ITJ | The International Tax Journal

Digital gaps and challenges of legal security

Derdiche Brahim [1] and **Nessil Omar** [2]

[1] Doctoral Student, Laboratory of Tourism, Region and Institutions, Faculty of Law and Political Sciences, University of Ghardaia, (Algeria). Email: derdiche.brahim@univ-ghardaia.edu.dz
[2] Doctor, Laboratory of Tourism, Region and Institutions, Faculty of Law and Political Sciences, University of Ghardaia, (Algeria). Email: omarnessil@yahoo.fr

Abstract---The rapid scientific development witnessed by the world has turned it into a small village, leading to many technological transformations that have impacted various communities and groups. These changes have influenced the patterns of economic, social, cultural, and other aspects of life. The spread of modern technologies, social media, digital applications, and others has posed a significant threat to the social fabric and the balance that ensures legal security. Despite the numerous advantages of the virtual environment on minds and their thinking patterns, as well as the scientific and life approaches they adopt, this is accompanied by many negative consequences that have become substantial threats and challenges to society as a whole. Hence, the importance of information security arises, along with how to employ its diverse methods and various applications to confront these threats. The role of information services and its functions as a profession, with its methodologies, models, and scientific approaches, significantly contribute to protecting all segments of society from becoming victims of many different problems and challenges, including threats from the digital environment. This is where the idea for this research paper originated, aimed at identifying the threats of the digital environment and the role of information security in addressing them. Subsequently, it seeks to propose a vision from an advanced digital perspective to tackle this issue.

Keywords---digital communication, technological advancement, legal security, cybercrime, artificial intelligence.

1. Introduction:

Communication in the field of contemporary technological sciences, within the digital environment, has several features that elevate humans from traditional interaction to an advanced digital world. These modern technologies were not born by mere chance, but rather through stages that had various

How to Cite:
Brahim, D., & Omar, N. (2025). Digital gaps and challenges of legal security. *The International Tax Journal, 52*(3), 224–234. Retrieved from https://internationaltaxjournal.online/index.php/itj/article/view/57

The International tax journal ISSN: 0097-7314 E-ISSN: 3066-2370 © 2025

Submitted: 07 February 2025 | Revised: 15 March 2025 | Accepted: 29 April 2025

impacts, some positive and others negative, across all fields; particularly regarding the challenges citizens face, distancing them from their legal security. Although humans are the ones who programmed this entire development—applications, computer software, and the Internet—there remains a type of imbalance in the regulation and protection of legal security, which has now become an urgent necessity.

This situation requires numerous measures to protect consumer rights and to safeguard digital security assets, which has become a fundamental requirement amid this astonishing technological advancement that grows day by day. This is achieved through enacting multiple laws that generally control the situation, especially due to the widespread global rise of cybercrimes.
In the health sector, for example, cutting-edge technologies supported by artificial intelligence are helping save lives, diagnose diseases, and extend life expectancy.

In education, virtual learning environments and distance learning have facilitated access to programs for students who would have otherwise been excluded. Similarly, thanks to the assistance provided by artificial intelligence, public services have also benefited. Moreover, the way these developments are managed is subject to considerable debate, both nationally and internationally.

1. **Importance of the Study Topic:** The challenges facing societies in the realm of legal security, particularly in light of the rapid and astonishing technological development, especially regarding privacy violations, render this topic extremely important in all aspects of cultural, legal, financial, and commercial life, among others. This necessitates addressing the difficulties associated with the use of modern scientific technologies. All the issues raised require a thoughtful confrontation, accompanied by legal support, which leads us to pose questions that we will discuss along with the key findings and recommendations reached.
   Thus, we posed the following questions for the research paper:
   - What are the gaps that have accompanied digital development?
   - What challenges face legal security?
   - How can these security challenges be addressed in the context of digitization?
2. **Reasons for Choosing the Topic:** Among the main motivations for selecting the fourth topic as a research paper are:
   A. **Subjective Reasons:** The desire to discover the intricacies of the advanced technical world that surrounds us, to understand it, and to study its hidden aspects, especially given the challenges posed by legal security.
   B. **Objective Reasons:** An attempt to confront the dangers threatening legal security, particularly with the emergence of legal gaps and deficiencies in dealing with modern scientific technologies.
3. **Study Objectives:** To achieve a secure digital environment that keeps pace with digital technological development while maintaining the pillars of legal security.
4. **Previous Studies:** To reach an original conclusion and idea, it is essential to rely on high-quality references that are directly related to the topic. This study draws on books and conferences organized in various countries, which clearly demonstrates the interest related to technological development. I have blended older works, such as Dr. Saleh Joad Kazem's "Modern Technology and Personal Privacy," which, while not explicitly addressing the term legal security, implicitly refers to it. When we mention personal privacy, we refer to one of the legal guarantees for individual freedom and data protection, which are among the guarantees and components of legal security. Our reliance on recent references cannot be overlooked when discussing a topic related to legal matters, such as Dr. Jamal Muhammad Ghaitas's "Information Security and National Security."

To address the issue presented in the study, we divided it into three main axes. In the first axis, we discussed the challenge arising from the loss of centralization and control mechanisms. In the second axis, we addressed the risks threatening privacy, and we concluded with the protection of personal privacy according to the following plan:

- **First Axis:** The challenge arising from the loss of centralization and control mechanisms
- **Second Axis:** The risks threatening privacy
- **Third Axis :** Protection of privacy

First Axis: The Challenge Arising from the Loss of Centralization and Control Mechanisms
The enactment of a national law or the development of a suitable national strategy to protect citizens may be effective due to the elements of control, sovereignty, and the presence of an authority capable of oversight and preventing violations or their continuation, which also allows for compensation and the pursuit of offenders. However, what is the situation in the context of the internet, which is owned by every individual and not by anyone specifically, lacking a central authority or sovereign body that provides protection or opportunities for legal protection in the event of violations?

Despite the fierce struggle for control of the internet, manifested in attempts to dominate domain names and website addresses, the competition to control the web hosting market through technical servers, and sometimes endeavors to control information and methods of exchange through controlling and monopolizing technical solutions, which become a means of manipulating users' destinies and a tool for actual control, the internet remains characterized by decentralization and the absence of regulatory authority. Initiatives to create an internet government, internet police, standardized usage policies, or self-regulatory frameworks are merely virtual means, akin to the environment in which they arose.

Thus, international cooperation on certain issues becomes crucial, particularly agreement in the field of jurisdiction and the applicable law in internet dispute environments. Despite existing trends toward international cooperation and regulation, as well as notable efforts by the Organization for Economic Cooperation and Development (OECD), the European Union, and various technical entities and sectors operating in the internet environment, all these efforts have not yet provided solutions to the problems due to the lack of an acceptable regulation governing the internet in all its aspects. The nature of the internet and the directions of the development of the information superhighway suggest that the internet will remain outside the aspirations of governments to establish legal frameworks that govern it or control its affairs.[1]

Data travels across the internet from country to country, from organization to organization, from workplace to workplace, from individual to institution, without restrictions and in all languages. Information travels through local and international networks, moving from one point to another in cyberspace. In this journey, it lands and visits numerous jurisdictions and sovereign regions, sometimes in areas that may lack cooperation or even connections.[2]

In such an environment, there is a need for exceptional international efforts. The most crucial aspect is to move beyond traditional frameworks and concepts of control; the will of the powerful is no longer the cornerstone. An individual may, in such an environment, have the ability to challenge even the greatest powers. Therefore, what we call internet democracy, fairness in dealing with knowledge, non-discrimination, and the end of monopolistic control are the principles that must be considered in any activity aimed at organizing the necessary aspects of the internet. Most importantly, such regulation should take into account these technological characteristics and features of infinite interactivity.[3]

---

1 Dr. Osama Abdullah Qaid, *The Criminal Protection of Private Life and Information Banks*, Dar Al-Nahda Al-Arabiya, 1994, p. 23.
2 Roger Clarke, *Personalia Page*, 2008, p. 46.
3 Westin, A. F., *Privacy and Freedom*, New York, Atheneum, 1967, p. 43.

Second Axis: Privacy Threat Risks

1-Modern Technologies and Their Impact on Information Privacy: The risks of modern technologies to privacy protection are increasing, such as video surveillance technologies (cameras), electronic identification and identity cards, personal database systems, methods of intercepting and monitoring mail and communications, workplace surveillance, and others. Due to the high efficiency of technical means and the unlimited capabilities in the field of information analysis and retrieval, all countries of the world, through their various bodies and institutions, have moved towards creating databases to organize their work. The use of computers for collecting, storing, and processing personal data for multiple purposes, known as national information banks and centers, has expanded greatly. As societies have experienced the benefits of using computers in this field, a rapid awareness of the risks of information technology and its threat to privacy also emerged. This feeling grew and evolved due to real-life cases of unlawful use of personal data and the expansion of violations of individuals' right to private life. This situation prompted international, regional, and national efforts to develop principles and rules that, if observed, would protect the right to privacy. It also necessitated balancing society's needs for collecting, storing, and processing personal data with the protection of such data from the risks of unlawful use.

Although international efforts and the trend toward protecting private life, especially against the misuse of computers and information banks, represent the correct path to confront the negative effects of technology on private life,[4] this path has been accompanied by a pessimistic view regarding the use of technology in processing personal data.

The massive expansion in the use of computers raised concerns about the potential violations of private life. The source of these concerns lies in the fact that information about all aspects of an individual's personal life—such as health status, social and financial activities, behavior, political opinions, and more—can be collected, stored indefinitely, and retrieved easily and quickly. As the flow of information increases with computers, the individual's ability to control the flow of information about themselves weakens.

It is said that technocracy, or the ownership of computers, might become so powerful that it confines private life within narrow limits, adapting the life of the individual and their family according to the interests of those controlling the technology—whether for economic or social reasons. Thus, a human being could become like a number processed by a computer, stripped of will in making conscious decisions, exploited, and ultimately emptied of their personality. It is even argued that what threatens humanity is not a nuclear war but a computer device.[5]

The main features of the risks that computers and information banks pose to the right to private life can be summarized as follows:

First: Many major institutions and private or governmental companies collect detailed information about individuals' financial, health, educational, family status, social habits, work, etc., and use computers and communication networks to store, process, analyze, cross-reference, retrieve, and compare such data. This greatly increases the opportunities for unauthorized or deceitful access to this data, broadening the possibilities for misuse, wrongful manipulation, surveillance, exposure of private matters, or secret judgment based on personal data records. For example, according to 1999 studies, the United States government collected 4 million different records on Americans. According to my view, this touches on privacy and shows the failure to reconcile digital service provision with individuals' legal security.

---

[4] Miller, A., *The Assault on Privacy*, University of Michigan Press, 1971, p. 87.
[5] Burkert, H., *Institutions of Data Protection*, 1982, p. 65.

Second: The widespread "digital transfer" of data created a national security problem, as it facilitated eavesdropping and electronic espionage. In data transmission, privacy threats emerge from the communication networks' inability to provide full security for the data confidentiality transmitted through them, and the possibility of using networks to unlawfully obtain information remotely. Even technical security measures have not eliminated these risks. For example, in 1984, U.S. President Reagan directed NEA[6] to search for ways to produce more secure telephone networks for communications concerning sensitive government information. However, it was revealed that installing secure telephones is expensive.[7]

Third: A major danger of information banks is the presence of inaccurate or incomplete data that has not been updated or corrected properly. For example, in 1981, the Office of Technology Assessment in the United States assigned Dr. Lorden, a criminology expert, to conduct a study on the value of FBI criminal records.

Fourth: Personal information, which was previously isolated and difficult to access, becomes consolidated, readily available, and easily accessible in information banks. It can now be used more than ever before for individual surveillance purposes. Thus, Arthur Miller's statement appears accurate: the computer, with its insatiable appetite for information, its reputation for accuracy, and its memory that forgets nothing, could become the nerve center of a surveillance system that turns society into a transparent world where our homes, financial transactions, meetings, and mental and physical conditions are exposed to any passerby.

Fifth: The integration of computing with communications and multimedia has provided advanced monitoring tools (audio, visual, and readable), in addition to automatic tracking and information-gathering software. The Internet, as the link between these elements, offers the tremendous ability not only to collect information but also to process it using artificial intelligence technologies embedded in servers (computer hosting systems and service providers). Search engines and behavior analysis software also have these capabilities. Thus, it is no longer surprising that when a user connects to an information site nowadays, they immediately find websites related to what they had been thinking about visiting. Similarly, Internet users are not surprised when they receive marketing emails from entities they have never contacted, covering their interests and desires.[8]

2: Privacy Risks in the Internet Environment and E-commerce: The issue of privacy began to emerge with the widespread use of computers in the 1970s when it became clear that automated data processing could seriously threaten individuals' private lives, especially if done without their knowledge or explicit consent. What further complicates these challenges is that the Internet is an open, decentralized network—there is no single authority managing or controlling the flow of information across it. Moreover, its global nature adds another layer of complexity since the network is not subject to specific laws or courts. Countries that early recognized the seriousness of this matter, particularly in Europe, initiated legislation to protect personal life in the 1970s and have continuously updated it alongside technological advances. Among the requirements imposed by this legislation are "the obligation to specify the purpose of data collection in advance" and "the prohibition of data use without the owners' consent," in addition to granting individuals rights such as "the right to access and correct their information."
The Internet is the largest machine for collecting, processing, and transmitting personal data. The development of digital computers and network technology—especially the Internet—has allowed the

---

6 Nugter, A.C.M., *Transborder Flow of Personal Data within the EC*, Boston, 1990, p. 12.
7 Michael, J., *Privacy and Human Rights: An International and Comparative Study with Special Reference to Developments in Information Technology*, 1994, p. 34.
8 Jerry Berman & Deirdre Mulligan, *Privacy in the Digital Age (The Internet and Law): Work in Progress*, Nova Law Review, Volume 23, Number 2, 1999, p. 87.

transfer of social, commercial, political, cultural, and economic activities from the physical world to the virtual electronic environment. Day after day, global information networks are integrating with all aspects of life. Simultaneously, a broad movement has emerged to protect individual privacy.
Privacy breaches on the Internet can occur from three main sources:

- Internet service providers
- The websites visited by the user
- Network hackers... whether individuals or security and intelligence agencies.[9]

The service provider can monitor everything the user does on the Internet (the time and place of network access, the websites visited, search terms used, conversations, exchanged emails, etc.) through tools like Internet Protocol (IP) addresses, Packet analyzers, and Proxy servers. These programs can analyze every movement made on the network.
The information collected may include:

1. The Internet Protocol (IP) address identifying the user, domain name, and the company or entity that registered the domain, and their location.
2. Basic information about the user's browser, operating system, and system hardware.
3. The time and date of the site visit.
4. The Internet sites and page addresses visited before the current page visit.
5. Information about the search engine used to reach the page, and possibly the user's email address depending on the browser type.
6. Information about the time spent on each page and the data sent and received.[10]

Many—if not all—interactive sites, especially commercial and e-commerce sites on the Internet, require users to fill out forms containing various types of personal information when subscribing to services, registering, joining discussion groups, posting comments, or sending messages. These forms typically include the user's name, work and home address, phone and fax numbers, email address, age, gender, marital status, place of residence, monthly or annual income, and sometimes personal interests.

Sales and purchase sites, and those requiring payment transactions, also request credit card numbers, their types, and expiration dates. Despite the tremendous benefits brought by information technology and global networks, they have also created a real danger—allowing the collection, storage, access, and use of personal information online without the knowledge or consent of the information owner.

3- How Fraudsters Steal Passwords: There are many methods to steal passwords:

1. One of the simplest methods used by fraudsters is to call you, pretending to be computer security experts, and ask for your password.
2. Another common method is guessing passwords—often based on the initials of names or the birth dates of relatives.
3. The last method is "discovery," where the fraudster tries to figure it out...

Third Axis: Protection of Information Privacy [11]

Privacy is one of the basic rights of citizens, a right that has stirred wide controversy throughout history. It is perhaps the right that is being increasingly emphasized today in light of the impacts and consequences of the use of information technology. Privacy is a right recognized, in whole or in part, in the holy books, acknowledged by many ancient legislations, and raised in several court rulings since the

---

[9] Joan E. Rigdon, *Internet Users: They'd Rather Not Share Their Cookies*, Wall Street Journal, 1996, p. 65.
[10] United Nations Publications, *The Work of the United Nations in the Field of Human Rights*, Volume I, New York, 1990, p. 34.
[11] Dr. Saleh Jawad Kazem, *Modern Technology and Personal Confidentiality*, First Edition, Baghdad, 1991, p. 11.

nineteenth century. In modern times, this right was recognized by the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the European Convention on Human Rights, the American Convention on Human Rights, among others.

Historically, privacy has evolved through three main stages. The first stage: the recognition of privacy as a right to protect individuals from physical intrusions into their lives and properties, known as physical privacy. The second stage: privacy encompassing the protection of the moral values and elements of the person, known as moral privacy. The third stage: privacy as a general right extending to protect individuals from all forms of intrusion and interference in their lives, regardless of its form or nature. Within this last meaning, a new concept of privacy emerged linked to the impact of technology on private life, represented in information privacy or the right of individuals to control their personal information and data in the face of the challenges of the digital age.

It can be said that nearly all countries around the world have recognized, in one form or another, the right to privacy[12] in one or more of its aspects. However, this does not mean that sufficient or comprehensive protection exists in all countries. While physical privacy protection is more widespread, protection of information privacy remains limited, even though it currently represents a major concern for legislative bodies and decision-making institutions worldwide.

Thus, the right to privacy and data protection developed during the 1960s and 1970s, influenced by information technology and the potential surveillance power of computer systems, which necessitated the establishment of rules governing the collection and processing of personal data. In this field, it is important to note that the first legislative treatment for data protection occurred in 1970 in the Land of Hesse in Germany.

However, this treatment did not constitute a comprehensive law for several reasons, the foremost being that it was not a state law. It was followed by the enactment of the first national (comprehensive) law in Sweden in 1973, then in the United States in 1974, Germany at the federal level in 1977, and France in 1978. [13]

In 1981, the Council of Europe established a convention to protect individuals from the risks of automated processing of personal data. Likewise, the Organization for Economic Cooperation and Development (OECD) issued a guiding framework for the protection of privacy and trans-border flows of personal data, setting a group of rules governing the electronic processing of data. These rules treated personal data as collections that must be protected at every stage: collection, storage, processing, and publication.

In a further step at the regional legislative level, which had a global impact, the European Union issued the Directive on the Protection of Personal Data and the Free Movement of Such Data in 1995, representing a new phase in reorganizing information privacy. This prompted many European countries to draft new legislations or update existing ones, influencing many countries outside Europe to align with the standards set forth by the Directive.
In general, we can briefly say that the concept of data protection in the advanced charters requires that personal data must:

1. Be obtained lawfully and legally.
2. Be used for the original, declared, and specified purpose, and not disclosed to unauthorized parties.
3. Be relevant to the intended purpose and limited to it.
4. Be accurate and subjected to updating and correction processes. [14]

---

[12] Dr. Hisham Mohammed Farid Rustum, *Penal Law and the Risks of Information Technology*, Modern Machines Library, 1992, p. 20.
[13] Dr. Malcolm O. Norris, *Privacy and the Legal Aspects of the Information Superhighway*, 2008, p. 17.
[14] Ulrich Sieber, *Computer Related Crime*, 1994, p. 34.

5. Allow access rights along with notification of processing or transfer activities, and allow for correction, modification, or even deletion requests.
6. Maintain confidentiality and be protected according to appropriate security standards for data and processing systems.
7. Be destroyed once the purpose for which they were collected is exhausted.

Interest in protecting privacy from the risks of modern technologies began in the 1960s, launching the concept of protecting private data from technological risks.[15] Since the early 1970s, countries started adopting privacy protection laws either through comprehensive legislations that recognize the right and establish fundamental principles and provide the legal framework for protecting information privacy or personal data, or through sectoral laws relating to specific data sectors such as health data, financial data, civil registry data, among others. This was accompanied by codes of conduct regulating specific sectors like the industrial or technical services sectors, a method known as self-regulation of sectors or markets.

The majority of these laws, if not all, were based on the decisions of the Council of Europe of 1973 and 1974, the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1980, the OECD Guidelines of 1980, and the later United Nations Guidelines of 1990. In their evolution and comprehensiveness during the last five years, these laws clearly relied on the European Union's 1995 Directive on Data Protection.

These collections of rules formed what can be referred to as the international charter for data protection or the constitution of information privacy, a term we use at this stage of the development of information privacy due to its tangible impact on shaping the legal system for data protection and privacy in the digital age.[16]

Returning to the European Union's 1995 Directive on Data Protection, it represented a qualitative leap, affirming the concept of information privacy and establishing a balance between the right to privacy and the right to the free flow of information across borders. Facing the challenges of employing technology in administrative, productive, and service activities of the state, the EU issued in 1995 a comprehensive and binding guide – often called a law or directive – concerning the protection of information privacy and the organization of data transfers across borders. It was approved by both the European Parliament and the Council of Europe.

In 1997, another guide was issued to regulate the processing of personal data in the communications sector. This new effort – in addition to the continued efforts of the United Nations, the unified European institutions, and the OECD through the issuance of multiple guides addressing various types of data and their protection in the digital environment – relied on the previous legislative activity that produced the aforementioned codes.
The European Directive of 1995[17] mandated European countries to incorporate it into their national legislations by the end of October 1998 at the latest. This resulted in a new wave of legislation and the amendment of existing legal measures across the fifteen EU member states. It also influenced dozens of countries outside Europe, which found in this mature experience of personal data protection a model to adopt or adapt in developing their own data protection or comprehensive privacy legislations.

Because balancing the right to protect private data according to privacy principles related to data collection, processing, and disclosure, and the right to access information, requires the adoption of an acceptable balancing standard – since privacy, in essence, restricts the right to access information – both

[15] Munir Al-Janbihi, *Internet and Computer Crimes and Methods of Combating Them*, First Edition, 2008, p. 21.
[16] Ali, Nabil, *Arab Culture and the Information Age*, 2001, p. 12.
[17] Dr. Amr Ahmed Jasbo, *Protection of Freedoms in the Face of Information Systems*, Cairo, 2000, p. 56.

experiences had to be reviewed and evaluated by data protection authorities and information agencies in comparative legal systems.

Most countries moved toward adopting independent legislations in both fields. Some countries, like Hungary, organized the two rights in a single piece of legislation to ensure that the balancing standard between access to information and the protection of privacy is properly reflected in detailed provisions regulating the exercise of both rights.

Furthermore, the 1995 European Directive regulated both the protection of personal data and the right to transfer data across borders – the latter being part of the right to access information. Some countries, even with two separate laws, assigned oversight of both rights to a single authority. For example, the UK in 1998 renamed the body overseeing personal data protection from the Data Protection Registrar (under the 1984 Data Protection Act) to the Data Protection Commissioner following the 1998 Data Protection Act and the 1998 Human Rights Act.

With the issuance of the UK Freedom of Information Act of 2000, further amendments were made to the 1998 Data Protection Act, including renaming the Data Protection Commissioner and Data Protection Tribunal to the Information Commissioner and the Information Tribunal, respectively,[18] assigning them competences relating to both rights: the protection of personal data (privacy) and the freedom of information (right of access to information and records).

This direction aimed to establish a single authority responsible for multiple information-related tasks, whether ensuring the right of access or protecting personal data to maintain a proper balance when exercising both rights.

2. The Role of Information Technology in Protecting Information Privacy: The recent developments in information technology have caused continuous and accelerating changes in work methods and all fields. The transfer of information through local and international networks and computers has become routine in our current era and one of its defining features that cannot be dispensed with, due to its clear impact on facilitating the requirements of modern life by reducing workloads and developing methods for storing and providing information. The spread of computerized information systems has made them vulnerable to breaches, turning this technology into a double-edged sword that organizations are keen to acquire and protect.

The issue of information security is closely linked to computer security; there is no information security without computer security. In light of the rapid developments worldwide, which have affected the advanced technical capabilities aimed at breaching computer systems for theft, information sabotage, or the destruction of computers, it became necessary to seriously think about defining defensive and preventive procedures according to available capabilities to protect them from any breach or sabotage. It has also become the responsibility of organizations' management to ensure the creation of a secure information environment to guarantee its protection.

Data privacy (or information privacy) has become one of the increasingly important fields of research[19] in our current era — the era of information technology — especially in the management of institutional and governmental data, as well as private commercial, service, and health companies, which store hundreds of thousands or millions of customer or citizen records. These records include their personal data, interests, activities, and preferences, with the powerful ability to analyze, compare, and transfer this data across continents in mere seconds.

---

[18] Jamal Mohamed Ghaitas, *Information Security and National Security*, Dar Nahdet Misr, 2007, p. 71.

[19] Dr. Moussa Massoud Arjouha, *Terrorism and the Internet*, Research from the International Conference at Al-Hussein Bin Talal University, 2008, p. 14.

With the increasing number of hackers and identity thieves (Identity Theft), data privacy breaches have begun to affect our private lives and businesses in ways we could hardly have imagined. According to the Privacy Rights Clearinghouse (PRC), from January 2005 to September 2008, the number of records containing sensitive personal information that were breached in the United States alone exceeded 730,411,230 records, with the number increasing daily.[20]

Conclusion

Our journey through the complex paths of the octopus-like Internet network, and our exploration of the knowledge aspects it has produced, along with the nature of the legal violations that can occur through its global computerized space — a space that no longer pays attention to traditional concepts of time and place, and that has established new knowledge concepts and frameworks — draws our attention to the necessity of initiating a solid legal process to address the prevailing violations in cyberspace, in order to ensure legal security.

The idea here connects to one of the most important protection strategies: the user of the system — especially within an institution — should have a defined scope of use and privileges regarding the system. However, in practice, usage privileges are often increased without assessing the risks or even without the user knowing that they enjoy privileges exceeding their role and needs. In this case, any hacker who accesses the system will not only be able to destroy or manipulate the user's data via their access point, but could also destroy various system files, even those not connected to the user's entry point, by exploiting the additional privileges the user unknowingly possesses. This alone illustrates the importance of information security strategies and protection within an organization. Defining privileges and authorities can actually prevent widespread destruction and render breaches ineffective. Conscious strategies should not allow the existence of unknown user privileges, and ideally, such privileges should not exist at all.

Results

1) The necessity of developing flexible legal systems that align with digital life transformations, ensuring the stability of transactions and legal positions that guarantee legal security.
2) The allocation of a specific law for information systems and dedicated courts to handle related issues.
3) Considering legal stability as both a blessing and a curse: while maintaining legal positions through fewer legal amendments ensures legal security, it also cannot keep pace with the tremendous technological development. Therefore, specialists should be involved and a legal policy set to minimize deficiencies in maintaining legal security.
4) Despite the issuance of regulations and laws to face challenges and protect privacy imposed by digitization, at the same time, individual freedoms must not be suppressed, as they are tied to rights guaranteed by the Constitution.

Recommendations

1) There is a pressing need to legislate at the highest level to protect information privacy confidentiality through specific laws.
2) Internet users and citizens in general must receive educational courses on how to protect their information privacy.

[20] Forum of Technical and Technological Security, *Privacy Protection on Networks*, 2010, p. 15.

3) Seminars, courses, and conferences should be held on this topic to discuss its dimensions and its impact on the national society, the citizen, and even internationally.
4) A partnership between the public and private sectors must be established, considering the advanced level reached by the private sector in the field of digital technologies. Breaking their monopoly by imposing technology transfer is necessary to understand the limits of legal security and what can be protected amid the real challenges facing digitization, whether at the national or international level.

References

1. Dr. Osama Abdullah Qaid, *The Criminal Protection of Private Life and Information Banks*, Dar Al-Nahda Al-Arabiya, 1994.
2. Roger Clarke, *Personalia Page*, 2008.
3. Westin, A. F., *Privacy and Freedom*, New York, Atheneum, 1967.
4. Miller, A., *The Assault on Privacy*, University of Michigan Press, 1971.
5. Burkert, H., *Institutions of Data Protection*, 1982.
6. Nugter, A.C.M., *Transborder Flow of Personal Data within the EC*, Boston, 1990.
7. Michael, J., *Privacy and Human Rights: An International and Comparative Study with Special Reference to Developments in Information Technology*, 1994.
8. Jerry Berman & Deirdre Mulligan, *Privacy in the Digital Age (The Internet and Law): Work in Progress*, Nova Law Review, Volume 23, Number 2, 1999.
9. Joan E. Rigdon, *Internet Users: They'd Rather Not Share Their Cookies*, Wall Street Journal, 1996.
10. United Nations Publications, *The Work of the United Nations in the Field of Human Rights*, Volume I, New York, 1990.
11. Dr. Saleh Jawad Kazem, *Modern Technology and Personal Confidentiality*, First Edition, Baghdad, 1991.
12. Dr. Hisham Mohammed Farid Rustum, *Penal Law and the Risks of Information Technology*, Modern Machines Library, 1992.
13. Dr. Malcolm O. Norris, *Privacy and the Legal Aspects of the Information Superhighway*, 2008.
14. Ulrich Sieber, *Computer Related Crime*, 1994.
15. Munir Al-Janbihi, *Internet and Computer Crimes and Methods of Combating Them*, First Edition, 2008.
16. Ali, Nabil, *Arab Culture and the Information Age*, 2001.
17. Dr. Amr Ahmed Jasbo, *Protection of Freedoms in the Face of Information Systems*, Cairo, 2000.
18. Jamal Mohamed Ghaitas, *Information Security and National Security*, Dar Nahdet Misr, 2007.
19. Dr. Moussa Massoud Arjouha, *Terrorism and the Internet*, Research from the International Conference at Al-Hussein Bin Talal University, 2008.
20. Forum of Technical and Technological Security, *Privacy Protection on Networks*, 2010.