Cybersecurity Challenges and International Cooperation

“Balancing Personal Data Protection and Information Sharing”

Rihab Yousfi[1], Doctorate student,
Mohamed El Bachir El Ibrahimi University, Bordj Bou Arreridj, Algeria
Cyberjustice Laboratory، rihab.yousfi@univ-bba.dz
Supervisor : Wahiba Laouarem, A Lecturer at Mohamed El Bachir El Ibrahimi University,
Bordj Bou Arreridj, Algeria
Cyberjustice Laboratory، wahiba.laouarem@univ-bba.dz

Received: 19/08/2024 *Accepted: 20/10/2024* *Published:02/11/2024*

Abstract:

Cybersecurity is a fundamental pillar of the security system, essential for protecting digital infrastructure and personal data. As cybercrime and digital attacks rise, they pose significant threats to these assets. To address these threats effectively, it is imperative to establish a robust cybersecurity framework. This framework necessitates the exchange of information across national borders and the storage of data in international locations, underscoring the crucial link between international cooperation and cybersecurity. However, one of the key requirements of cybersecurity—the protection of personal data—can sometimes conflict with the demands of international collaboration.

Keywords: Cybersecurity, Personal Data,Cybercrime,International cooperation.

1. INTRODUCTION

With the increasing pace of digitization, cybersecurity and the protection of personal data have become paramount on the international scene. The growing interest in cybersecurity coincides with the expansion of international cooperation to combat cyber threats and exchange information between countries. However, this cooperation faces significant challenges ; balancing the protection of data and personal information with the need to exchange information to ensure network and system security is complex.

Cybersecurity is a vital field focused on protecting systems and networks from digital attacks and breaches that threaten data confidentiality and integrity. Concurrently, the protection of personal data is crucial. It aims to safeguard individuals’ information from unauthorized use and ensure privacy. Cooperation in information and data exchange raises complex issues. Countries must coordinate to confront digital threats while maintaining personal data protection standards. This necessity has prompted the international community and organizations to seek agreements and treaties

[1] Rihab Yousfi

to address these threats. One of the most important international agreements is the Budapest Convention, held on November 23, 2001, within the framework of the Council of Europe. It is considered the most significant international agreement to combat cybercrime.

Algeria, like the rest of the world, has sought to enact laws to combat cybercrime, face future risks and defend its cybersecurity since 2004 by amending the 2004 Penal Code through Law 04-15 and Law 04-09 on preventing and combating crimes related to information and communication technologies.

First: Defining the Topic: Given the importance of cybersecurity and the seriousness of cybercrime, it is essential to address their impact on individuals and state interests. Legal mechanisms are necessary to confront these attacks. Due to the transnational nature of cybercrime, combating it requires concerted efforts and international cooperation. This includes the exchange of information and facilitating procedures to prosecute perpetrators and obtain necessary evidence. However, this cooperation may conflict with the protection of data and personal information. This research paper will clarify these issues.

Second: Objectives of the Topic: The objectives of this research are as follows:

1. Define cybersecurity and its techniques, and identify the risks of cybercrime.
2. Highlight national and international efforts to combat cybercrime and assess their effectiveness. Address the Algerian legislator’s response to these risks that threaten security and individual interests.
3. Explain the legal mechanisms available to protect personal data against digital threats.

Third: The Research Question: This study focuses on the following main question:

To what extent is it possible to achieve effective integration between legal frameworks and policies related to cybersecurity and personal data protection to ensure information security and confidentiality of individuals in light of increasing digital threats? This question raises two sub-issues that support the topic of this study:

- Is it possible to find a balance between information exchange within the framework of international cooperation and the protection of personal data?
- To what extent are criminal legislative texts sufficient to ensure effective protection of cybersecurity?

Fourth: Research Methodology: The research methodology adopted is the deductive (analytical) and comparative approach. This approach clarifies the concept of cybersecurity and personal data protection. It also addresses the substantive aspects of enhancing international cooperation in cybersecurity matters.

Fifth: Research Plan: To answer the research question and explore the topic, this study is divided into two sections:

- **First Section: Cybersecurity and International Cooperation**

  - **First Requirement:** The concept of cybersecurity.
  - **Second Requirement:** International cooperation frameworks in cybersecurity.
- **Second Section: Protecting Personal Data in the Face of Digital Threats**
  - **First Requirement:** The definition of personal data and the importance of protecting it.
  - **Second Requirement:** Balancing the protection of personal data with international cooperation.

First Section: Cybersecurity and International Cooperation

The digital Information and Communication Technology (ICT) infrastructure and the convergence of telecommunications and information services offer significant opportunities to respond quickly to cyber threats and prevent the loss of property and money. Information security, or cybersecurity, has become a crucial pillar within the security system. It must be achieved in light of the growth of cybercrime and digital attacks that negatively affect national infrastructure, sensitive information, and personal data.

To defend against digital threats and attacks, it is necessary to build a robust cybersecurity system. The IT infrastructure is the integrated framework on which digital networks operate. This infrastructure includes the physical devices used to connect computers and users. It encompasses data centers, computers, Internet networks, submarine cables, database management systems, regulatory systems, and transportation. There are two main types of IT infrastructure: traditional infrastructure and cloud infrastructure.

On April 21, 2010, Google launched a new service called "Government Requests." This service aims to increase transparency about the requests Google receives from various governments worldwide for user data and content deletion from the Internet. The report issued by the company shows the number of requests it receives from countries and the type of data requested by governments. For example, the report indicated that France was among the countries making the largest number of requests for personal data of users during the second half of 2009[1].

The issue of cybersecurity and its realization is related to the exchange of information that crosses national borders or is stored outside the country. Hence, there is a close link between international cooperation and cybersecurity. This will be addressed through the following two requirements:

First Requirement: The concept of cybersecurity.

Cyber-attack operations include infiltrating computer systems, collecting, exporting, destroying, altering, or encrypting data, as well as planting malicious software for espionage. The complexity of these attacks is heightened by the fact that they are not exclusive to countries. Individuals, organized criminal groups, or multinational

[1] Nicolas Arpagian,La Cybersécurité,ITCIS,Alger,2014,p03.

companies may also conduct them, and their effects are dire, impacting all fields. Hence, the need for cybersecurity.

Cybersecurity is a modern term encompassing the security of open information network systems, information systems, devices, systems, and connected applications. It focuses on protecting information equipment, preventing the theft of sensitive data, countering digital hacking operations, and mitigating defamation campaigns. This reveals a conflict between various parties that are not necessarily equal. Countries can be attacked by isolated activists, commercial companies can be targeted by government intelligence services, and individuals can be attacked by other individuals. In this context, the size of communication and security budgets does not guarantee superiority.

Cybersecurity involves limiting digital attacks on programs, computers, and networks. This includes tools used to detect intrusions, stop viruses, and prevent their arrival. The following sections will define cybersecurity and present cybersecurity techniques.

Firstly: Definition of Cybersecurity

The word “cyber” refers to everything related to computer electronic networks and the Internet. It is one of the most frequently used terms in the international security lexicon. Linguistically, “cyber” is of Greek origin, derived from the word “kuberneïn.” Some historians trace its origin to Norbert Wiener, a professor at the Massachusetts Institute of Technology (1894-1964). Wiener used it to express automatic control[1], referring in a 1948 book to “the whole field of control and communication theory, whether in a machine or in an animal.”

Several decades later, science fiction author William Gibson used the term “cyberspace” in his novel *Neuromancer*. The main character is a data thief who can establish connections between his mind and a global network linking computers[2].

The origins of interest in cybersecurity date back to 1962, when the US authorities, through the Advanced Research Projects Agency (ARPA)[3], announced the desire to create a communications system that could withstand a nuclear attack from the Soviet Union. In 1969, the University of California-Los Angeles began developing the ARPANET network, which eventually became the foundation of the current Internet. In 1971, French computer engineer Louis Pouzin led the “Cyclades” project, connecting 25 computers in France, Italy, and the UK. This allowed researchers to collaborate remotely and develop a global network based on packet switching. In 1973, the University of California-Los Angeles (UCLA) and Robert Kahn of ARPA built a communications protocol. However, the Cyclades project was halted in 1979 due to a lack of funding from the French government, which did not prioritize it. Consequently, the United States continued to develop this sector.

[1] Mouni Abdullah Al-Samhan, Requirements for Achieving Cybersecurity for Administrative Information Systems at King Saud University, Journal of the Faculty of Education, Mansoura University, Issue 111, July 2020.

[2] Nicolas Arpgian,op.cit,p07.

[3] ARPA (advanced Research Project Agency).

Gradually, the term "cyber" has contributed to the construction of new names related to the information society that emerged at the end of the twentieth century. Cybersecurity is therefore related to the defensive and offensive uses of these information systems, which include technical means such as information networks, telephone networks, and satellites.

There are many definitions of cybersecurity. It is defined as "a set of actions taken in the field of defense against cyber attacks and their consequences, including the implementation of required countermeasures." Cybersecurity is also defined as "the set of technical and administrative means used to prevent unauthorized use and misuse, and to recover electronic information, communication systems, and the information they contain.[1]"

Based on its objectives, cybersecurity is defined as "the activity that ensures the protection of human and financial resources associated with information and communication technologies. It ensures the possibility of limiting losses and damage in the event of risks and threats, and allows the situation to be restored as soon as possible so that production does not stop and damage does not turn into permanent losses.[2]"

Cybersecurity is "the activity, process, capability, or information and communication systems of a country where the information contained therein is protected from any motive of damage, unauthorized use, modification, or exploitation."

Cybersecurity involves taking necessary measures to protect cyberspace from cyber attacks. This includes technical, organizational, and administrative means to prevent illegal access to electronic information and its exploitation. The aim is to maintain the continuity of systems and the information they contain, ensuring privacy and confidentiality through necessary data protection measures and procedures.

In the International Telecommunication Union (ITU) report on Telecommunication Reform Trends 2010-2011, cybersecurity is defined as "a set of tasks such as compiling security tools, policies, procedures, guidelines, risk management approaches, training, best practices, and technologies that can be used to protect the cyber environment, organizational assets, and users."

The U.S. Department of Defense defines cybersecurity as "a set of tools, policies, procedures, guidelines, risk management approaches, training, best practices, and technologies that can be used to protect the cyber environment, organizational assets, and users."

The U.S. Department of Defense also provides a precise definition of cybersecurity as "all organizational actions necessary to ensure the protection of information in all its physical and electronic forms, from various crimes: attacks, sabotage, espionage, and incidents."

[1] Khaled Mamdouh Ibrahim, Digital Judicial Expertise in Cybercrime (a comparative study in Egyptian, UAE and US law), first edition, Dar Al-Fikr Al-Jami'i, Alexandria, 2023. P 114

[2] Samir Bara, Cybersecurity in Algeria: Policies and Institutions, Algerian Journal of Human Security, Issue 4, July 2017. p 257

The European Declaration defines cybersecurity as “the ability of an information system to resist intrusion attempts targeting data.”

Cybersecurity is also defined as “the desirable state of information and communication systems that gives them the ability to resist and counter everything from cyberspace that could expose stored, processed, or transmitted information to damage, alteration, or espionage.[1]”

It should be noted that cybersecurity is a broader concept than information security. Cybersecurity concerns the security of everything in cyberspace, while information security focuses on the security of physical information. Cybersecurity is not concerned with physical information security.

Cybersecurity is related to several concepts, the most important of which are cyberspace, cyberattacks, and cybercrime:

- **Cyberspace:** The French Agency for Information Systems Security (ANSSI) defines cyberspace as “the communication space formed by the global interconnection of equipment for the automated processing of digital data. It includes physical and non-physical elements, consisting of a set of digital devices, network systems, software, and users, whether operators or users.”
- **Cyberattacks:** Cyberattacks are defined as “any act that undermines the capabilities and functions of a computer network for national or political imposition, by exploiting a specific vulnerability that enables the attacker to manipulate the system.”
- **Cybercrime:** Cybercrime is defined as the set of illegal acts and actions carried out through electronic equipment, devices, the Internet, or the transmission of its contents. It is also defined as “crimes that have to do with computers, their information, and social networks.[2]”

Secondly: Cybersecurity Technologies

With the growing digital information exchange processes on the Internet, and the absence of a digital anchor for these exchanges, it has become necessary to generalize advanced technologies. These technologies, created by network users, help secure the protection, security, and confidentiality functions urgently required for exchanging sensitive data online.

There are many protection techniques adopted in cybersecurity, varying according to needs. The first of these techniques is encryption. Other available techniques include programs that provide anonymity, known as “Anonymous Remailers,” firewalls, updates, intrusion detection systems, data loss prevention techniques, and security engineering.

[1] J. Radwan, “Cybersecurity is a Priority in Defense Strategies, Al-Jaich Magazine, Issue 630, January 2016. p 40 - 41

[2] Mostafa Mohamed Moussa, Criminal Investigation in Cyber Crimes, first edition, Police Press, Cairo, 2008. p 112

1- **Information Encryption:** Encryption techniques are at the forefront of providing security and safety for information and transactions exchanged on the Internet. These techniques not only protect and ensure the confidentiality of digital messages but also strengthen information evidence. Encryption uses advanced technologies and specialized software, offering effective protection for subscribers’ files and preventing unauthorized access[1].

   Encryption itself is not new. Encrypted and coded writing has existed since ancient times and is still primarily used in military and diplomatic intelligence[2].

   There are several definitions of encryption. One definition is: “Encryption or coding is a mechanism by which understandable information is translated into incomprehensible information through the application of secret protocols that are reversible, allowing the information to be returned to its original state.”

   Encryption agreements in information technology can be categorized into two main types. The first uses a private key and is called symmetric encryption technology. The second uses a public key and is called asymmetric encryption technology.

   In the United States and Canada, the use of encryption methods is unrestricted domestically. However, their export requires a license from state authorities due to their classification as war munitions under the International Traffic in Arms Regulation (ITAR). In Europe, most European Union member states have legal regulations prohibiting the export of encryption programs. These programs are generally classified as weapons equipment and are subject to prior authorization. In France and Belgium, encryption is considered related to public and national security, necessitating a licensing and authorization system[3].

   The use of encryption tools and programs in the Internet era presents a dilemma for countries and their governments. They must balance protecting the confidentiality and security of information and exchanges on the Internet with addressing the risks and repercussions of advanced information technology in producing encryption tools.

2- **Anonymity Technology:** This service is available from Internet service providers and is offered as an additional service to subscribers. It erases all elements identifying the real owners of messages and then sends them to their destinations with anonymous addresses. This technology can be

[1] Hocine Taheri, Cybercrime, first edition, published by Dar Al-Khalduniya, Algeria, 2022. p 446.

[2] Pauline Antonius Ayoub, Legal Protection of Personal Life in the Field of Informatics - A Comparative Study, Halabi Law Publications, Lebanon, 2009. p 229.

[3] Pauline Antonius Ayoub. op. cit. p 240.

misused, leading to negative consequences. Prominent negative uses include criminal activities, incitement to violence, racial hatred, defamation, or libel.

Under the Internet Protocol (IP), which deals with data addressing in the network, it is possible to know the server used by the network user to connect to other sites. Techniques allow tracing the path of the connection to identify the geographical location of the distributor who provided network access. This can reveal the true identity of the network user if relative anonymity is traceable. For example, the Finnish judiciary faced this issue in a lawsuit filed by the Church of Scientology. It was found that the complained subscriber was a US citizen, forcing the organization to pursue him before the US judiciary[1]. Absolute anonymity, which is not traceable, means that the provider of communication services uses anonymous repeaters that achieve complete anonymity, unlike devices that provide relative anonymity.

3- **Anti-malware Programs:** These programs help combat malware by detecting and removing malicious software and viruses from systems.

4- **Firewalls:** Firewalls protect systems from intrusion by monitoring traffic between the internal and external networks.

5- **Updates:** Regularly updating software and systems closes security gaps and enhances overall security.

6- **Intrusion Detection Systems:** These systems monitor network traffic to detect and prevent unwanted intrusions.

7- **Identity Management:** This technology allows users to access resources based on their permissions, reducing the risk of unauthorized access and ensuring that only authorized persons connect to systems or networks.

8- **Data Loss Prevention Technologies:** This technology prevents unauthorized data leakage.

9- **Security Monitoring:** Security monitoring allows organizations to track cyber activities and analyze incidents for rapid response.

10- **Security Engineering:** Through security engineering, systems and networks are designed to be more resistant to attacks.

Second Requirement: Frameworks for International Cooperation in Cybersecurity

[1] Tony Michel Issa, Legal Organization of the Internet, a comparative study in the light of positive laws and international conventions, first edition, Lebanon, 2001. p 405.

Due to the seriousness of cybercrime and the rapid development of technology, exploiting the Internet for criminal purposes has become easier. Criminals can enter networks, obtain data, and then change or destroy it. These digital attacks are transnational and do not recognize geographical borders. Therefore, it is necessary to combine international efforts to confront these attacks that target state security and individual interests, affecting cybersecurity.

International organizations have affirmed the human right to the sanctity of private life from data attacks. At the regional level, the Council of the European Union has issued several binding directives and recommendations to address the illegal use of computers and information networks. These directives represent the minimum standards that EU countries must adhere to when preparing their related legislation[1].

Among the most important results of these efforts is the Budapest Convention on Cybercrime. The General Secretariat of the League of Arab States sought to adopt a unified Arab convention to combat cyber terrorist crimes. Similarly, the African Union and the United States have adopted special conventions to address terrorist crimes via the Internet. The following sections will present international conventions and treaties related to cybersecurity, and cooperation between countries at the regional level.

Firstly: International Efforts Related to Cybersecurity

The importance of international cooperation lies in the need for the global community to recognize the dangers of cyber and digital attacks and their impact on cybersecurity. Many international bodies and organizations play a significant role in concluding agreements to establish the necessity of international cooperation to confront computer crimes and digital attacks. Leading these efforts are the United Nations, the Council of Europe, and other bodies. This section presents the efforts made by these organizations.

1. United Nations Efforts in the Field of Cybercrime:

The United Nations is making significant efforts to address computer crime and emphasize the need for joint action among its members. This cooperation aims to limit the spread of information technology crimes through international conferences on crime prevention and the treatment of criminals, as well as through international agencies operating under its auspices[2].

The United Nations has been working to ensure the safe use of technology and information networks. Its various agencies are involved in negotiations to find

[1] Omar Abbas Khudair Al-Obeidi, Procedural obstacles to combating terrorist groups via the Internet and ways to overcome them, Drop Al-Maarifa for Publishing and Distribution, Alexandria, 2022. p 130 – 131.

[2] Rachida Boker, Crimes of Assault on Automated Processing Systems in Comparative Algerian Legislation, first edition, Halabi Law Publications, Lebanon, 2012. p 132.

consensus on several issues, including the development of standards for the protection of Internet networks[1].

Regarding crime prevention conferences, the Seventh Congress, held in Milan, Italy, in 1985, mandated the Twentieth Committee of Experts to study the issue of protecting automated processing systems and computer attacks. They were to prepare a report for the Eighth Congress[2]. The Ninth Congress on the Prevention of Crime and the Treatment of Offenders, held in Cairo in 1995, recommended protecting individuals' private lives and intellectual property. The Tenth Congress, held in Budapest, Hungary, in 2000, recommended serious efforts to reduce emerging crime patterns.

Among the most prominent resolutions is United Nations General Assembly Resolution No. 57-239 on establishing a global culture of cybersecurity. This resolution, along with others on cybersecurity, effective crime prevention, and criminal justice to combat the sexual exploitation of children, highlights the importance of these issues. The International Telecommunication Union (ITU), which includes 192 countries and 700 private sector companies, provides a strategic platform for cooperation as a specialized agency within the United Nations[3].

2. The Role of the European Council:

As part of the European Union's efforts to combat cybercrime, the Budapest Convention, signed on November 23, 2001, is one of the most important agreements in this field. It addresses crimes against automated processing systems and information technology. The Convention focuses on key interests within automated processing systems and includes provisions for judicial assistance in combating cybercrime[4]. It emphasizes the necessity of international cooperation between states, particularly in information exchange.

The International Society of Penal Law has also addressed this topic through various conferences. Notably, the Norwegian conference in Oslo in 2000 discussed the impact of digital attacks, such as the "Love Bug" virus. Additionally, the G8 countries have made significant efforts to cooperate in protecting against computer crime[5].

Secondly: Regional and Arab Cooperation in Cybersecurity

In addition to the efforts of the United Nations, other significant efforts have been made through conferences on crime prevention and the treatment of criminals, as well as human rights conferences. Notable examples include the Tehran Conference in 1968 and the Vienna Conference in 1993. Specialized agencies such as the World Intellectual Property Organization (WIPO) have also contributed, alongside the Council of Europe.

[1] Lahcen Nani, Investigation of IT-related crimes between legislative texts and technical privacy, New University Publishing House, Tlemcen, 2018. p 39.

[2] Mahmoud Ahmed Ababneh, Computer Crime and its International Dimensions, first edition, Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 2009. p 156.

[3] Lahcen Nani. op. cit. p 41

[4] M.M. Omar Abbas Khudair Al-Obeidi, The Concept of Crimes Resulting from the Electronic Currency (Bitcoin) and its Applications in the Crimes of Financing Terrorist Groups and Money Laundering, first edition, Arab Center for Publishing and Distribution, Egypt, 2021. p 212.

[5] Mahmoud Ahmed Ababneh. op. cit. p 180;

At the regional level, several important conferences and forums have been held:

- Fifth International Cybersecurity Conference for Law Enforcement, Industry, and Academic Experts, New York, 2015.
- Seventh Regional Conference on Digital Forensics and Cybercrime, Seoul, South Korea, 2015.
- Third Regional Conference on Cybersecurity, Muscat, 2014.
- First Regional Conference on Combating Cybercrime, Riyadh, 2015.
- Criminalization of Cyber Terrorism Forum, Abu Dhabi, 2017.

In addition to these efforts, the League of Arab States, as an Arab regional organization, has sought to address illegal activities committed through information technology. A significant highlight of these efforts is the adoption of the Unified Arab Penal Code by the Council of Arab Ministers of Justice as a model law. This code includes a chapter on the violation of rights resulting from information technology[1]. The twelfth meeting of the Committee on Emerging Crimes in 2004 focused on credit card fraud.

The most important convention signed by Algeria in the field of information technology is the Arab Convention on Combating Information Technology Crimes, ratified by Presidential Decree 14-252.

Second Section: Protecting Personal Data in the Face of Digital Threats

The protection of individuals’ private lives enjoys constitutional and legal safeguards in various state legislations due to the paramount importance of privacy. The right to privacy is an inherent right of the individual. In its modern form, private life is represented in information banks associated with technology. This private life is threatened by numerous violations and attacks, especially with the emergence of the Internet and the information highway. Traditional texts are powerless against these attacks on individuals’ privacy and secrets. To protect the privacy of communications and personal data, laws must be enacted to strengthen cybersecurity and protect data from digital threats.

First Requirement: The Concept of Personal Data Protection

The issue of personal data is not about the stored information itself, but the interests threatened by incorrect or distorted information. Personal data has become a highly valuable resource as individuals and companies rely on it to make decisions and develop services. With the increasing use of technology in the collection, storage, and exchange of personal data, new legal challenges have emerged related to its protection from unlawful exploitation. Algeria is among the countries striving to protect personal data, as stipulated by law. Many countries have made significant efforts to establish a legal framework ensuring effective protection of personal data. Algeria, through Law 18-07 on the protection of natural persons in the field of processing data of a personal nature, has taken an important step towards strengthening legal guarantees to protect personal

[1] M.M. Abbas Khudair Al-Obeidi, Procedural Obstacles to Countering Terrorist Groups via the Internet and Ways to Overcome Them, Droob Al-Maarifa for Publishing and Distribution, Alexandria, 2021. p 137.

data amidst continuous technological development. In the first section, we will define personal data and its importance. In the second section, we will address international and local legislation related to personal data protection.

Firstly: Definition of Personal Data and the Importance of Protecting It

Personal data is any information that enables the direct or indirect identification of a person. This includes family name, personal name, identification card number, address, email address, voice, and image. The Algerian legislator defines personal data in Article 3 of Law 18-07[1] as “any information, regardless of its basis, related to an identified or identifiable person, referred to below as the person concerned, directly or indirectly, especially by reference to the identification number or one or several elements related to their physical, physiological, genetic, biometric, psychological, economic, cultural, or psychological identity.” In the same context, it defines a “data subject” as any natural person whose personal data is the subject of processing.

The Algerian legislature also defines the processing of personal data in the same article as “Any operation or set of operations performed with or without automated methods and means on personal data. This includes collecting, recording, organizing, saving, adapting, altering, extracting, accessing, using, or communicating by transmission, publication, or any other form of availability. It also includes approximation, interconnection, locking, encryption, erasure, or destruction.

Some define automated processing of personal data as any process or set of processes, with or without automation, applied to personal data. This includes collection, recording, organization, preservation, adaptation, modification, alteration, extraction, access, use, communication by transmission, broadcasting, or any other form of making information available.

Secondly: International and Local Legislation Related to the Protection of Personal Data

The violation of privacy in data transmission over networks that lack complete security for data confidentiality is a significant concern. Messages exchanged via email can be intercepted and transcribed, and data files belonging to others can be accessed illegally. This raises questions about the efforts made to confront the risk of violating individuals’ privacy, which has increased with the rise in Internet users and those dealing with information systems.

In the following sections, we present the efforts made to protect personal data in the face of information systems. First, we will discuss international efforts in this regard. Second, we will examine the path of local legislations.

1. International Efforts to Protect Personal Data in the Face of Information Systems

[1] Law 18-07 of June 10, 2018 on the protection of natural persons in the field of processing personal data, published in the Official Journal No. 34 of June 10, 2018.

The United Nations has made significant efforts to protect private life against technical progress and safeguard individuals and their freedoms from infringement. These efforts culminated in the first International Conference on Human Rights, held in Tehran in 1968. The conference highlighted that electronic computers pose the greatest threat to private life and personal freedom, as they are modern surveillance tools and snooping devices. When personal data is stored on computers and analyzed, it reveals patterns of interaction and relationships.

At the regional level, the Council of Europe has played a crucial role. The Council of Europe Convention on the Protection of Persons against the Risks of Automatic Processing of Data of a Personal Nature was signed and entered into force in October 1958[1]. Additionally, the Council of Europe has issued several recommendations to expand protection, most notably Recommendation No. 13/R80 in 1980 on the exchange of legal information related to data protection.

The Organization for Economic Cooperation and Development (OECD) has also contributed significantly. The OECD Guidelines on Privacy Protection and Personal Data Flows are well-known efforts in this regard.

The General Data Protection Regulation (GDPR**)** is the European Union's comprehensive framework for protecting personal data. It aims to strengthen individuals' rights to control their personal data and promote transparency in its collection and processing.

The Convention for the Protection of Individuals with regard to the Processing of Personal Data, developed by the European Commission, is the first international agreement to address personal data protection.

Personal data is protected by the right to privacy under international human rights instruments. For example, the European Court of Human Rights ruled that phone data, emails, usage, and data stored on computer servers against Austria fell within the scope of protection under the European Convention on Human Rights. Additionally, the African Union Convention on Cybersecurity and Personal Data Protection of 2014 covers the right to respect for personal data.

2. The Behavior of Local Legislation in Protecting Personal Data in the Face of Information Systems

In addition to international and regional data protection laws, countries and intergovernmental organizations have developed and implemented their own laws. The Algerian legislator, like others, has enacted Law 18-07 on the protection of natural persons in the field of processing personal data. This law is an important step towards organizing the protection of personal data. One of its basic principles is prior consent,

[1] Mohammed Amin Al-Shawabkeh, Computer and Internet Crimes, first edition, Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 2009. p 73.

meaning that personal data processing can only occur with the explicit consent of the person concerned.

A body called the National Authority for the Protection of Personal Data has been established to ensure compliance with this law. It ensures that the use of information and communication technologies does not pose risks to human rights, public freedoms, and private life.

Germany was the first country to address information privacy under the law of the state of Hessen in 1970, making it a pioneer in legislative data protection. In 1977, Germany issued the Data Protection Law. Sweden followed in 1973 with a law to protect personal data, and France issued the "Information and Freedoms" law in 1978[1].

In the United States, only certain types of data collected, stored, analyzed, and shared by private companies are regulated. Mexico has two data protection laws: the Federal Law on the Protection of Personal Data Held by Private Parties of 2010, which regulates the private sector, and the General Law for the Protection of Personal Data in the Possession of Binding Subjects of 2017, which regulates the public sector. Mexican law includes provisions for private data related to cloud services, including regulating law enforcement access to data stored in the cloud and the processing of data after the termination of cloud services.

In Canada, a privacy protection law was enacted that includes ten principles to protect privacy on the information superhighway[2]. Similar laws exist in China, Austria, and Belgium. The Tunisian legislator provided special protection for personal data in the face of technological development under the Electronic Commerce Law of 2000 and issued the Personal Data Protection Law in 2004.

Second Requirement: Balancing the Protection of Personal Data and International Cooperation

In the era of high technology and rapid information movement, the exchange of information between countries has become an urgent necessity. Information now crosses national borders and does not remain within a specific geographical space. However, this inevitable international cooperation faces significant challenges related to the protection of personal data.

In the first section, we will present the challenges faced by information exchange and the protection of personal data. The second section will address the solutions and strategies to enhance international cooperation and protect personal data.

Firstly: Challenges to Information Sharing and Personal Data Protection

In 2008, the Federal Bureau of Investigation (FBI) shut down a platform for hiding stolen data. This forum, dubbed "The Dark Market," provided its 2,500 global clients with banking information (credit card numbers, access codes to individual bank

[1] Aicha Ben Kara Mustafa, The Right to Information Privacy Between Technical Challenges and the Reality of Legal Protection, Arab Journal of Science and Research Dissemination, Issue 2016. p 47.

[2] Mohammed Amin Al-Shawabkeh. Op. cit. p 25

accounts, etc.) captured through fraudulent online transactions. This allowed perpetrators to embezzle money deposited in distant banks quietly and non-violently.[1]

In the summer of 2009, Albert Gonzalez was arrested in the United States after committing a series of bank card fraud operations. He hacked about 130 million accounts using computer servers in the United States, Latvia, the Netherlands, and Ukraine. In 2010, the computer company Netwitness announced that a hacking campaign had seized 74,000 computers in more than 200 countries, including the United States, Saudi Arabia, Egypt, and Turkey. Cyber attacks no longer target specific groups or countries but are transnational. Despite calls for international cooperation in this field, there are obstacles that prevent this. Some difficulties can be outlined as follows:

1. Differing National Legislation: There is no single agreed-upon model regarding criminal activity, nor is there a unified legal framework for the misuse of information systems. Personal data protection laws vary from one country to another, complicating the exchange of information and creating legal contradictions. Some countries impose strict restrictions on data transfer, while others are less stringent.

2. Lack of Coordination: There is a lack of coordination regarding criminal procedures between different countries, especially concerning evidentiary or investigative work. Obtaining evidence in such crimes outside the state's borders through inspection is very difficult.[2]

3. Government and Security Secrets: Sharing information and allowing access to personal data may pose a security threat, especially if it involves national security secrets. This raises concerns about the leakage of sensitive information to unauthorized parties.

4. Privacy and Individual Consent: Ensuring the consent of individuals to share their information across borders is crucial. This consent must be clear and explicit, requiring transparent mechanisms and international approval.

5. Protection of Trade Secrets: Companies sharing their data with international partners may worry that their data could be used for illicit purposes.

Secondly: Strategies for Strengthening International Cooperation and Protecting Personal Data

States and international organizations are seeking to develop solutions to protect personal data in light of international cooperation. Among the strategies to enhance international cooperation and protect personal data are the following:

[1] Nicolas Arpagian. Op. cit. p 16

[2] Abdel Fattah Bayoumi Hegazy, Criminal Evidence in Computer and Internet Crimes, Legal Books House, Egypt, 2007. p 190.

1. Developing Global Regulatory Frameworks: It is necessary to create and develop international regulatory frameworks that provide unified standards for the protection of personal data. These frameworks will help unify legislation and reduce legal gaps.

2. Enhancing International Cooperation: International cooperation must be strengthened through the exchange of knowledge and experience in the field of data protection.

3. Adopting Modern Technologies: This involves using encryption techniques and modern security solutions.

Conclusion :

The importance of international cooperation in the field of cybersecurity and combating cybercrime lies in the nature of these crimes as non-national. International cooperation impacts the convergence and compatibility of legislation against cybercrime, leading to the creation of a common legal system to combat this phenomenon. The importance of international cooperation is evident in the varying roles of law enforcement authorities from one country to another, which can hinder the effectiveness of combating cybercrime. This calls for concerted international efforts through the application of international cooperation in criminal matters.

In light of the above, our study on cybersecurity and international cooperation highlights the difficulties posed by data protection. The process of seizing electronic data may conflict with the right to privacy. Additionally, differences in national legislation and lack of coordination regarding criminal procedures between different legislations pose obstacles to prosecuting perpetrators of these attacks. Based on these findings, we propose the following:

1. **Adopt a Unified International System:** Establish a unified international system based on cooperation between various countries within a unified policy and procedural framework.
2. **Combine International Efforts:** Harmonize criminal policies to address cybersecurity violations by creating international agreements that align with national legislation and respect sovereignty.
3. **Train Human Competencies:** Develop professional national capabilities in cybersecurity by training human resources and establishing criminal laboratories equipped with advanced technologies, managed by specialized technical teams.
4. **Legislative and Judicial Cooperation:** Promote legislative and judicial cooperation to achieve cybersecurity through agreements and treaties, leveraging the experiences of developed countries in combating cybercrime.

BIBLIOGRAPHY

I. **Legal texts:**

1. Law 04-15 of 10/11/2004 amending and supplementing Ordinance 66-156 containing the Penal Code, Official Journal No. 71 of 10/11/2004.

2. Law 09-04 of August 05, 2009, containing the rules for preventing and combating crimes related to information and communication technologies.
3. Law 18-07 of June 10, 2018 on the protection of natural persons in the field of processing personal data, published in the Official Journal No. 34 of June 10, 2018.

2. Books:

4. Pauline Antonius Ayoub, Legal Protection of Personal Life in the Field of Informatics - A Comparative Study, Halabi Law Publications, Lebanon, 2009.
5. Hossein Taheri, Cybercrime, first edition, published by Dar Al-Khaldounia, Algeria, 2022.
6. Khaled Mamdouh Ibrahim, Digital Judicial Expertise in Cybercrime (a comparative study in Egyptian, UAE and US law), first edition, Dar Al-Fikr Al-Jami'i, Alexandria, 2023.
7. Rachida Boker, Crimes of Assault on Automated Processing Systems in Comparative Algerian Legislation, first edition, Halabi Law Publications, Lebanon, 2012.
8. Tony Michel Issa, Legal Organization of the Internet, a comparative study in the light of positive laws and international conventions, first edition, Lebanon, 2001.
9. Abdel Fattah Bayoumi Hegazy, Criminal Evidence in Computer and Internet Crimes, Legal Books House, Egypt, 2007.
10. Omar Abbas Khudair Al-Obeidi, Procedural obstacles to combating terrorist groups via the Internet and ways to overcome them, Drop Al-Maarifa for Publishing and Distribution, Alexandria, 2022.

11. Mostafa Mohamed Moussa, Criminal Investigation in Cyber Crimes, first edition, Police Press, Cairo, 2008.

12. Mahmoud Ahmed Ababneh, Computer Crimes and their International Dimensions, first edition, Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 2009.

13. M.M. Omar Abbas Khudair Al-Obeidi, The Concept of Crimes Resulting from the Electronic Currency (Bitcoin) and its Applications in the Crimes of Financing Terrorist Groups and Money Laundering, first edition, Arab Center for Publishing and Distribution, Egypt, 2021.

14. M.M. Abbas Khudair Al-Obeidi, Procedural Obstacles to Countering Terrorist Groups via the Internet and Ways to Overcome Them, Droob Al-Maarifa for Publishing and Distribution, Alexandria, 2021

15. Mahmoud Ahmed Ababneh, Computer Crime and its International Dimensions, first edition, Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 2009.

16. Mohammed Amin Al-Shawabkeh, Computer and Internet Crimes, first edition, Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 2009.

17. Lahcen Nani, Investigation of IT-related crimes between legislative texts and technical privacy, New University Publishing House, Tlemcen, 2018.

18. Nicolas Arpagian,La Cybersécurité,ITCIS,Alger,2014.

3: Articles:

19. Samir Bara, Cybersecurity in Algeria: Policies and Institutions, Algerian Journal of Human Security, Issue 4, July 2017.

20. Aicha Ben Kara Mustafa, The Right to Information Privacy Between Technical Challenges and the Reality of Legal Protection, Arab Journal of Science and Research Dissemination, Issue 2016.

21. J. Radwan, “Cybersecurity is a Priority in Defense Strategies, Al-Jaish Magazine, Issue 630, January 2016.

22. Mouni Abdullah Al-Samhan, Requirements for Achieving Cybersecurity for Administrative Information Systems at King Saud University, Journal of the Faculty of Education, Mansoura University, Issue 111, July 2020.