

## THE JUDICIAL POLICE SPECIFICITY IN OFFENCES AFFECTING DIGITAL DATA

Gahgah Oualid, Echahid Cheikh Larbi Tebessi University, Tebessa, Algeria,  
[oualid.gahgah@univ-tebessa.dz](mailto:oualid.gahgah@univ-tebessa.dz)

Send Article Date: 2025-08-06

Date of acceptance of the article 2025-10-10

---

### Abstract:

Public action, in Algeria, follows a series of stages, starting with the preliminary investigation and progressing to the final investigation. The search and inquiry phase, handled by the judicial police, is crucial for uncovering crimes and identifying those responsible. The importance of this phase has increased due to the rise of modern technology and digital landscape shifts.

Traditional judicial oversight often falls short in tackling digital data-related crimes. Algerian legislators have recognized the need for internet service providers to take a more proactive role in detecting specialized crimes.

**key words:** judicial police, investigation, specificity, digital data, providers, ...

### Introduction:

The judicial police authority is generally responsible for investigating a wide range of crimes. However, there are specific laws that sometimes assign this role to certain organizations or agencies, especially when they have specialized knowledge that makes them better suited to tackle particular types of crime. That said, it's still crucial for these entities to work closely with the traditional judicial police authority to ensure that crime detection and prevention efforts are as effective as possible.

The importance of this topic really stands out when you consider that the practical reality shows us how vital it is for information to be exchanged over the internet. This process relies heavily on the teamwork of those who manage it.

These key players, known as service providers, are essential to its functioning. The law includes specific rules designed to prevent crimes related to technology, media, and communication, and it requires these providers to help authorities gather and document data about communication content. This obligation exists because crimes involving digital data have their own unique characteristics.

The core problematic at hand can be summed up like this: **What part do service providers play in spotting and investigating crimes that impact digital data?**

To tackle this question, we relied on a mix of descriptive and analytical approaches, as they fit perfectly with our goals. We turned to the descriptive methodology to clarify the concepts tied to our study, while the analytical one came into play when we examined the legal texts that outline the specific rules aimed at preventing crimes related to information and communication technology.

### **THE FIRST TOPIC : THE NATURE OF DIGITAL DATA**

The world has stepped into a whole new era, one that has reshaped various ideas and events, and it's really changed how we take in and understand information. This period is often referred to as the Information Age or the Information Revolution. Thanks to the rise of the internet, computers have become even more crucial, creating a clear divide between the intangible aspects of software and the physical parts of hardware.

This is the moment when the software industry really started to take off, and these programs have turned into products all on their own, significantly influencing automated data processing systems. It's no surprise, considering this area has become a hotspot for breaches by various individuals and groups.

Because of this, we decided to kick off the first topic of this presentation by defining key concepts related to digital data, which we've split into two subsections. The first one is called "Definition of Digital Data", and the second is "Characteristics of Crimes Affecting Digital Data".

### **FIRST REQUIREMENT: DIGITAL DATA DEFINITION**

The rapid growth in information technology, combined with the need to handle tasks related to providing, collecting, processing, and sharing information, has unfortunately given rise to crimes that involve automated processing systems. This issue has come about as a result of blending information system technology with remote communication technology. Because of this, it's crucial to clarify some key concepts: data and information.

#### **Firstly: Definition of digital data**

Legal scholars and jurists have put in a lot of effort to nail down what we mean by digital data. Some define it as a mix of numbers, operations, words, symbols, or even raw documents and statistics that don't really connect with each other and haven't been modified or organized for practical use. On the other hand, information is all about the meaning we extract from that data.<sup>(1)</sup>

The French agency defined data as: "Any event or instruction that's understood and presented in a way everyone agrees on, which can be shared by people or through a computer."<sup>(2)</sup>

On top of that, the Budapest Convention on Cybercrime embraced the same definition put forth by the global certification body, which stated: "Data is any representation of facts, information, or concepts in any format, set up for processing, including through a program of the same kind that allows the computer to carry out the task."

Consequently, data is often seen as the building blocks from which we derive information through automated processing. This involves collecting and processing the data, and then repeating this cycle to gather even more insights.

When we look back at Algerian legislation, we notice that digital data hasn't been clearly defined. In Section 7 bis, there's a mention of "Interference with Automated Data Processing Systems." On the other hand, the term "informational data" is outlined in the law that sets specific rules to prevent crimes related to information and communication technology. It describes informational data as "any presentation of facts or concepts formatted for processing within an information system, including the necessary software that allows the system to function properly".<sup>(3)</sup>

### **Secondly: Definition of data**

Idiomatically, data can be thought of as a collection of letters, numbers, and symbols that represent facts and ideas, all aimed at helping us gather information. It acts as the essential building block for researchers, allowing them to develop a solid understanding of their research topic, drawing on their initial insights gained through experience, observation, and practice.

Data provides insights into the phenomenon being studied without needing to explain it, whether it's been examined before or not. It also gathers information from customers and suppliers across various organizations connected to the one being analyzed, along with feedback from consumers, market trends, sales reps, publications, newspapers, and more.

When we talk about digital data, we're referring to the information that helps identify individuals and state institutions. This can either be clearly outlined by digital regulations or found within the data set itself, or even processed in ways that reveal someone's identity. This kind of data is typically divided into two categories: internal data and external data.

Internal data is all about the information that lives within an organization. It's where internal processes get recorded and analyzed, often showing up in a repetitive and periodic manner.

On the flip side, external data is the information that comes from outside the organization. This includes details related to clients and describes the products and services that the organization offers.

Upon revisiting Algerian legislation, it becomes clear that the Algerian legislator has outlined the definition of data in Law N<sup>o</sup>.09-04. This law includes specific guidelines concerning crimes related to information and communication technology, and here's how it breaks down:

(It's an all process of presenting facts, information, concepts, instructions, observations, or measurements. This can come in various forms like numbers, letters, symbols, images, or other formats. Data providers collect, produce, and process this information, which is included wherever it appears in this law).

Article 03 of law that focuses on protecting individuals in the realm of personal data processing describes personal data as “any information—regardless of how it's stored—that relates to a person who can be identified, either directly or indirectly. This includes references to things like identification numbers or specific traits tied to their physical, physiological, genetic, biometric, psychological, economic, cultural, or social identity”.<sup>(4)</sup>

The Tunisian legislator describes it as “any data, no matter where it comes from or what form it takes, that can identify a natural person or make them identifiable, either directly or indirectly. This definition excludes information related to public life or anything deemed public by law”.

The term covers all information that relates directly to a person or is processed or analyzed in any format, whether that's on paper, electronically, or in other ways, but it doesn't include information about public life. The individual being referred to is “any natural person whose personal data is being processed”.

Finally, It's worth mentioning that digital data comes with a unique set of characteristics that set it apart from other types, and these can be summarized as follows:

### **1: Credibility of Digital Data**

Where data is regarded as one of the key features of sectors, representing a collection of relative attributes and characteristics that define a product or service. It meets the needs and expectations of the customer while considering the comfort and safety of the community and the ability to satisfy customer demands and needs.

### **2: The Legitimacy of Digital Data Trading**

Digital data is seen as a crucial element across many industries, especially since a lot of crimes are linked to the trading of data online. This reality makes it all too easy for data to be compromised and shared among people.

Right now, the quickest way to trade data on the internet poses a serious risk to its integrity, as it can result in unauthorized destruction, deletion, modification, or erasure of data, along with illegal access for carrying out criminal activities.

### **3: Digital Data Confidentiality**

Data is deemed confidential when it's stored on computer systems, requiring robust protection and a solid firewall setup. It's crucial to implement all necessary legal measures to keep unauthorized individuals at bay. Take, for example, government data tied to national security—this information is incredibly sensitive and must be shielded from any potential breaches or violations.

### **4: Diversity of Data Sources**

Data is truly the lifeblood of any business. When it comes to analyzing and interpreting this data, it all starts with collecting various types from their primary sources, which are essentially the real and original data. The main goal of gathering primary data is to find solutions to specific research problems.

On the other hand, secondary data is collected from earlier time periods and published for a variety of reasons, which might not always align with the goals of the studies that organizations or companies are conducting at any given time.<sup>(5)</sup>

## **THE SECOND REQUIREMENT: CHARACTERISTICS OF DIGITAL DATA-RELATED CRIMES**

The internet is a huge web that links up countless networks from different countries, enabling millions of computers to access the same websites at the same time. This gives us quick access to a treasure trove of information and services.

However, this digital landscape has also become a hotspot for various crimes that can impact individuals. Crimes related to digital data come with a few distinct characteristics, which include the following:

### **Firstly: Transnational Crimes**

This kind of crime shows a blatant disregard for national borders, as the criminal might live in one country while their victim is in another. Because of this, these crimes frequently span multiple international lines and borders.

The rise of information technology has changed the way we connect and communicate across the globe, and it has also transformed criminal behavior. Nowadays, criminals are leveraging these technologies to break the law, which means that a crime involving digital data isn't just happening in one place—it's now a global issue.

The offender doesn't need to be physically at the crime scene; they can commit their acts from afar. This creates a clear divide between the actions taken through computer devices and the information that becomes the target of their crimes.

## **Secondly: Computer data-related crimes**

### **1: Computer as a tool for committing crime**

Digital data crimes have a distinct feature that sets them apart from traditional offenses, primarily because computers are the main tools used in these illegal activities. Moreover, these crimes often involve attacks on other computers, which can include unauthorized access to software, stealing information, tampering with data, or even destroying and viewing data without permission.

The act of attacking a computer or its peripherals and connected devices, the goal is often to compromise the data stored within. This includes all the information and files that the computer holds. Unlike physical objects, this data is more like abstract concepts or ideas that are processed and stored by the computer.

### **Thirdly: Soft Crimes**

Cybercrimes are quite different from the traditional crimes we often think of, like murder or theft, which can involve violence. Instead, cybercrimes are typically non-violent, which is why they're often labeled as soft crimes. These offenses require a unique set of skills, including intelligence, access to the right tools, and a knack for navigating the internet.

Actions like transferring data between computers, messing with automated data systems, or gaining unauthorized access to computers are all examples of these stealthy crimes. Cybercriminals usually have a strong grasp of computer programs, making it even tougher for law enforcement to pursuit and track them down.<sup>(6)</sup>

### **Fourthly: The perpetrator of the crime is skillful and an expertise**

To engage in cybercrime involving digital data, a user needs to have a solid grasp of how computers work. This means they should be aware of the context of the crime, how to carry it out, and evaluate the chances of it succeeding or failing. Moreover, a savvy cybercriminal will have a deep understanding of their illegal activities. As mentioned earlier, they also possess a high level of skill in computer and internet technologies.

### **Fifthly : Crimes difficult to detect and proven**

Digital data crimes are tricky because they don't leave behind any physical evidence, which makes them hard to spot and prove. The distance between the criminal and the victim adds to the complexity, especially since offenders often use advanced technology to carry out their illegal activities. Plus, these crimes can happen in the blink of an eye and can be wiped away just as quickly, sometimes in mere seconds. The challenges in uncovering and proving these crimes stem from several key factors:

### **1: Secrecy of the crime**

Digital data crimes are often described as "invisible," setting them apart from traditional crimes. The victims might not even realize they're happening while they're online. This is largely due to the technical prowess of the criminals, who can execute their schemes with precision—whether it's unleashing harmful viruses or siphoning off money, among other malicious activities.<sup>(7)</sup>

### **2: Speed of erasing traces and evidence**

Cybercrimes that target digital data operate in a world that's quite different from our physical reality. They unfold in an electronic space where information is shared and moved around without us even seeing it. Plus, tracking down any evidence of these crimes can be really tough, if there's any to find at all.<sup>(8)</sup>

### **Sixthly: crimes typically committed with the collaboration of multiple individuals**

Digital data crimes often involve a team effort, where multiple individuals play different roles. Typically, there's someone with a knack for technology who handles the technical side of the crime, while another person—either from the local area or outside the organization—helps to cover up the wrongdoing and funnel the profits elsewhere.

## **THE SECOND TOPIC: THE ROLE OF SERVICE PROVIDERS IN OF RESEARCH AND INVESTIGATION**

The challenges posed by crimes involving digital data are significant within Algerian law, creating legal obstacles for authorities at every level, especially during the investigation and inquiry stages of these offenses.

The role of the judicial police is vital and shouldn't be underestimated, as they are key to launching an investigation once there's enough evidence to prove the crime commission.

Despite all these advancements, the judicial police hasn't has not been immune to the negative effects of technology and the new types of crime it has brought about. This has posed a real challenge for criminal justice agencies overall, as law enforcement officers often find themselves struggling to investigate crimes involving digital data. These cases are quite different from traditional crimes, making them particularly tricky to handle.

The European Council Recommendation N°.95, issued on November 9, 1995, confirmed the need to address issues surrounding criminal procedure and information technology. It emphasized the importance of creating specialized units dedicated to tackling computer crimes.

The Algerian legislator put this into action with Law No.09-04, which lays out specific guidelines aimed at preventing crimes tied to information and communication technology.

This law involves internet service providers, as well as both fixed and mobile telecommunications, in the fight against technological crimes. In this section, we'll break it down into two main parts. The first part is called "The Concept of Service Providers", and the second part is "Obligations of Service Providers".

### **THE FIRST REQUIREMENT: THE CONCEPT OF SERVICES' PROVIDERS**

In today's world, the security of our information and digital spaces is a big worry for everyone, from individuals to organizations, whether they're public or private. It's crucial to set up technical safeguards and take steps to tackle illegal or harmful content that can spread through information and communication technology.

To offer various services related to this tech, we need the cooperation of different players, especially service providers. This is all laid out in the law, which includes specific rules aimed at preventing crimes linked to information and communication technology.

The text describes service providers as any public or private organization that allows users to connect via an information system or communication network, along with any other entity that handles or stores data to support these communication services for users.

It's interesting to note that the Algerian legislator has identified three types of intermediaries that play a crucial role in delivering information technology services in various forms to users: delivery service providers, hosting providers, and content providers.

#### **Firstly: Delivery contractors**

Delivery contractors play a crucial role by sharing and managing information across networks. They offer devices and technical services that help users stay connected to the network.

#### **Secondly: hosting providers**

The Algerian legislator describes them as any entity that handles or stores data for the benefit of the specified communication service or its users. As a result, no individual, whether a natural person or a legal entity, is allowed to create a private site without going through a hosting provider.

### **Thirdly: Content providers**

The content provider or publisher is essentially the person who takes the time to edit a message and then shares it online, which is just a fancy way of saying they publish it digitally. They make use of various communication tools, especially the internet, to get the word out to the public.

### **THE SECOND REQUIREMENT: OBLIGATIONS OF SERVICES' PROVIDERS**

The Algerian legislator, much like their French counterpart, has laid down a series of obligations for service providers. However, it seems they've missed the mark when it comes to recognizing the crucial role that these providers play in investigating and probing crimes that impact digital data. Section One: The duty to preserve data and support judicial authorities.

#### **Firstly: Commitment to assisting law enforcement authorities**

This means that media and communication service providers, like internet service providers, need to make their stored data accessible to judicial authorities. As a result, these service providers must share the information they have stored in their computer systems with the judicial authorities, but there are specific limits to what they can disclose.<sup>(9)</sup>

These boundaries are all about figuring out who uses their services and understanding the content of their communications, which is crucial for getting to the bottom of things. This can only happen if service providers, like access and hosting providers, are diligent in protecting their users' data. Plus, it's really important to keep investigative secrets confidential, as law requires.

It's worth mentioning that the Algerian legislator has made a specific exception regarding the type of information that must be shared with judicial authorities. This exception relates to certain details tied to professional secrecy, as specified in Article 65 bis 5 of the Code of Criminal Procedure.

This article states that: (If the necessities of investigation into the crime...) which includes crimes impacting automated data processing systems. In this context, and following the guidelines of Article 65 bis 5, the authorized public prosecutor has the power to permit the following:

- Interception of correspondence carried out through both wired and wireless methods.
- Setting up technical arrangements without the consent of those involved, aimed at capturing, storing, broadcasting, and recording private or confidential conversations by one or more individuals in either private or public spaces, or taking photos of individuals in a private setting.
- Conducting authorized operations based on this premise under the direct oversight of the appropriate public prosecutor.

**Secondly: Commitment to save Traffic-related data**

The Algerian legislator has outlined what traffic data means in Article 2, paragraph (e). It specifies that this data includes any information linked to communication via an information system, which is generated as part of a communication process. This data sheds light on various aspects, such as where the communication originated, its intended destination, the path it took, the time and date it occurred, the amount of data exchanged, how long the communication lasted, and the type of service used.

The requirement set forth in Article 11 of Law N°.09-04 pertains to potential notifications to judicial authorities or situations where these authorities request investigations or inspections.

The law specifies that service providers aren't obligated to keep identifiable records of their users, nor are they allowed to store information about the content of communications, text messages, or email subjects. Additionally, the maximum retention period for this data is capped at one year from the date of registration.

The information that needs to be kept safe mainly includes the following:

- Details data that help identify the service user.
- Data about the device used for communication.
- Technical specs, along with the date, time, and length of each communication. Information about any additional services requested or used, along with their providers.
- Data that helps identify the sender or recipients of the communication, including the addresses of the sites visited.

**Thirdly: Commitment to filtering sites and specifying their type**

The text of Law No.09-04 lays out the following requirements: (In addition to the commitments mentioned in Article 11 above, internet service providers are required to:<sup>(10)</sup>

**A-** Act swiftly to remove any content they provide access to as soon as they become aware, either directly or indirectly, of any violations of these laws. They must either store this content or ensure that access to it is blocked.

**B-** Set up technical measures that limit access to servers hosting information that goes against public order and morals, and they must inform their subscribers about its existence.).

Regarding the immediate intervention to withdraw content that they allow access to upon direct or indirect knowledge of its violation of laws, service providers are not facing criminal charges if they don't comply. This indicates that the liability is more of a moral obligation.

THE JUDICIAL POLICE SPECIFICITY IN OFFENCES AFFECTING DIGITAL DATA

---

So, if service providers neglect their duty to take down illegal or harmful content, they can't be held legally responsible for any damages that arise from that content being displayed.

The French lawmakers have set up both civil and criminal penalties for hosting service providers who either refuse or neglect to take down content that breaks law or make it inaccessible.

Regarding the statement about the types of websites that host content against public order and morals, law requires service providers to set up technical measures. These measures should help internet users easily recognize the nature of these sites. It's important that this information is presented clearly, so that anyone looking to visit certain sites—those known to breach public order and morals—can be fully aware of what they're getting into before they click through.

**Conclusion:**

The internet is like a huge web that connects countless e-activities and information services happening every single day. That's why internet service providers are so crucial—they help keep the internet running smoothly and manage all the content and information we rely on.

Given that crimes involving digital data have their own distinct technical and creative aspects, it's so important to bring internet service providers into the mix when investigating and researching these types of crimes. Traditional judicial police has a limited role here, and since the digital world is a hotbed for this kind of activity, having experts from the digital field involved in the investigation is absolutely essential.

**Results:**

- ✓ When it comes to investigating and searching for crimes that involve digital data, there's a key difference in the principles at play. The unique nature of digital information means we need to set up different rules and procedures, whether we're dealing with individuals or organizations.
- ✓ Law obliges internet service providers to act quickly—removing any content they can access as soon as they become aware of it, whether that awareness is direct or indirect.
- ✓ Furthermore, these providers must clearly outline which types of websites host information that goes against public order and morals.

**Recommendations:**

- ✓ Experts and investigators need to be well-trained to tackle crimes that involve data with unique technical features, especially during the research and investigation stages.

- ✓ Moreover, it's crucial to give the telecommunications regulatory authority a bigger role in ensuring that internet service providers are following the rules.

**References:**

**Legal Texts:**

(1)- Law N°.09-04 of August 5, 2009, containing special rules for the prevention and combating of crimes related to information and communication technology, Official Gazette, N°.47.

(2)- Law N°.25-11 of Muharram 28, 1447 corresponding to July 24, 2025, amending and supplementing Law N°.18-07 of Ramadan 25, 1439 corresponding to June 10, 2018, concerning the protection of natural persons in the processing of personal data.

**Books:**

(1)- Khaled Mamdouh Ibrahim, *Cybercrime Security*, University House, Alexandria, 2008.

(2)- Meftah Mohammed Dabbab, *Dictionary of Terms and Information and Communication Technology*, International Publishing House, Egypt, 1995, p. 42.

(3)- Nahla Abdelkader Al-Moumni, *Cybercrimes*, Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, first edition, 2008.

**Theses:**

(1)- Afef Khediri, *Criminal Protection of Digital Data*, PhD Thesis, Larbi Tebessi University, Tebessa, 2017/2018.

**Articles:**

(1)- Aicha Safrani, *Data Review and Analysis*, Journal of Social Empowerment, University of Laghouat, Volume 6, Issue 2, 2014.

(2)- Mohammed Baadji, *Obligations of Online Service Providers*, journal of teacher researcher of legal and political studies, Msila university, Volume 4, Issue 1, 2019.

---

**Endnotes:**

(1)- Afef Khediri, *Criminal Protection of Digital Data*, PhD Thesis, Larbi Tebessi University, Tebessa, 2017-2018, p.13.

(2)- Meftah Mohammed Dabbab, *Dictionary of Terms and Information and Communication Technology*, International Publishing House, Egypt, 1995, p.42.

(3)- Article 2, Paragraph C of Law N°.09-04 of August 5, 2009, containing special rules for the prevention and combating of crimes related to information and communication technology, Official Gazette, N°.47.

(4)- Article 3 of Law N°.25-11 of Muharram 28, 1447 corresponding to July 24, 2025, amending and supplementing Law N°.18-07 of Ramadan 25, 1439 corresponding to June 10, 2018, relating to the protection of natural persons in the field of processing personal data.

(5)- Aicha Safrani, *Data Review and Analysis*, *Journal of Social Empowerment*, University of Laghouat, Volume 6, Issue 2, June 2014, p.172.

(6)- Nahla Abdelkader Al-Moumni, *Cybercrimes*, Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, First Edition, 2008, p.58.

---

(7)- Afef Khediri, Op.cit., p.21.

(8)- Khaled Mamdouh Ibrahim, *Cybercrime Security*, University House, Alexandria, 2008, p.45.

(9)- Mohammed Baadji, Obligations of Online Service Providers, *journal of teacher researcher of legal and political studies*, Msila university, Volume 4, Issue 1, 2019, p.32.

(10)- Article 11 Law 09-04, aforementioned.