INFORMATION PROVIDED BY THE GOVERNMENT OF

THE REPUBLIC OF MOLDOVA

Report of the Office of the High Commissioner for Human Rights on the right to privacy in the digital age

1. Recent developments in national or regional legislation, case law, and practice concerning the right to privacy in the digital age.

In the context of fast and robust technological evolutions and the worldwide rapid digitalization, the Republic of Moldova acknowledges that there is a necessity to create the conditions to ensure an effective implementation of the right to privacy and personal data protection. The commitment of the Republic of Moldova in ensuring the realization of the right to privacy resulted in th eestablishement of a National Center for Personal Data Protection (NCPDP). Currently the Center is focused on two main actions:

The first consist in creating a robust data protection legal framework. A privacy legal framework exists in the Republic of Moldova since 2007, drafted based on *Convention for the Protection of Individuals with regard to Automatic Data Processing of Personal Data* (Convention 108) of the Council of Europe and *Directive 95/46/EU*. Furthermore, with the signing of the Association Agreement with the European Union in 2014, both parties agreed to cooperate in order to ensure a high level of personal data protection. Taking into account this context, the NCPDP started the process of drafting a new personal data protection legal framework by redrafting the current Law no. 133 of 08/07/2011 and forging a new Law on the National Center for Personal Data Protection. These two new draft laws aim to bring Moldovan legislation on par with the European Union standards, namely with Regulation 2016/679 (General Data Protection Regulation – GDPR) and Directive 2016/680.

Besides creating a new framework to ensure an adequate level of data protection, it is also crucial to communicate, inform and raise awareness of society. Indeed, a 2017 survey shows a rather interesting trend – the vast majority of the population (95%) considers *very important* or *important* the right to intimate, private and family life. However, 39% of the respondents to the same survey do not know what personal data are and 76% do not know about the existence of the NCPDP as the public authority defending the right to privacy in the Republic of Moldova.[1]

Therefore, there is an evident need to raise awareness on these issues and on the modalities to protect one's right to privacy. Several activity aiming awareness were undertaken through various means, namely by creating specific materials (video, presentations and public discussions) for the general populations but also targeting vulnerable groups. Indeed, the majority of NCPDP actions tried to focus on young people and, most recently, children, as there is an increasing number of digital services (games, websites) that are designed for them. These efforts complement national initiatives

[1] Survey from the Center for sociological and marketing studies CBS-AXA, *Assessment of the knowledge, attitudes and practices of the population regarding the protection of personal data,* Chișinău 2017

like siguronline.md and #superparents that aim to give the means of personal data subjects to know how to protect their personal data and inform about the potential threats.

Furthermore and complementary to the legislation on personal data protection in 2017 the national legal framework on electronic communications has been amended so that it would increase the protection of human rights and fundamental freedoms of final users.

Thus, the Law no. 135 of 07.07.2017 amending the Electronic Communications Law no. 241-XVI of 15.11.2007, hereinafter "Law No 241/2007", in force since August 18, 2017, contains a chapter specifically dedicated to the protection of confidentiality in the field of electronic communications, which provides for specific conditions to guarantee the right to privacy protection in the processing of personal data used in electronic communications.

The provisions of the new chapter of Law no. 241/2007 apply to the processing of personal data related to the provision of publicly available electronic communications services through public electronic communications networks, including networks that support devices for data collection and identification, except cases when this work is performed:

a) within the framework of national defense and security actions, under the law;
b) within the framework of actions aimed at prevention, investigation, prosecution of criminal offenses and maintenance of public order, as well as other activities in the field of criminal procedure, carried out under the law.

The chapter specifies the rights of electronic communications service subscribers and users to personal data protection, the obligations of providers to ensure service and personal data security, as well as the responsibilities of the National Center for Personal Data Protection and ANRCETI in this area.

In such a way, providers of publicly available electronic communications services are required to take appropriate technical and organizational measures to protect the security of the services. The measures must ensure a level of security adequate and proportionate to the existing risks and comply at least with the following conditions:

a) to ensure that personal data can only be accessed by authorized persons and for purposes specified by law;
b) protect stored or transmitted personal data against accidental or unlawful destruction, accidental loss or damage, and unauthorized storage, processing, access or disclosure;
c) to ensure the implementation of the security policy developed by the provider regarding personal data processing.

Where there is the risk of network security violation, providers are required to inform subscribers of this risk. Where the risk goes beyond the scope of the measures that may be taken by the providers, they must inform subscribers of possible solutions, including the costs involved. In case of a personal data violation, the provider shall notify the National Center for Personal Data Protection, without undue delay. Where a breach of personal data is likely to prejudice the personal or private life of a subscriber or user, the provider shall notify him of the breach without undue delay.

Moreover, the new chapter of Law no. 241/2007 provides for a number of interdictions related to the tapping, recording, storing or other types of interception or surveillance of communications and data transfer, by persons other than the end-user participating in the communication, as well as related to storage and processing by providers of transfer data related to subscribers and users and billing of

services offered to them, processing of location data, using dial-up and automatic communication systems, faxes or e-mail for advertising purposes, etc.

On the other hand, in order to ensure the children online protection without allowing any undue interferences with the rights in digital age, has been developed the draft law for amending Article 5 of the Law no. 30 of 7 March 2013 on protecting children from the negative impact of information. It stipulates that Internet access providers shall offer end-users the option/possibility to install Internet content filtering applications. A section dedicated to Internet safety information shall be provided as part of the main menu on their official web pages. This project pursues an essential social impact, with benefits to children - the most vulnerable to the dangers of the Internet.

2. Surveillance and communications interception:
    a) Government surveillance, including, for example, communications interception and bulk data collection and processing, targeted intrusions in ICT systems and issues relating to cross-border surveillance and access to personal data.
    b) Role of business enterprises in contributing to, or facilitating government surveillance activities, including:
        i. Sale of surveillance technology by business enterprises and ensuing responsibilities;
        ii. Business enterprises' internal safeguards and remedial mechanisms

Interception of communications, data processing and collection, intrusions into ICT systems and other such special investigative measures are estimated by the Code of Criminal Procedure of the Republic of Moldova which, in Section V "Special Investigative Activity", provides special ways of authorizing and carrying out special investigative measures, through which the risk of violation of the rights of a person and personal data is created. This process takes account of the principle of proportionality, so that the lesion of a right is dictated by an appropriate need applicable to the intended purpose.

At the same time, in order to implement the provisions of the Council of Europe Convention on Cybercrime, the draft law no. 161 regarding the amendment and completion of certain legislative acts, it was proposed to supplement the Criminal Procedure Code of the Republic of Moldova with new articles:

a) "Interception and registration of computer data" - introduction of the special investigative measure "Intercepting and recording of computer data", authorized by the investigative judge. The interception of computer data is provided in Title 5 art. 20 and 21 of the Council of Europe Convention on Cybercrime, adopted in Budapest on 23 November 2001 and involves the collection and recording of traffic and content data, associated with such communications.
b) "Computer search and retrieval of objects containing computer data" - according to art. 19 para. 1 of the Council of Europe Convention on Cybercrime, "Each Party shall adopt such legislative and other measures as may be necessary to confer on its competent authorities the right to search or access in a similar manner a computer system or a part thereof , as well as the computer data stored therein and a computer storage that allows the storage of computer data in its territory. "

3. Encryption and anonymity as enablers for the enjoyment of human rights, including the right to freedom of expression and of opinion; challenges raised by encryption and anonymity and ways to address these challenges.

In accordance with art. 11 of the Law no. 133 of 08.07.2011 "On the protection of personal data", after the processing of the personal data, if the subject of this data has not given its consent for another destination or for further processing, they shall be: a) destroyed; b) transferred to another operator, on condition that the original operator guarantees that subsequent processing has purposes similar to those in which the initial processing was carried out; c) transformed into anonymous data and stored exclusively for statistical purposes, historical or scientific research.

The main risks and vulnerabilities identified: the means of anonymizing computer system connections to the most commonly used global Internet network are: TOR, Proxy and VPN (which hide the technical identification data of the user).

TOR (The Onion Router) - is a free software that allows anonymity to be kept on the Internet through a close-to-close routing algorithm. In the TOR network, generated online traffic is anonymous, without listing the search terms and without keeping a record of IPs from where those searches were initialized. The TOR network also includes a special system that rises the signals between different IP addresses. It also allows this mechanism to access sites that are filtered by proxy servers installed on the network. The TOR is also a browser (The Tor browser), a darknet access gateway, the "dark internet", and accessing the "Deep Web" sites in the "Onion" domain.

VPN - virtual private network that expands a private network over a public network, such as the Internet. VPN allows a computer or a network-capable device to send and receive data over public or shared networks as if it were connected to the private network, while benefiting from the functionality, security, and policy of the public network.

PROXY servers are computers that act as an interface between the Internet and the computer. Any type of traffic driven through proxy servers will appear as coming from their IP address, not from your computer address. Unlike VPN servers, proxy servers do not have resources set aside to encrypt the traffic passing through them and are therefore able to accept simultaneous connections from multiple users at the same time. Proxy servers usually communicate with the Internet using HTTP or SOCKS.

- wireless access points with unrestricted (open) access to the global Internet network in public places;
- the use of asymmetric complex algorithms for crippling critical information to extinguish financial means through information technologies;
- the use of deconcentrated electronic payment systems based on crypto-algorithms (crypto-currency Bitcoin and others);
- direct data exchange networks between users, which leave no trace of activity in the content of the history recorded in the computer system or in the logs held by the service providers;
- the use of web hosting by offenders. Thus, although people who distribute infantic pornography or manage web sites with prohibited content are registered with IP addresses attributed to the Republic of Moldova, they often have contracts with national service providers located outside the state;
- 'small service providers' do not ensure a minimum level of cyber-security of their own network and often do not record service users and do not record metadata on Internet access.

7. Procedural and institutional safeguards, oversight mechanisms and remedies available to individuals exposed to domestic or extraterritorial surveillance, the interception of digital communications or other forms of processing of personal data by governments, business enterprises or private organisations.

- Decision no. 1123 of December 14, 2010 regarding the approval of the Requirements for ensuring the security of personal data in their processing within the personal data information systems;
- Order of Ministry of Internal Affairs (MAI) no. 444 of December 28, 2012 ,, Regarding the approval of the Regulation on the regulation of the processing of personal data by the subdivisions of the Ministry of Internal Affairs (as amended by MAI Order No. 260 of 04.09.2017);
- The provisions of MAI no. 10/229 of 17.02.2014 regarding the approval of the personal data confidentiality pledge form;
- Order of MAI no. 260 of 04.09.2017 regarding the filling in and amendment of the MAI Order no. 444 of 28.12.2012 (in item 43 was approved the Declaration of confidentiality of the personal data processed by MAI users;
- Order of MAI no. 70 of March 1, 2018 regarding the approval of the Special Affairs Service Regulation of the Ministry of Interior (authority responsible for monitoring the implementation of internal rules for confidentiality in the exchange of personal data).

In order to avoid interference with the privacy of individuals and to ensure the respect of human rights in the criminal proceeding, the use of mechanisms for supervision and interception of digital communications by the state is regulated by the national regulatory framework. Thus, the Criminal Procedure Code of the Republic of Moldova, no.122-XV of 14.03.2003, regulates the special investigative measures and the procedure for their execution, such as: home search and/or installation of the devices for video surveillance and audio recording (art.132^6), the supervision of the place of residence through the use of the technical means of registration (art.132^7), the interception and recording of communications (art.132^8), the execution and certification of the interception and recording of communications (art. 132^9), recordings of images (art. 132^{10}), verification of recordings of interceptions (art.132^{11}), retrieval, research, surrender, search or retrieval of postal items (art.133), examination and removal of postal items (art. 134), monitoring the connections of telegraphic and electronic communications (art.134^1), documentation using technical methods and means, location tracking through the Global Positioning System (GPS) or other technical means (Article 134^3), collection of information from electronic communications service providers (Article 138^4), identification of the subscriber, owner or user of a communications system electronic or access point to an information system (Article 134^5).

For those subject to the surveillance or interception mechanisms mentioned above, criminal law sets out a series of safeguards. Thus, according to art. 132^1 paragraph (2) of the Criminal Procedure Code, the special investigative measures are ordered and carried out if three conditions are cumulatively fulfilled:

1) if otherwise the purpose of the criminal proceeding is impossible to realize and/or if it might affect considerable the administration evidence;

2) there is a reasonable suspicion regarding the preparation or commission of a grave, particularly serious or exceptionally serious crime, with the exceptions provided by the law;

3) action is necessary and proportionate to the restraint of human rights and fundamental freedoms.

The execution of the measures shall be ordered only through the motivated order of the prosecutor or, as the case may be, through a judge's decision and shall be carried out in strict compliance with the provisions of the respective order/decision, and if the measure is executed with the manifestly human rights violations or when the investigative officer acted in breach of the ordinance, the prosecutor or the investigative judge shall declare the minutes void and dispose by ordinance/termination the immediate destruction of the material bearer of information and of the materials accumulated during

the execution of the special investigative measure. Assessing the practice of 2017 from the point of view of the application of the special investigative measures, there is a low share of the involvement by special measures in the criminal investigation activity, which is appreciated by 8.5%, which equates to 4898 special measures out of 57 313 criminal cases.

At institutional level, in order to ensure the observance of personal data protection, the Prosecutor's Office of the Republic of Moldova is guided by the provisions of Law no.133 of 08.08.2011 on the protection of personal data; by the requirements regarding the security of personal data in their processing within the personal data information systems, approved by the Government Decision no.1123 of 14.12.2010; Security policy and protection of personal data processing within the Prosecutor's Office, approved by Prosecutor General Order no. 20/4 May 15, 2017; Regulation on how to process the documented information, personal data and access to the information system of Prosecutor's offices, the Internet and e-mail, approved by the General Prosecutor's Order no.35 / 4 of 31.10.2016; Regulation on the processing of information containing personal data in the accounting system of the Public Prosecutor's Office, approved by the Order of the Prosecutor General no.32 / 28 of 26.10.2016; Regulation on the processing and protection of personal data of the employees of the Public Prosecutor's Office, approved by the General Prosecutor's Order no. 30/28 of 24.10.2016.

A separate mechanism to ensure the integrity of personal data processing within the Prosecutor's Office of the Republic of Moldova and to make the law enforcement agencies more efficient is the Integrated Automated Information System "Criminal Investigation: E-File", established by General Prosecutor's Order no.4/23 of 23.05. 2017 on the completion and use of the Integrated Automated Information System "Criminal Investigation: E-File" and of the Prosecutor General Order no.14 / 4 of 27.02.2018 on the approval of the Regulation on the Structure and Operation of the Integrated Automated Information System "Criminal Investigation: E-File ".

The purpose of the system is to replace existing information systems, including procedural and criminal acts drawn up in the criminal proceeding, including other acts and information relating to the criminal case, which may be attached as separate files with the addition of boxes to briefly describe them exports a criminal record in electronic format, also includes the possibility of managing process documents and documents by passing them from one user to another, allowing access to the materials of a single file of all participants in the criminal prosecution group at the same time, including the confidentiality of the information, and restricts access to other categories of users, enables the use of electronic signature, and finally generates statistical data on the activities of prosecutors.