states is the imperfection of the legislative regulation of the grounds, conditions and procedure for legal interference of the state with these persons' rights, taking into account the factor of the rapid development of information and telecommunication technologies.

In this context, for example, the decision of the ECHR in the case *Liberty and Others v. the United Kingdom*, July 1, 2008, may be indicative. The applicants, a British and two Irish civil liberties' organisations, alleged that between 1990 and 1997 their telephone, facsimile, e-mail and data communications, including legally privileged and confidential information, were intercepted by an Electronic Test Facility operated by the British Ministry of Defence. They had lodged complaints

with the Interception of Communications Tribunal, the Director of Public Prosecutions and the Investigatory Powers Tribunal to challenge the lawfulness of the alleged interception of their communications, but to no avail. The Court held that there had been a violation of Article 8 of the Convention. It did not consider that the domestic law at the relevant time indicated with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the authorities to intercept and examine external communications. In particular, it did not, as required by the Court's case-law, set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material. The interference with the applicants' rights under Article 8 was not, therefore, "in accordance with the law" [4].

Consequently, as we see, the desire of the state to counteract serious challenges regarding unlawful and extremely dangerous criminal offenses against public security can, on the one hand, lead to abuses of the competent public authorities while investigating and detecting crimes and, accordingly, unlawful restriction or violation of human rights and freedoms, on the other hand.

And therefore, the law and the due legal procedure enshrined in it is a guarantee against the specified abuses. That is why we consider it expedient to analyze legal regulation of the procedural instruments (means) which enable to obtain evidence constituting personal data of a person, as well as data concerning the exchange and use of information that can be attributed to private communication.

As it is supposed, such ambiguity is caused by the uncertainty of legal regulation of this issue, as well as by the very specific, unequal technical and legal nature of the above telecommunication means (devices) and information that is stored, processed and used with the help of the latter. For example, the mobile terminal of communication systems – "smartphone" - can be used as:

1) a means of communicating in real time (online), for example, for making telephone calls;

2) a means of access to electronic information systems using various forms of data transmission, including, as a rule, via the Internet (for example, for communication in various chats, social networks, namely, Facebook, Twitter, Instagram, Telegram, Snapchat, etc.; or for use of e-mail, including using the so-called "cloud-based technologies" ("cloud computing") for storing and processing information (for example, Google Drive or the like); or using so- called "messengers" such as Viber, WhatsApp, Skype, Facebook Messenger, Telegram, etc.). As the researchers point out, these telecommunication technologies represent network convergence supporting a wide range of access methods (traditional telephony, DSL, networks WLAN, RAN, etc.); at the level of service convergence during mobile communication sessions with the help of specialized software, mobile access to data, audio and video contraction, voice and instant messaging can be carried out. The widespread use of smartphones with installed programs that combine IP-telephony and instant messengers (Skype, Viber, etc.) or only instant messengers (ICQ, Telegram, WhatsApp, etc.) by mobile telecommunication subscribers form them as

elements of distributed electronic information systems (hereinafter, DIS). DIS components are distributed, therefore, on several computers. In turn, DIS is composed of file-server information systems and client-server information systems. In the latter, for example, a database and database management system are located on the server, and client- side software is located on the workstations. As specified in the literature, both local and distributed electronic information systems can be open for the public and closed, i.e. access to which is limited to their owner, proprietor or holder, to obtain more information on the features of individual electronic information systems and IREIS. At the same time one very significant feature should be mentioned. As a rule, information displayed on the device screen is not physically stored on it. It is stored in electronic information systems (information (automated) systems), on servers of the relevant companies providing appropriate information and telecommunication services. In other words, in this case, a mobile device serves only as a means of access (a kind of "key") to information that constitutes communication content. Otherwise, if specified information is stored in the memory of the device itself, the features of the use of the latter will be described below, in the third group. In addition, it should also be noted that some of the mentioned messengers or social networks also allow real-time communication (online). Therefore, in such cases, the smartphone should be assigned to the previous group according to its functional (functional, technical and communication) purpose;

3) A means of storing and/or processing data (a variety of text, image, audio, video and other files and digital content). For example, audio, video, photo files, SMS messages and others sent and saved by a user can be stored in the device memory. Access to this information contained in a technical device can be gained either directly by an operating system of the latter or with the help of a specially-designed software, so-called applications (commonly known as "a mobile application" or just "an application").

As it is supposed, given the different functional purpose of the said mobile terminals of communication systems, access to the information contained therein should be carried out on a case-by-case basis in different procedural order, using diverse methods of collecting evidence, taking into account the above-mentioned features in each particular case. Thus, the due legal procedure of the procedural order, ways of obtaining evidence in the context of access to it using the specified mobile terminals of communication systems (technical means of telecommunication) should be carried out as follows.

In the first case, when a mobile device is used as a means of communication in real time (online), information constituting private communication content can be obtained by conducting such a CISA as IRTTN (or monitoring a means of communication, since data transfer is carried out with the help of appropriate technical capabilities of transport telecommunication networks (communication channels). It should be borne in mind that when communication takes place in real time with the help of (by means of) software of a device that transmits data through social networks or similar online services, i.e. provides communication with electronic information systems (information (automated) systems) which are located

on the servers of the respective companies, access to such information in the context of "penetration" into these systems has to be gained by means of such a CISA as IREIS.

In the second case, when a smartphone (or other technical device) serves only as a means of access to information stored in electronic information systems and only displayed on the screen of a device, but physically not stored in it, obtaining and recording (copying) such information has to be done by means of conducting such a CISA as IREIS (such information is recognized as valid and admissible evidence in the court which is confirmed in the Jordan judicial practice.

Finally, in the third case, when a device is, virtually, a technical stored data carrier, the latter is characterized by all the features that are inherent in actual evidence or documents (in this case, these are electronic documents) in criminal proceedings. Therefore, only in this case access to the data stored in a technical device (a mobile terminal of communication systems), received and saved by a user (or automatically saved in this device), if the user is familiar with its content, can be obtained in such a procedural way as any other things or documentsin criminal proceedings. In other words, namely, seizure of a mobile device and access to the information content in it can be gained in connection with a search, examining a housing or other person's possessions, searching a person during a search in a housing or other property, temporary access to things and documents, etc. Examination of information contents contained (stored) in a device seized in such a way, copying of the relevant electronic documents have to be carried out during examination of the device, which includes involving expert assistance (in case of the need to apply expert knowledge while examining a device or information contained therein, it is also possible to involve an expert and conduct an expert examination in accordance with the procedure established by the procedural law).

In our paper, while characterizing the procedural order for obtaining (collecting) evidence, as an example, a smartphone is used as a mobile terminal of communication systems (a technical means of communication, telecommunication device). However, according to the same principle, taking into account the similarity of technical and legal nature, similarity of algorithms for collecting, storing, processing, transmission and use of information, functional purpose, etc., the indicated methods of procedural order of access (collection) to evidence may be applied to other types of technical means (devices) of telecommunication (personal computers, tablets, laptops, etc.).

Consequently, taking into account different functional purposes of technical means of telecommunication, access to and collecting evidence contained therein should be carried out on a case-to-case basis, in a different procedural form, considering specifics of telecommunication technologies in each particular case.

Here is a typical example that can illustrate the problems at both the national and international (transnational) levels of legal regulation.

Interesting that the entry into force of the General Data Protection Regulation (GDPR) (EU) 2016/679 of 25.05.2018 improved the protection of personal data of all persons within the EU and the European Economic Area, but at the same time, from

the point of view of legal regulation of the problem of access to personal data by law enforcement agencies, Directive (EU) 2016/680 of the European Parliament and of the Council, of 27 April 2016 "On the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA" is more specialized, along with Directive (EU) 2016/681 of the European Parliament and of the Council, of 27 April 2016 "On the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime". However, consistently emphasizing the protection of citizens' rights to privacy, the specified Directives also determine the direction of restricting this right in connection with the need to protect public and national interests from criminal infringements.

Discussion. Therefore, at the level of international legal treaty regulation, it is necessary to envisage a specific universal mechanism in criminal procedural sphere (co-operation) which, under certain conditions, would provide legal reasons and real possibilities for authoritative bodies of one state to have a power to influence companies being under the jurisdiction of another state. Appropriate unification and harmonization of national legislation should take place on certain principles of the common framework of conventional international legal regulation.

And the EU Directives alone cannot solve the problem, given that there are non-EU countries. Such countries can easily become so- called "information offshore" providing opportunities to evade the itemized conventional IT-regulation.

Among other issues, despite the fact that The Regulation and Directives were passed and enforced, it is seriously worrying that there are still ongoing discussions in the EU countries on finding legitimate reasons for preventing the transmission of information spread over the Internet, e.g., via Skype and Viber beyond the scope of criminal proceedings (as is already the case in the United States), which poses a threat to human rights.

Conclusions. On the basis of the research, the shortcomings of the legal regulation of the protection of personal data and the right to private communication at the national level, as well as inconsistency with international legal requirements and recommendations were revealed. This requires improvement of the legislative consolidation (in accordance with the requirements of the current level of development of telecommunication facilities), the bases, conditions and procedure for legal intervention of the state in the sphere of private life and communication; also bringing national legislation in line with international requirements and practices of international judicial institutions.

Taking into account different functional purposes of technical means of telecommunication, access to and collecting of evidence contained therein should be carried out on a case-to-case basis, in a different procedural form, considering specifics of telecommunication technologies in each particular case.

At the level of international legal treaty regulation, it is necessary to envisage a specific universal mechanism in criminal procedural sphere (co-operation) which,

under certain conditions, would provide legal reasons and real possibilities for authoritative bodies of one state to have a power to influence companies being under the jurisdiction of another state. Appropriate unification and harmonization of national legislation should take place on certain principles of the common framework conventional international legal regulation.

The specified mechanism should be universal, efficient, operative, guaranteeing protection of human rights and freedoms against unlawful violation, as well as compensation for damage caused by unlawful restrictions (violations) of these rights.

References:

1. Available at: https://eur-lex.europa.eu/legal- content/EN/TXT/?qid= 1549487787863 &uri=CELEX:32016R0679(accessed on February 5, 2019)

2. Recommendation CM/Rec (2018) 2 of the Committee of Ministers tomember States on the roles and responsibilities of internet intermediaries (Adopted by the Committee of Ministers on 7 March 2018 at the 1309th meeting of the Ministers' Deputies). Available at: https://search.coe.int/cm/Pages/result_details.aspx? ObjectID=0900001680790e14(accessed on February 5, 2019)

3. See in particular item 133 of Judgement in Case of Benedik v. Slovenia, April 24, 2018. Available: at https://www.echr.com.ua/translation/sprava- benedik-proti-slovenii- povnij-tekst-rishennya/ (accessed on September 30, 2018)

4. Case of *Klass and Others v. Germany*, September 6, 1978. The data is taken from: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf (accessed on September 30, 2018)

5. Dita Plepa. L¯ıdzsvara mekle¯jumi starp pamatties¯ıbu ieve¯rošanu un valsts droš¯ıbas aizsardz¯ıbu Satversmes tiesas prakse¯. Socrates: RSU elektroniskais juridisko zina¯tnisko rakstu žurna¯ls. № 2 (5). P. 56–73. P. 70. (2016). Available at: https:// www.rsu.lv/sites/default/files/imce/Dokumenti/izdevumi/socrates_5_2016.pdf (accessed on February 5, 2019)

6. The data is taken from the official web-portal of the National Commission for the State Regulation of Communications and Informatization. Available at: https:// nkrzi.gov.ua/index.php?r=site/index&pg=59&id=4182&language=uk (accessed on September 30, 2018)

7. An exception to this is, for example, Viber and some others where information on the content of messages, sent files, etc. is physically contained (stored) in the memory of a technical device itself since, as the company claims, information content of messages is deleted from the servers of the company as soon as a message is sent to an end user. See more about Viber's privacy and security policy. Available at: https://www.viber.com/security (accessed on September 30, 2018) On the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecutionof criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA: Directive (EU) 2016/680 of the European Parliament and of the Council, of 27 April 2016. Available at:https:///eur-lex.europa.eu/legalcontent/en/TXT/%3Furi%3 DCELEX%253A32016L0680&prev=search (accessed on February 5, 2019)

8. On the use of passenger name record (PNR) data for the prevention,detection, investigation and prosecution of terrorist offences andserious crime: Directive (EU) 2016/681 of the European Parliamentand of the Council, of 27 April 2016. Available at: https://consilium.europa.eu/en/press/press-releases/2016/04/21-council-adopts-eu-pnr-directive/&prev=search (accessed onFebruary 5, 2019).

Received: April 21, 2021
Approved: May 12, 2021