Risk management, protection, and security of personal data in Romania

George-Loredan POPA,
Politehnica National University for Science and Technology, Bucharest
georgepopa1986@yahoo.ro

Abstract
In recent years, the digitization of institutions has gained momentum as a result of the coronavirus pandemic. The pandemic period imposed the digitization of services in an aggressive and forced way, many authorities had to apply immediate measures, without having a test base behind them. People were forced to interact with a computer, thereby giving up physical contact with colleagues, which in one way or another increased the exposure of companies, thus allowing cyber-attacks easier access to target targets. The human factor, education, and balance are important elements when it comes to the area of data security. Any digitization process is meant to provide operational efficiency, productivity, and information security. Analyzing cyber attacks we will notice that they evolve with the help of AI, attackers use this technology to be able to produce personalized messages, customer information, etc. At the moment, Romania is at an average level, or even below the average level in terms of the functioning of the Internet and data security. In this article, we will present the results regarding data security, as well as the measures that were taken to protect them, both at the level of Romania and other EU member states after the coronavirus pandemic period.

Keywords: coronavirus, data security, digitization, management.

1. Introduction

IT risk [1] management represents all efforts made to reduce threats, vulnerabilities, and consequences as a result of unprotected data. The risk analysis starts with its vulnerabilities, the evaluation of a potential computer attack, and the identification of the necessary measures to prevent or interrupt it.

Data protection [2] aims to protect information from unauthorized access, destruction, or modification. The main component of a process within an institution is represented by information. The information system represents a set of processes of the organization, the object of realization of the information being represented by technology. To protect data, at the level of each institution it is necessary to implement a very well-structured set of procedures, practices, functions, IT equipment, software applications, etc.

Data protection and security include a fairly wide range of activities such as risk analysis, best practices guide, management in situations (coronavirus pandemic), development, responsibility, and liability.

The crisis caused by the coronavirus pandemic [3] has put cyber security to the test [4], becoming a very important topic both at the level of the European Union and in its member states. The public sector had to quickly face new challenges in terms of IT, especially in the transition from working with physical presence to working from home. Since then, institutions have stepped up their activity in terms of data protection, paying a lot of attention to the preparation of systems against cyber attacks, especially on data protection.

However, fast digitization has had the role of offering the world new opportunities bringing a plus to the IT side, but also many threats in terms of increasing risks [5], many public institutions have faced cyber-attacks which have led to a social and economic impact.

2. Data Use Strategy

Following the coronavirus pandemic, the European Commission through its digital strategy has acquired enormous importance [6].

The approval of the strategy through digital tools was aimed at monitoring and limiting the virus, supporting research and development of new diagnostic strategies, treatments, and vaccines, and more than that, assuring the population about data protection as a result of the transfer of work online.

The imposition of restrictions, social distancing, and the working environment have become much more digitized, and public institutions and people have relied heavily on the internet and connectivity.

Governments took swift action, ensuring the continuity and availability of public services through e-government and e-health, while security systems protected online identity.

EU member states applied social distancing measures to combat the COVID-19 pandemic, and the demand for internet capacity increased massively, regardless of whether it was the provision of remote activities, e-learning, or entertainment, that led to network tension.

But as a result of these activities, new dangers have emerged, and cyber security has had a lot to do from the online safety of consumers, and the normal functioning of hospital facilities, to the management of existential energy and water supplies.

The coronavirus pandemic has highlighted digital skills for work and how to interact with others, while also demonstrating deficiencies in IT knowledge and the importance of digital education. In 2021, according to the EUROSTAT database, just over half of the workforce aged 16-74 had at least minimal IT knowledge.

According to this ranking, Romania ranks last, with a percentage of 28%, and at the opposite pole with the highest percentage are the Netherlands and Finland with 79%. As we can see from Fig. 1, an equally low percentage is also found in the case of Bulgaria 31% and Poland 43%.

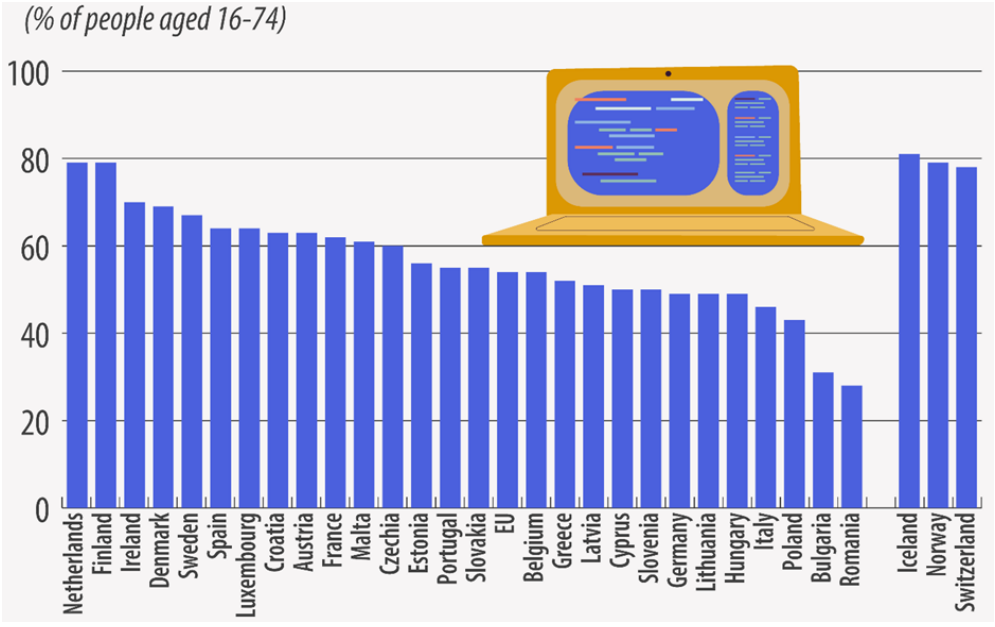

Fig. 1. People with at least basic overall digital skills in 2021
Source: EUROSTAT

Making a comparison, in the year 2023, according to EUROSTAT, of the analyzed population, the highest percentage is found in the Netherlands, and the lowest level of minimum knowledge is still occupied by Romania.

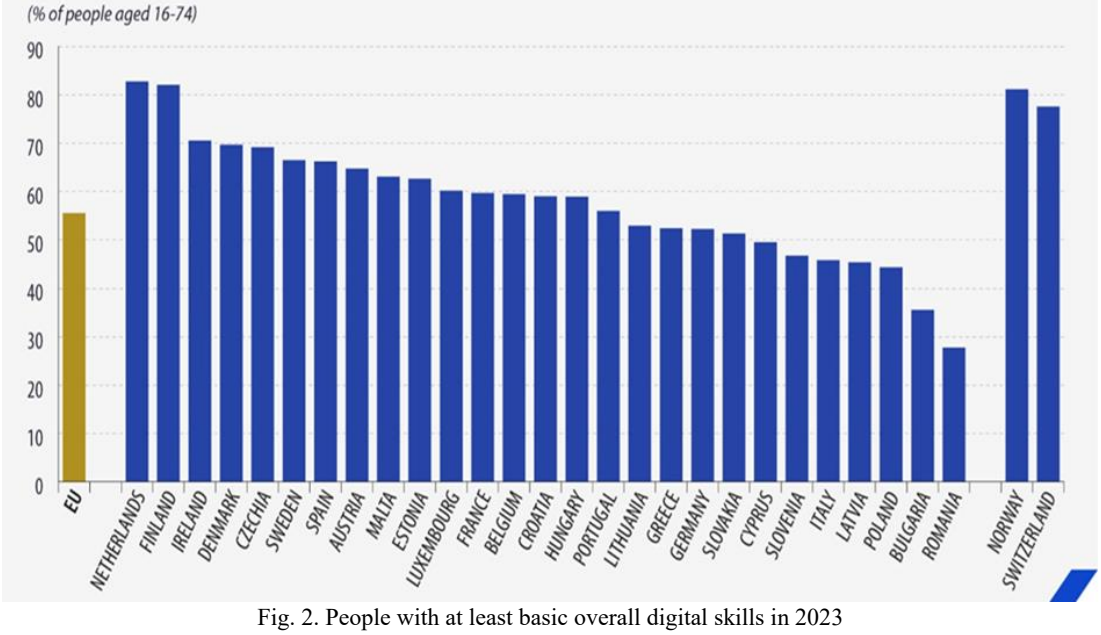

Fig. 2. People with at least basic overall digital skills in 2023
Source: EUROSTAT

Following what was presented by EUROSTAT, at the beginning of March, the European Commission proposed to transform the results of digital skills by 2023, as follows:

- Digitally literate staff and highly qualified digital professionals, 80% of adults with basic digital skills by 2030;
- Secure digital infrastructures;
- Digitization of companies, three out of four companies use cloud computing services, big data systems, and artificial intelligence;
- Digitization of public services, the possibility of accessing and processing all public services in the online system.

This Compass proposed by the European Commission for the digital dimension establishes a robust governance structure, shared with Member States, based on an annual monitoring system in the form of color codes.

3. Data Security

Data Security refers to the process of protecting digital information against potential threats. These include cyber attacks, hacking, phishing, and malware.

To prevent, detect, and respond to cyber threats, it is necessary to use physical, administrative, and technical measures. Data is a valuable asset and the document cycle is a key success factor.

Data protection is not only a legal and ethical responsibility but also a strategic necessity. A data security incident can have serious consequences, possible actions, or financial losses.

Online platforms are the important side of life and the economy.

Data confidentiality refers to the guarantee that data is accessible only to authorized personnel. Integrity assures that data is accurate and complete and has not been tampered with, and availability conveys that data is accessible when it is needed.

Another important role belongs to Technology, which has a vital part in Data Security.

In the age of digitization, the use of specialized software and hardware is becoming increasingly important. Firewalls, intrusion detection systems, encryption, multi-factor authentication, and backup solutions are some examples of technologies used to protect data and prevent security incidents.

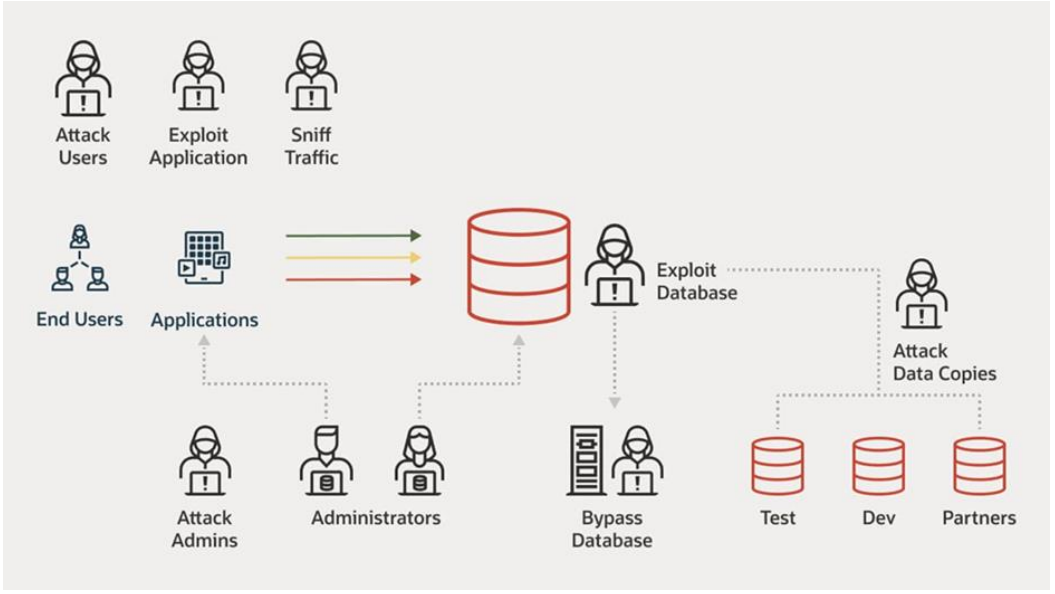

Fig. 3. What is data security?
Source: ORACLE

Data encryption is an effective solution for protecting information. This involves transforming the data into an unreadable format without using a decryption key. Thus, the data remains inaccessible to unauthorized persons, but the costs related to this procedure are very expensive and can slow down the performance of the systems.

Antivirus and antimalware software is an important solution for Data Security. These programs detect and remove malware, such as viruses, trojans, or spyware, that can compromise data security. Antivirus software often has low detection rates or may be ineffective against new threats.

Firewalls control network traffic and protect the network and data from unauthorized access. Firewalls filter data packets and can block unsafe or suspicious connections. Be careful though, they can be overcome by sophisticated attacks and require constant configuration and updates.

Cloud security services provide a scalable and efficient solution for protecting data. They include continuous monitoring of network activity, detection, and prevention of cyber attacks and secure data storage. There are also security risks associated with cloud services, such as unauthorized access to data. Consider Cloud ERP solutions in which to integrate Data Security components, for a complex and efficient IT ecosystem.

Multi-factor authentication involves using at least two authentication methods, such as password, fingerprint, or two-factor authentication. This solution adds an extra layer of security because even if an authentication method is compromised, there is still one step to verify the user's identity.

Blockchain technology can be used to secure transactions and data decentralized and transparently. This provides a method of recording and verifying information without the need for a central authority. Blockchain technology is still in development and may have limitations in terms of scalability and efficiency.

4. Data security risks

The most important risk is misusing or disclosing personal data to third parties without users' consent. The risks must be taken into account when using especially artificial intelligence for data processing and the implementation of appropriate measures to minimize them. Thus, data protection must be guaranteed regardless of the circumstances, and artificial intelligence systems must mature, adapt, and guarantee this right of citizens [7] [8].

Giving up artificial intelligence and the benefits it has in daily activities would be regrettable, it's all about risk assessment and prevention.

According to a study carried out by IPSOS regarding the degree of understanding of artificial intelligence, in Figure 4 we will find the following values:

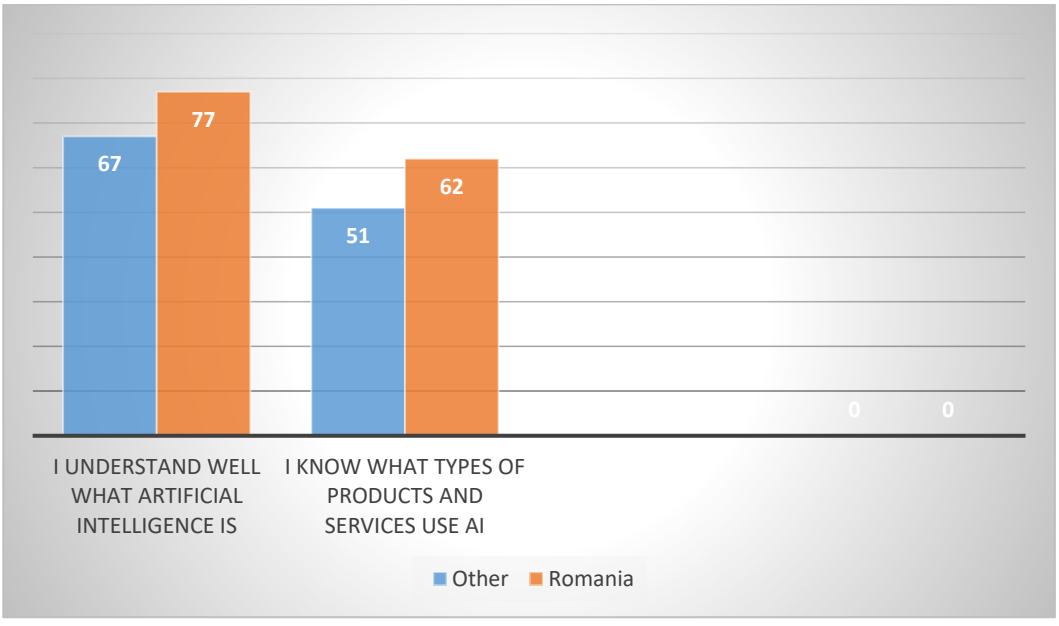

Fig. 4. What is data security?
Source: IPSOS

A total of 31 countries participated in this sampling, two-thirds 67% think they understand what artificial intelligence is, but only 51% also know what products and services use AI. This knowledge of products and services is increasing among adults, the employed, the educated, and the better-off.

Romanians think they know enough about AI, so Romania ranks 4th, with 77% of citizens claiming to know what artificial intelligence is.

In 2022, at least one Romanian out of twenty was the direct or indirect target of cyber attacks. According to INSSE, approximately 82% of households have Internet access, meaning that approximately 775,000 Romanians have received emails, messages, and calls or have been directly targeted by groups of hackers specializing in phishing, social engineering, or scamming campaigns.

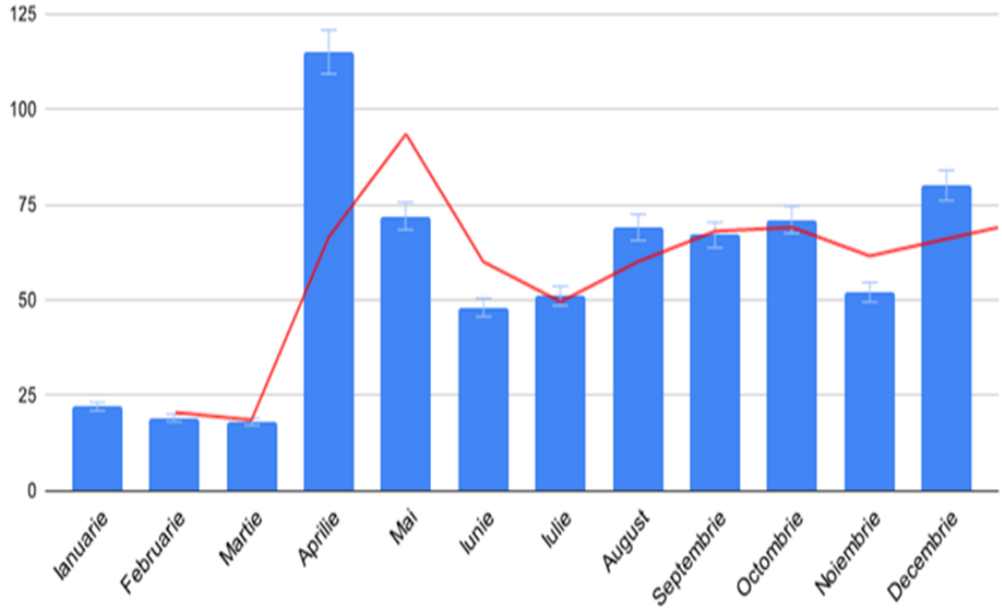

Fig. 5. Evolution of cyber attacks in 2022
Source: Hackout

Taking into account the fact that communication infrastructures are interconnected worldwide, cyber attacks [9] can be carried out from anywhere in the world, and at the same time, they can take place over very long time intervals and sometimes even without interruption, depending on the resources and technical capabilities and human that the attackers possess.

The last period has presented massive challenges regarding attempts to compromise email accounts. Such attacks are aimed at stealing access credentials (username and password) either to change them, block users' access to their own e-mails, or use the account to launch new attacks or obtain information available in these accounts.

Most of the time, these attacks present repeated attempts to identify the password or urgency, the obligation to do something in 30 seconds or minutes, which can send us an alarm signal. That is why it is advisable to have backups for important things in the digital environment, using external personal storage devices or in public clouds.

As published and recommended by the Special Telecommunications Services, an additional measure of protection is that access to various applications is protected with a second authentication factor. Second-factor authentication would make it impossible for the attacker to quickly access the account. It should only be available on the user's phone and should be changed at regular intervals.

Optimizing data protection at the individual level will also have positive consequences for the organization in which the individual works. Self-protection will be extremely useful and will provide long-term support in carrying out the activity.

5. Conclusions

SARS-COV-2 coronavirus has caused intense political, economic, and legal effects. The decree promulgated by the Government, which instituted the state of emergency, did not limit the right to the protection of personal data, at least not directly, as it would have had consequences on the right to private life according to Human Rights.

The actions of data protection supervisory authorities were put in different ways: most offered guides, and guidelines on the application of data protection rules in the context of labor relations, others made collages with the legal rules adopted during the emergency, and certain states have sanctioned operators for non-compliance with data protection rules.

Organizations must implement minimum protection measures against cyber threats. They consist of:

- Updating the IT and communication systems used;
- Implementation of authentication using 2 factors (2FA);
- Securing and monitoring services that present risks;
- Promotion of awareness campaigns and training of own users.

At the moment there are no miracle solutions that ensure 100% availability, integrity, and confidentiality of data.

Data security is a shared responsibility, it requires cooperation at the institutional level, between several categories of experts. This must be effective and materialize with the dissemination of information in real-time, as well as the exchange of knowledge and information.

References

[1] "Open security," [Online]. Available: http://www.opensecurityarchitecture.org/cms/definitions/it-risk.

[2] "Data security," [Online]. Available: https://www.microsoft.com/ro-ro/security/business/security-101/what-is-data-protection.

[3] World Health Organization, "Coronavirus disease (COVID-19) pandemic," 2020. [Online]. Available: www.who.int/emergencies/diseases/novel-coronavirus-2019.

[4] "Cybersecurity of EU institutions, bodies and agencies: Overall, the level of preparedness is not proportionate to the threats," [Online]. Available: https://op.europa.eu/webpub/eca/special-reports/hack-proofing-eu-institutions-05-2022/ro/.

[5] "Managementul riscului informatic," [Online]. Available: https://en.wikipedia.org/wiki/IT_risck.

[6] European Commision, [Online]. Available: https://commission.europa.eu/strategy-and-policy/coronavirus-response/digital-solutions-during-pandemic_ro.

[7] "Artificial intelligence in the context of data privacy," [Online]. Available: https://issuemonitoring.eu/inteligenta-artificiala-in-contextul-confidentialitatii-datelor/.

[8] "Artificial intelligence and GDPR - the impact of the use of AI on the protection of personal data," [Online]. Available: https://gdprcomplet.ro/inteligenta-artificiala-si-gdpr/.

[9] M. Simoes, M. Elmusrati, T. Vartiainen, M. Mekkane, M. Karimi, S. Diaba, W. Lopes and others, ""Enhancing data security against cyberattacks in artificial intelligence based smartgrid systems with crypto agility. arXiv preprint arXiv:2305.11652," 2023.