



MINISTRY OF HIGHER EDUCATION AND
SCIENTIFIC RESEARCH
UNIVERSITY OF ORAN 1 – AHMED BEN BELLA
INSTITUTE OF CRIMINOLOGY



Subject

**DIGITAL EVIDENCE IN PERSONAL
DATA CRIMES**

Dissertation submitted in partial fulfilment of the requirements for the degree of an
Academic Master's

Field: Law and Political Science

Field: Law

Specialisation: Criminal law and criminal science

Submitted:

- DJAMEL ABD NASSER YKHLEF
- MOHAMED ZAKI DJEZZAR

Supervised by:

- MOUHAMED EL AMINE ADDA BOUHADDA

Presented and defended before the following examining committee:

Academic Status	Full Name	University
Chairperson of the Jury	Meki ahmed	University of oran 1 ahmed ben bella
Academic Supervisor	Adda bouhadda Mohamed amine	University of oran 1 ahmed ben bella
Examiner	Boukeriris siham	University of oran 1 ahmed ben bella

Academic Year: 2025/2026

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

﴿ يَا أَيُّهَا الَّذِينَ آمَنُوا إِذَا قِيلَ لَكُمْ تَفَسَّحُوا فِي الْمَجَالِسِ فَافْسَحُوا يَفْسَحِ
اللَّهُ لَكُمْ وَإِذَا قِيلَ انشُزُوا فَانْشُزُوا يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنْكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ
دَرَجَاتٍ وَاللَّهُ بِمَا تَعْمَلُونَ خَبِيرٌ ﴾

[سورة المجادلة الاية 11]

Dedication

To those who were the light of my path, the secret of my success, and the source of my strength...

To those who instilled in me the love of knowledge and hard work,

To my dear parents, may God grant them long life and keep them as a crown upon my head.

To my beloved family, who have always been my support throughout all stages of my life,

And to everyone who offered me sincere words of encouragement in moments of difficulty.

To my respected teachers, who illuminated my path with knowledge and guidance,

And who played a significant role in directing and mentoring me.

To my friends and everyone who shared this journey with me,

And to all those who contributed, directly or indirectly, to the completion of this work.

I dedicate this humble effort as a token of love, loyalty, and appreciation.

Djamel abd nasser ykhlef

Dedication

To those who were the light of my path, the secret of my success, and the source of my strength...

To those who instilled in me the love of knowledge and hard work,

To my dear parents, may God grant them long life and keep them as a crown upon my head.

To my beloved family, who have always been my support throughout all stages of my life,

And to everyone who offered me sincere words of encouragement in moments of difficulty.

To my respected teachers, who illuminated my path with knowledge and guidance,

And who played a significant role in directing and mentoring me.

To my friends and everyone who shared this journey with me,

And to all those who contributed, directly or indirectly, to the completion of this work.

I dedicate this humble effort as a token of love, loyalty, and appreciation.

Mohamed zaki djezzar

Acknowledgments

All praise is due to Allah, the All-Hearing, the All-Knowing, the
Possessor of greatness and immense

Peace and blessings be upon the noble Prophet, and upon his family and
companions.

In accordance with the Almighty's saying: "If you are grateful, I will
surely increase you," we express our gratitude to Allah, the Most High,
who guided us on the path of knowledge and granted us the strength to
complete this work.

We would also like to extend our sincere thanks and appreciation to our
supervisor, Dr. MOHAMED EL AMINE ADDA BOUHADDA, who
spared no effort in providing guidance and advice throughout the course
of this study, through his valuable instructions and continuous support
at every stage of the research.

We also express our gratitude to our esteemed teachers for their guidance
and valuable advice.

Finally, we would like to thank the members of the examination
committee for kindly accepting to review and evaluate this work.

Abstract

Rapid developments in the digital environment have led to the emergence of new forms of crime, particularly those related to personal data, making digital evidence an essential tool for their detection.

Digital evidence relies on electronic data to establish criminal facts and is characterized by its intangible nature and vulnerability to alteration or manipulation.

Such evidence requires a precise legal and procedural framework to ensure its legality and integrity during collection and use.

Algerian legislation provides a set of rules governing digital evidence, particularly through laws related to personal data protection and criminal procedures.

Personal data includes any information that allows the identification of an individual, directly or indirectly, requiring effective legal protection.

Personal data crimes include illegal access, espionage, unlawful modification, and unauthorized disclosure.

The proof of these crimes depends mainly on digital traces such as system logs, electronic records, and usage data.

The collection of digital evidence is subject to strict legal controls, especially the principle of legality and respect for procedural rules.

The nature of digital evidence requires maintaining its integrity through proper documentation and protection against tampering.

Technical expertise plays a central role in analyzing and interpreting digital evidence before the courts.

Judges exercise discretionary power in evaluating digital evidence based on the principle of free evaluation of proof.

Digital evidence raises practical challenges, particularly due to technical complexity and difficulties in attributing responsibility.

Its effectiveness depends on compliance with both legal and technical requirements.

Continuous technological evolution requires updating legislation and strengthening professional training in digital fields.

Digital evidence remains a crucial means of achieving justice while ensuring the protection of fundamental rights and freedoms

Keywords :

Digital Evidence ,Personal Data, Cybercrime, Criminal Procedure, Data Protection, Technical Expertise, Fair Trial

الملخص

شهدت البيئة الرقمية تطورًا متسارعًا أدى إلى ظهور أنماط جديدة من الجرائم، خاصة تلك المرتبطة بالمعطيات الشخصية، مما جعل الإثبات الرقمي عنصرًا أساسيًا في الكشف عنها.

يُعد الإثبات الرقمي من الوسائل الحديثة التي تعتمد على البيانات الإلكترونية في إثبات الجرائم، ويتميز بخصائص خاصة أهمها طبيعته غير المادية وقابليته للتغيير أو التلاعب.

يفرض هذا النوع من الأدلة إطارًا قانونيًا وإجرائيًا دقيقًا يضمن مشروعيتها وسلامته عند جمعه واستعماله.

يكرّس التشريع الجزائري مجموعة من القواعد المنظمة للإثبات الرقمي، خاصة من خلال النصوص المتعلقة بحماية المعطيات الشخصية والإجراءات الجزائية.

تشمل المعطيات الشخصية كل المعلومات التي تسمح بتحديد هوية الشخص، سواء بشكل مباشر أو غير مباشر، مما يستوجب توفير حماية قانونية فعالة لها.

تتعدد جرائم المعطيات الشخصية، من بينها الدخول غير المشروع، التجسس، التعديل غير القانوني، والإفشاء دون ترخيص.

يعتمد إثبات هذه الجرائم أساسًا على الأدلة الرقمية مثل سجلات الأنظمة، البيانات الإلكترونية، وآثار الاستخدام.

يخضع جمع الأدلة الرقمية لمجموعة من الضوابط القانونية، وعلى رأسها مبدأ الشرعية واحترام الإجراءات القانونية.

كما تفرض طبيعة هذه الأدلة ضرورة الحفاظ على سلامتها من خلال توثيق مراحل التعامل معها وضمان عدم التلاعب بها.

تطلب الخبرة التقنية دورًا محوريًا في تحليل الأدلة الرقمية وتفسيرها أمام القضاء.

يتمتع القاضي بسلطة تقديرية في تقييم الأدلة الرقمية وفق مبدأ حرية الإثبات، مع مراعاة مشروعيتها ومصادقيتها.

تطرح الأدلة الرقمية عدة تحديات عملية، خاصة فيما يتعلق بالتعقيد التقني وصعوبة تحديد هوية الفاعل.

ترتبط فعالية الإثبات الرقمي بمدى احترام الضوابط القانونية والتقنية المعتمدة في جمعه وتحليله. يستدعي التطور التكنولوجي المستمر

تحديث التشريعات وتعزيز التكوين في المجال الرقمي.

يظل الإثبات الرقمي وسيلة أساسية لتحقيق العدالة مع ضرورة ضمان حماية الحقوق والحريات

الأساسية.

الكلمات المفتاحية :

الدليل الرقمي, المعطيات الشخصية, الجرائم المعلوماتية, الإجراءات الجزائية, حماية البيانات, الخبرة التقنية, المحاكمة العادلة

list of abbreviations :

p : page

ed : edition

rd : third

No : number

Op cit: the
work cited.

Ibid: the same
reference.

Introduction

Introduction

Today, digital technology is a part of daily life in Algeria. People use phones, computers, and the internet to communicate, work, and manage personal matters. Many services, both public and private, now depend on digital systems. Because of this personal data such as names, identification details, phone numbers, and online information are constantly stored and shared in electronic form.

This situation has also created new risks. Personal data has become an easy target for misuse and illegal acts.

In recent years, Algeria has seen new types of crimes linked to digital technology. These include illegal access to systems, data theft, unauthorized modification, and disclosure of personal information. Such crimes are often committed from a distance and without direct contact with the victim, which makes them difficult to detect.

To deal with these challenges, the Algerian legislator has introduced specific legal rules. **Law No. 25-11** aims to protect personal data and regulate how it is processed and used. At the same time, **Law No. 25-14 on criminal procedures** sets the rules for investigation, evidence collection, and prosecution, including cases that involve digital tools and electronic data.

In this context, digital evidence has become very important. It includes electronic data, messages, files, and records stored on digital devices or networks. Through this evidence, investigators and judges can better understand how a crime was committed and who is responsible. However, digital evidence is not easy to handle. It is invisible, technical, and can be changed or lost if it is not collected in a correct legal way.

Importance of the Topic:

The importance of digital evidence in personal data crimes is clear for several reasons.

First, personal data is directly linked to the private life. Any misuse of such data may seriously harm individuals. Therefore, criminal procedures involving digital evidence must ensure strong legal protection.

Second, Algerian law has recently developed in this area through:

- Law No. 25-11 on the protection of personal data
- Criminal Procedures Law No. 25-14

These legal texts show that the Algerian legislator recognizes the importance of regulating digital evidence. However, practical and doctrinal difficulties remain.

Third, judges and lawyers face challenges in evaluating digital evidence, especially regarding authenticity, legality, and attribution of criminal responsibility.

For these reasons, studying digital evidence in personal data crimes is both legally necessary and practically important.

Research Methodology:

This research adopts several legal methods:

- **Analytical method:** to analyze legal texts and judicial principles
- **Descriptive method:** to explain procedural mechanisms
- **Comparative method:** to refer to international standards such as the Budapest Convention and the GDPR

Reasons for Choosing the Topic:

The choice of this topic is based on a set of subjective and objective factors, as follows:

First: Subjective Motivations

Personal interest in the subject of digital evidence, as it is a modern field that combines law and technology.

The desire to deepen knowledge in the field of law, particularly with regard to modern methods of proof.

Second: Objective Motivations

The increasing reliance on digital evidence in criminal investigations.

The legislator's effort to keep pace with technological developments.

Research Difficulties:

During the preparation of this research, several difficulties were encountered, the most important of which are:

-The novelty of the topic, as digital evidence is considered a relatively recent subject in the field of law, which has led to a lack of specialized references.

-The technical complexity of the subject, due to the close connection between digital evidence and technological aspects, which required acquiring a basic understanding of certain technical concepts in order to comprehend how digital evidence is collected and analyzed.

Scope of the Study:

This study falls within the scope of Algerian law and primarily focuses on analyzing the legal framework of digital evidence in personal data crimes under Algerian legislation. Accordingly, the study is limited, **in terms of subject matter**, to:

- Examining the concept of digital evidence and its characteristics.
- Studying its applications in personal data crimes.
- In terms of the **geographical scope**, the study focuses on Algerian law, while making reference to certain international models and standards.
- As for **the temporal scope**, the study focuses on recent legal texts, particularly Law No. 25-11 relating to the protection of personal data and Criminal Procedure Law No. 25-14, with the aim of highlighting the extent to which the Algerian legislator keeps pace with modern technological developments in the field of digital evidence.

research question:

This reality raises important legal questions. How can digital evidence be used effectively without harming personal privacy? How can the law protect individual rights while fighting personal data crimes? **This leads to the main How does Algerian law, especially Law No. 25-11 and Law No. 25-14, regulate digital evidence in personal data crimes while respecting individual rights and ensuring a fair trial?**

Plan Statement:

This study is structured into two main chapters. The first chapter examines the nature and characteristics of digital evidence through two sections. The first section is

devoted to the study of the concept and characteristics of digital evidence, as well as its application in personal data crimes, while the second section addresses the principle of legality and the admissibility of procedures, in addition to the role of the National Authority for the Protection of Personal Data and international standards.

The second chapter focuses on the procedural framework of digital evidence under Criminal Procedure Law No. 25-14, also through two sections. The first section deals with judicial powers and evidence collection procedures, as well as the role of technical expertise, whereas the second section examines the evidentiary value of digital evidence in trial proceedings, along with procedural challenges and proposed legislative reforms.

Chapter one:

**Conceptual and Legal Framework of
Digital Evidence in Personal Data
Crimes.**

Chapter one: Conceptual and Legal Framework of Digital Evidence in Personal Data Crimes.

This chapter introduces the basic ideas related to digital evidence in personal data crimes under Algerian law. It explains what digital evidence is, how it is different from traditional evidence, and how it can be used in cases involving n personal data. It also discusses the main legal rules that organize the collection and use of this type of evidence, as well as the role of national authorities and international standards.

Through this chapter, the research aims to build a clear and simple foundation, helping the reader understand why digital evidence is essential today and how Algerian law deals with it before moving to the procedural aspects in the next chapter.¹

Section one: Nature and Characteristics of Digital Evidence.

Before going deeper into legal rules, it is important to stop for a moment and understand what digital evidence really means. In simple terms, digital evidence is not something we can see or touch easily. It exists inside computers, phones, and electronic systems, and it appears in the form of data, files, or digital records.

In personal data crimes, this kind of evidence is especially important. When personal information is misused, the effects of the crime are usually hidden inside digital systems. What happened can only be discovered by looking at electronic traces left behind during the use of these systems. This makes digital evidence a key element in understanding such crimes.

⁻¹ **Abderahmane khalfi**, algerian criminal procedures, 8 ed, Dar belkis, Algiers, 2025, p. 300.

This section focuses on explaining digital evidence in a clear and simple way. It looks at its meaning, its main characteristics, and how it appears in personal data crimes, while referring to the legal protection provided under Algerian law. This helps the reader build a basic understanding before moving to more detailed legal analysis.

Subsection one: Concept and Characteristics of Digital Evidence.

Before analyzing procedural rules, it is necessary to define digital evidence and identify its main features. Unlike traditional evidence, digital evidence exists in an electronic environment and requires technical tools for its discovery and interpretation.

Legal doctrine has developed different definitions of digital evidence, reflecting its complex nature. This subsection presents the linguistic, legal, and doctrinal definitions of digital evidence, followed by an analysis of its distinctive characteristics.

Sub-branch one: Definition (linguistic, legal, and doctrinal).

1-Linguistic Definition of Digital Evidence

Understanding digital evidence requires first examining the meaning of the words used to describe it. In legal research, and particularly in criminal law, definitions play an important role because they help clarify concepts before addressing legal rules and procedural mechanisms. The expression “digital evidence” is composed of two main terms: “digital” and “evidence”. Each term has its own meaning, and together they provide a first general understanding of this form of proof.¹

¹ **Abderahmane khalfi**, *ibid.*

From a linguistic perspective, the term “digital” refers to information represented in numerical form. In modern technological systems, this usually means data expressed through binary code based on the numbers 0 and 1. This method of representation allows information to be created, stored, processed, and transmitted by electronic devices such as computers, smartphones, servers, and digital networks. Any information that exists through this numerical system can therefore be described as digital.¹

The word “evidence”, in ordinary language, refers to proof or any element used to establish the truth of a fact. It serves to confirm that an event occurred or that a claim is valid. Evidence may take different forms, including documents, objects, or observable signs. This general meaning is essential in criminal law, where evidence plays a central role in determining criminal responsibility.

When the terms “digital” and “evidence” are combined, the expression “digital evidence” generally refers to proof that exists in electronic or numerical form and that is linked to digital systems. From a linguistic point of view, digital evidence can therefore be understood as data or information with probative value that is created, stored, or transmitted through digital technology. This definition is simple and accessible, making it useful as an introductory explanation of the concept. However, it remains limited because it does not address the legal value or procedural rules governing such evidence.²

One of the key aspects revealed by the linguistic and doctrinal analysis of digital evidence is its intangible nature. digital evidence differs fundamentally from traditional physical evidence in that it cannot be perceived directly by human senses. Instead, it exists in electronic form within digital systems and can only be

¹**Eoghan Casey**, Digital Evidence and Computer Crime, forensic science, computers and the internet, 3ed, amsterdam, 2011, p.p 5–7.

²**Abderahmane khalfi**, algerian criminal procedures, op cit, p. 301.

accessed through specialized technical tools and software. This immaterial character implies that digital evidence requires specific procedures for handling, preservation, and examination, and it also presents unique challenges for criminal investigations, particularly in terms of integrity, reliability, and admissibility before the courts.¹

In Algerian legal doctrine, this linguistic approach is often used as a starting point before moving to legal and procedural analysis. Understanding the nature of electronic data helps clarify how digital evidence functions within criminal proceedings, particularly in cases involving modern technologies and personal data crimes. This step allows a smoother transition toward legal definitions and doctrinal discussions.²

In conclusion, from a linguistic perspective, digital evidence refers to proof that exists in numerical or electronic form as a result of the use of digital systems. While this definition helps introduce the concept in a clear and understandable way, it is not sufficient on its own. For this reason, it must be complemented by legal and doctrinal definitions, which allow a deeper understanding of the role and value of digital evidence in criminal law.

2. Legal Definition of Digital Evidence

After explaining the linguistic meaning of digital evidence, it is necessary to examine its legal definition. In criminal law, a legal definition is essential because it determines how evidence can be collected, used, and evaluated by courts. Unlike ordinary language, legal definitions are closely linked to legality,

⁻¹ **Eoghan Casey**, *Digital Evidence and Computer Crime*, op cit, p.p. 3–7.

⁻² **Abderahmane khalfi**, *algerian criminal procedures*, op cit, p300.

procedure, and protection of individual rights. For this reason, digital evidence must be understood through legal texts and legal doctrine.

The Algerian legislation does not provide a single and explicit definition of digital evidence. Neither Criminal Procedures Law No. 25-14 nor Law No. 25-11 on personal data protection contains a direct definition of this concept. However, both laws refer to electronic means, digital data, and modern investigation techniques. This shows that digital evidence is legally recognized, even if it is not formally defined as a separate category.

Criminal Procedures Law No. 25-14 allows judicial authorities to use electronic means during criminal investigations. It authorizes the collection of electronic data, the seizure of digital devices, and the use of technical methods to access stored information. This law integrates digital evidence into the traditional system of criminal proof by subjecting it to procedural legality and judicial control.¹

In Algerian law, digital evidence is not defined by a single legal text, but it is clearly recognized through procedural rules and personal data legislation. It can be understood as electronic data that is lawfully obtained and used to prove a crime or establish criminal responsibility. This legal understanding combines Algerian doctrine and comparative studies and prepares the analysis of procedural rules discussed in the next part.

3. Doctrinal Definition

Legal doctrine has played a fundamental role in the construction of the concept of digital evidence. This role became necessary because classical criminal law was developed in a context where evidence was mainly physical, visible, and directly perceptible by human senses. Objects, written documents, confessions, and

⁻¹ **Abderahmane khalfi**, *ibid* , p.p 300-303

witness testimony formed the traditional core of proof. The emergence of digital technologies has deeply disrupted this structure. Crimes are now often committed through electronic systems, without physical contact and without leaving visible traces. Doctrine therefore intervenes to explain how these new traces can be integrated into criminal law.

In doctrinal analysis, digital evidence is generally understood as electronic data that is capable of proving a legally relevant fact within criminal proceedings. This understanding shifts the focus away from the technical form of the data and places it on its legal function. Digital evidence is not defined only by the fact that it is electronic, but by its capacity to support judicial reasoning. This approach is essential because modern digital systems generate enormous quantities of data, most of which has no legal relevance. The doctrinal concept helps isolate the data that can truly contribute to establishing the truth.¹

Another central doctrinal element concerns the immaterial nature of digital evidence. Unlike traditional evidence, digital evidence has no physical substance. It exists as sequences of codes stored on electronic media or circulating through networks. This immateriality creates uncertainty and sometimes mistrust, especially for judges trained in classical evidentiary models. Doctrine insists that the absence of physical form does not reduce evidentiary value, but it does require special handling and interpretation.

Digital evidence cannot be evaluated through direct observation, but only through technical processes that translate data into readable form.¹

The ease with which digital data can be copied, transferred, or modified is another major doctrinal concern. Unlike a physical object, a digital file can exist in

⁻¹ **Eoghan Casey**, Digital Evidence and computer Crime, op cit, p.p 67

multiple identical copies without loss of information. This characteristic challenges traditional ideas of originality and uniqueness. The authenticity in digital evidence does not depend on physical originality, but on integrity and traceability. The key question is not whether the data is “original,” but whether it has remained unchanged from the moment of collection to its presentation before the court.¹

The Doctrinal researches also see the indirect nature of digital evidence. Digital traces do not directly show the criminal act; they reflect interactions between a user and a technical system. This means that digital evidence always requires interpretation. An email, a log file, or a connection record only acquires meaning when placed in context. This context includes technical parameters, system settings, and patterns of human behavior. Doctrine highlights that misunderstanding this context can lead to serious judicial errors.²

The relationship between digital evidence and human responsibility is therefore a central doctrinal issue. Criminal law is based on personal responsibility, intention, and fault. Digital systems, however, often function automatically and may involve multiple users. Doctrine clarifies that digital evidence is never self-sufficient; it must always be connected to a human actor. Establishing this link is often complex, especially in cases involving shared devices, stolen credentials, or anonymous networks. This complexity explains why digital evidence rarely stands alone and usually needs to be supported by additional proof³.

¹ **Ghribi abdelkader**, (Legal Value of Forensic Digital Evidence : Between the Requirements of the Legal Text and _the Demands of the Digital Environment), journal of legal and economic research, 02, research center for Islamic sciences and civilization, laghouat, Algeria, 2025.

² **Kadri Saoucen., & Abbar Omar**, (Digital evidence between a personal conviction of the criminal judge and Supreme Court control), *Algerian Journal of comparative public law*, 01 university of belabes , 2024, p239.

³ **Bourtal Amina**, (Proving Electronic Crime With Digital Evidence According to Algerian Legislation), *Algerian Journal of Legal and Political Sciences*, 01, university of ain temouchent, 2026, p ,48.

Doctrinal analysis further addresses the role of technical expertise. Digital evidence is deeply technical, and judges often lack the specialized knowledge required to understand how data is created, stored, and extracted. Doctrine accepts the necessity of expert intervention, but at the same time warns against excessive dependence on technical opinions. Expert reports should assist the judge, not replace judicial reasoning. The doctrinal definition of digital evidence therefore includes a methodological dimension, reminding courts that technical explanation and legal evaluation are distinct tasks¹.

Another important doctrinal dimension concerns procedural legality. Digital evidence cannot be separated from the conditions under which it is collected. Electronic data often relates to private life, communications, and personal data. Doctrine strongly insists that evidence obtained through unlawful access, unauthorized surveillance, or violation of privacy loses its legitimacy. This position aims to preserve the balance between the efficiency of criminal justice and the protection of fundamental rights.²

In the Algerian legal context, doctrinal reflection integrates digital evidence into existing procedural principles rather than treating it as an exceptional category. Algerian scholarship emphasizes that digital evidence must respect the principle of legality, judicial control, and the rights of the defense. Electronic traces are accepted as evidence only when they are collected within the framework of criminal procedure and under judicial supervision³.

Doctrinal analysis in Algeria also highlights the strong connection between digital evidence and personal data protection. Many digital traces involve sensitive

⁻¹ **Beladjeraf, S.** The Authority of the Criminal Judge to Accept and Appreciate Digital Evidence. *Journal of Comparative Legal Studies*, 2021, p.p 685-686.

⁻² **Ghribi Abdelkader**, op cit, p.p 164 -165.

⁻³ **Abderahmane khalfi**, op cit p.p 301 -303.

personal information. The use of such data in criminal proceedings must therefore remain proportionate and justified. The evidentiary value of digital data is reduced or excluded when its use results in serious violations of privacy. This approach reflects a broader doctrinal concern for maintaining public confidence in the justice system².

In a broader sense, doctrinal definitions aim to stabilize judicial practice in a rapidly changing technological environment. By identifying the essential characteristics of digital evidence immateriality, dependence on human activity, technical mediation, and procedural legality doctrine provides judges with conceptual tools to evaluate electronic proof more consistently. This stability is particularly important in personal data crimes, where technical complexity and rights protection are closely intertwined.

This concept has gained increasing importance with the expansion of digital technologies and their use in criminal activities.

It is any evidence that can be derived from a computer or other electronic devices. It is also considered a means of proof in legal proceedings through which the disputed fact can be established using modern technological tools. It may further be defined as any data that can be stored, transmitted, or multiple process by a computer, and which may take forms. Accordingly, digital evidence refers to any element that can be relied upon to prove crimes committed through electronic means

In conclusion, doctrinal analysis defines digital evidence as electronic data with probative value, derived from human interaction with digital systems, and integrated into criminal proceedings through lawful and controlled procedures. This definition goes beyond technical description and addresses the human, legal,

^{2 1} **Abderahmane khalfi**, op cit, p.p 304-305

and procedural dimensions of electronic proof. Through this expanded understanding, doctrine ensures that digital evidence can be used effectively in criminal justice while respecting the fundamental principles of Algerian law.

Sub-branch Two: Distinctive Features of Digital Evidence

Digital evidence has several distinctive features that clearly differentiate it from traditional forms of criminal evidence. These features explain why digital evidence requires specific legal treatment and why classical procedural rules are often insufficient when dealing with electronic proof. In crimes related to personal data, digital evidence is usually the main or even the only source of proof. For this reason, understanding its characteristics is essential for ensuring both the effectiveness of criminal prosecution and the protection of individual rights.³

1. Intangible Nature of Digital Evidence

The first and most fundamental characteristic of digital evidence is its intangible nature. Unlike physical evidence, digital evidence has no material existence. It cannot be touched, held, or observed directly by human senses. Instead, it exists only in the form of electronic data stored on digital devices, servers, or online platforms. Access to this data always requires the use of technical tools and specialized software.

This immaterial nature creates important legal and practical difficulties. Investigators cannot seize digital evidence in the same way as traditional evidence. While a physical object can be placed under seal and preserved, digital data must be extracted, copied, and secured through technical processes. Any mistake during this process may result in the loss of information. The absence of physical form also makes digital evidence more vulnerable, since its

1. Ghribi Abdelkader, *op cit*, p.p 164 -165

disappearance often leaves no visible trace. This increased risk linked to intangibility is widely emphasized in doctrinal analysis¹.

The intangible nature of digital evidence also affects judicial perception. Judges are traditionally trained to assess tangible proof. Electronic data, however, appears abstract and distant from everyday experience. This may create mistrust or misunderstanding. Doctrine therefore insists that immateriality should not be confused with unreliability. Digital evidence can be highly precise, but only if it is properly collected and explained within a clear legal framework.²

2. Fragility and Volatility of Digital Evidence

Another essential feature of digital evidence is its fragility and volatility. Electronic data is extremely sensitive to manipulation, deletion, and alteration. Even simple and ordinary actions may affect stored data. Restarting a computer, connecting a device to the internet, or opening certain applications can automatically modify system files, logs, or metadata.

This volatility makes the early stages of investigation particularly critical. If investigators intervene too late or without proper precautions, valuable digital traces may be irreversibly lost. This risk exists even when there is no intention to destroy evidence. Automatic system processes may erase or overwrite data without human intervention. For this reason, doctrine stresses the need for immediate and careful handling of digital devices once they are identified as potential sources of evidence.³

¹ Ghribi Abdelkader. Ibid p.p 152–153

² Beladjeraf, S. The Authority of the Criminal Judge to Accept and Appreciate Digital Evidence. Journal of Comparative Legal Studies, 2021, p. 680.

³ Eoghan Casey, op cit, p 19

The fragile nature of digital evidence also explains why preservation techniques are so important. Specialized methods are required to secure data while maintaining its integrity. Without such methods, the evidentiary value of digital proof may be challenged before the court. Volatility therefore justifies the development of specific procedural safeguards adapted to electronic evidence.¹

3. Ease of Duplication and Reproducibility

Digital evidence is also characterized by its ease of duplication. Unlike physical evidence, digital data can be copied perfectly, without any loss or alteration of content. This feature offers significant advantages for criminal investigations. Investigators and experts can work on copies of the data, allowing the original source to remain preserved and untouched.

However, ease of duplication also raises serious legal concerns. When multiple identical copies exist, it becomes difficult to identify which version should be considered the reference. Questions of authenticity and integrity naturally arise. The court must be assured that the data presented during trial corresponds exactly to the data originally collected. For this reason, strict procedural controls are required to document each step of the duplication process.²

This characteristic challenges traditional evidentiary concepts such as originality. In the digital context, originality is replaced by integrity and traceability. Doctrine explains that the value of digital evidence depends less on its physical uniqueness and more on the ability to demonstrate that it has not been altered throughout the procedure.³

¹ Beladjeraf, S p. 682.

² Brenner susan, *Cybercrime and the Law: Challenges, Issues, and Outcomes*, Northeastern University Press, 2012, p.p 179–181.

³ Mostefaoui Abdelkader, (La protection de la vie privée à l'épreuve de l'extension des pouvoirs d'enquête), *Journal of Law and Human Sciences*,2, algeries, 2021, p. 136.

4. Technical Complexity and Dependence on Expertise

Digital evidence is deeply technical. Its collection, preservation, analysis, and interpretation require specialized knowledge that goes beyond general legal training. Judges, prosecutors, and defense lawyers often depend on technical experts to understand how digital systems function and how electronic traces are generated.

This dependence introduces new challenges for criminal justice. While expert assistance is necessary, it must remain under judicial control. There is a risk that technical complexity may overshadow legal reasoning. Doctrine therefore insists on maintaining a clear distinction between technical explanation and legal evaluation. Experts explain how data works; judges decide its legal value. Excessive reliance on experts may weaken judicial independence and affect the balance of the trial¹.

Technical complexity also affects the rights of the defense. If digital evidence is not clearly explained, the accused may be unable to challenge it effectively. This situation raises concerns related to equality of arms and fair trial guarantees.

5. Risk of Manipulation and Integrity Issues

Digital evidence is particularly exposed to the risk of manipulation. Specialized software tools can modify, fabricate, or falsify electronic data with relative ease. This possibility creates constant doubts regarding authenticity and reliability, especially when procedural safeguards are weak or absent.

To address this risk, doctrine highlights the importance of integrity controls, chain of custody, and detailed documentation. Every action taken on digital evidence

¹ Kadri, S., & Abbar, O, op cit, p. 239.

must be recorded from the moment of seizure until presentation before the court. In the Algerian legal context, the principle of legality plays a protective role by imposing limits on investigative powers and ensuring judicial supervision¹.

Manipulation risks also explain why digital evidence is often assessed together with other forms of proof. Electronic traces rarely stand alone. They must be supported by contextual elements to strengthen judicial confidence.

Digital evidence is distinguished by its immaterial nature, fragility, ease of duplication, technical complexity, and vulnerability to manipulation. These features justify a specific legal approach adapted to electronic proof. In personal data crimes, where digital traces play a central role, understanding these characteristics is essential for ensuring both effective repression and respect for fundamental rights within the Algerian criminal justice system.²

Subsection Two: Application of Digital Evidence in Personal Data Crimes

Personal data crimes are closely linked to digital environments. They involve unlawful access, processing, or disclosure of personal data stored electronically.

Digital evidence is the primary means to prove such crimes. This subsection explains the concept of personal data, the scope of its legal protection, and the main types of personal data crimes.

Sub-branch One: Concept of Personal Data and Scope of Legal Protection

The notion of personal data has become central in contemporary legal systems due to the rapid digital transformation of society. Daily activities such as communication, online services, electronic payments, and administrative

⁻¹ **Abderahmane Khalfi**, op cit, p.p 304-307.

⁻² **Beladjeraf s** , op cit p 686.

procedures generate large amounts of information related to individuals. Legal doctrine explains that this evolution has increased the exposure of individuals to risks related to misuse of information¹ In criminal law, personal data often appears either as the object of the crime or as an element involved in the investigation, which explains the need for a precise legal framework.

In the context of Algerian law, the importance of personal data protection has been formally recognized through the adoption of Law No. 25-11. This law establishes the basic legal framework governing the collection and processing of personal data. the introduction of this law reflects Algeria's alignment with international trends in data protection while maintaining national legal specificities.²

1. Definition of Personal Data

Personal data refers to any information relating to an identified or identifiable natural person. Identification may be direct, such as through a name, or indirect, through numbers or technical identifiers. This broad understanding corresponds to the reality of digital environments, where individuals are often identified through electronic traces rather than physical presence³

Terminological Definition

(Personal data is defined as any information, audio recording, or image relating to an identified or identifiable person, whether directly or indirectly. In other words, it includes any element capable of establishing a person's identity by

⁻¹ **Mostefaoui Abdelkader**, op cit p 135.

⁻² Article 3, Law No. 18-07 of June 10, 2018, relating to the protection of individuals in the processing of personal data. Official Gazette of the Algerian Republic, No 34.

⁻³ **Titouche**, Radia. The territorial principal of criminal law and cybercrime, voice of Law Magazine 02, University of tizi ouazou,p. 538.

reference to distinguishing characteristics such as physical, biological, or genetic features, among others.

With reference to computer and internet dictionaries, the term **“Data”** is defined as the set of information generated by a user, whether in the form of documents, images, or audio recordings.

Furthermore, a review of certain legislations reveals the existence of similar terminology referring to this concept, such as “personal data,” “nominal data,” “data of a personal nature,” as well as the terms “data” and “information.” Despite their differences in wording, these terms essentially convey the same meaning.⁴

Doctrinal Definition

The doctrinal approach focuses primarily on data directly related to the concerned individual, excluding other data that may indirectly lead to their identification, such as tools or means used by that person. Some legal scholars have used the term “data” while distinguishing between public data and private data, defining personal data as a set of information forming part of an individual’s private life, the disclosure of which may cause harm to its subject.

Another doctrinal view considers personal data as information directly linked to a specific individual, such as their name, social status, place of residence, and criminal record, which are regarded as inherent elements of personality rights.

Scholars have diverged in establishing a unified concept of personal data. A segment of French legal doctrine defines it as all information related to private life, including health status, family situation, professional activity, economic and social condition, as well as family secrets.

⁻¹ Mostefaoui Abdelkader, op cit, p.p 152-154

⁻² article 6. 7. Law No. 18-07 op cit.

Conversely, another view holds that personal data encompasses various categories, including data related to private life, as well as information concerning identity, nationality, political and ideological orientations, religious beliefs, and financial and banking transactions. Accordingly, data acquires a personal character when it is linked to an individual, either directly or indirectly. Examples of direct personal data include address, telephone number, social security number, vehicle registration number, and email address. Indirect data refers to information that does not identify a person by itself but may lead to identification, particularly within the digital environment.

Data generated through internet use, such as email addresses or social media accounts, constitute personal data whenever they enable, directly or indirectly, the identification of a natural person. Determining whether data is direct or indirect requires a case-by-case assessment, taking into account the fact that the digital environment often challenges the traditional concept of civil identity due to the complexities faced by courts in identifying individuals. The diversity of identifying elements grants judges broad discretionary power in determining the personal nature of information, while ensuring a balance between the protection of privacy and the free flow of information, in light of ongoing technological advancements.

From the foregoing, it is evident that legal doctrine has not reached a unified definition of personal data, raising the question of how legislation addresses this divergence.⁶

Legislative Definition

As a general rule, legislators tend to avoid providing precise definitions, leaving this task to legal doctrine and judicial interpretation. However, it is observed that

⁻¹ Article 3, Law No. 18-07 op cit .

many modern legislations have explicitly defined personal data within their legal texts.

The Algerian legislator has followed this approach through Law No. 25-11, which provides definitions of both personal data and the processing of such data under Article 3. Nevertheless, a degree of ambiguity remains in these definitions, particularly in distinguishing them from the concept of privacy.

Personal data is considered broader in scope than private life, as any violation of privacy constitutes a violation of personal data, whereas the reverse is not necessarily true. Article 2 of Law No. 25-11 emphasizes that personal data must be processed in a manner that respects human dignity, private life, and public freedoms, without infringing upon individuals' rights, honor, or reputation.

This broader scope is further confirmed by the definition provided in Article 3, which states that personal data includes: “Any information, regardless of its medium, relating to an identified or identifiable person.”)

Article 2 of Law No. 25-11 provides a clear statutory definition. It defines personal data as “any information, regardless of its form, relating to an identified or identifiable natural person” (Law No. 25-11, Art. 2). The expression “regardless of its form” is legally significant, as it includes written, visual, sound, and electronic data. This formulation allows the law to adapt to technological change without constant legislative amendments.⁷

The law also gives examples that clarify the scope of personal data. These include names, identification numbers, electronic identifiers, and location data (Law No. 25-11, Art. 2). Electronic identifiers such as IP addresses, user accounts, and device identifiers play a key role in digital identification. Location data is particularly sensitive because it allows the monitoring of a person's movements

⁻¹ Article 3, Law No. 18-07 op cit .

and daily habits. these examples show the legislator's awareness of modern technological risks.¹

The breadth of this definition has important consequences for criminal proceedings. Many types of data used by investigators may fall within the scope of personal data, even when they appear purely technical. As a result, judicial authorities must respect legal safeguards when accessing or processing such data, otherwise they risk violating privacy rights protected by law²

2. Legal Protection of Personal Data in Algeria

The legal protection of personal data in Algeria is based on several fundamental principles established by Law No. 25-11. These principles regulate how personal data may be collected, processed, stored, and used. They apply to public authorities and private actors, including in situations related to criminal investigations (Law No. 25-11).

One of the central principles is consent. Personal data should, in principle, be collected and processed with the consent of the concerned person. This principle reflects respect for individual autonomy and private life. Although criminal investigations may justify exceptions, consent remains a reference point that limits arbitrary interference.³

Another essential principle is purpose limitation. Personal data must be collected for specific and legitimate purposes and must not be reused for incompatible objectives. This rule aims to prevent excessive accumulation and misuse of

⁻¹ Article 3, Law No. 18-07 op cit .

⁻² **Mostefaoui Abdelkader**, op cit, p.p 141-142.

⁻³ article 6. 7. Law No. 18-07 op cit.

personal information. In criminal matters, it limits the possibility of reusing data collected for administrative or commercial purposes without legal authorization¹.

Security obligations are also a core element of legal protection. Data controllers must take appropriate technical and organizational measures to protect personal data against unauthorized access, loss, or alteration. This obligation is particularly important in digital environments, where data breaches may lead to serious violations of individual rights.²

Compliance with personal data protection rules is supervised by the **Autorité Nationale de Protection des Données à caractère Personnel (ANPDP)**. This authority monitors data processing activities and may intervene when violations occur. the ANPDP plays both a preventive and corrective role, ensuring that data protection rules are effectively applied.³

Legal doctrine also emphasizes that criminal law complements administrative supervision. When violations of personal data protection reach a serious level, criminal sanctions intervene to punish unlawful behavior. This complementary relationship strengthens the overall system of protection and enhances its deterrent effect.⁴

Sub-branch two: Major types of personal data crimes (Hacking, espionage, unlawful modification, disclosure)

Personal data crimes represent one of the most serious consequences of the digital transformation of society. In Algeria, the growing use of electronic systems in administration, business, and private life has increased the exposure of personal

¹ Mostefaoui Abdelkader, op cit, p 136.

² article 41.42, Law No. 18-07 op cit.

³ Bourtal, A. (2024). Proving Electronic Crime With Digital Evidence According to Algerian Legislation, p. 47.

⁴ Titouche, R. (2018). Territorialité du droit pénal et cybercriminalité. *Review of the Voice of Law*, p. 538

data to unlawful practices. These crimes are generally committed through digital means and do not require physical contact with the victim or the data storage location. As a result, digital evidence becomes the primary, and sometimes the only, way to establish the existence of the offense and the responsibility of the offender.

Algerian criminal law addresses these crimes through a combination of general criminal rules and specific legal texts related to cybercrime and personal data protection. Understanding the main types of personal data crimes is essential in order to appreciate the role and importance of digital evidence in criminal proceedings.¹

1. Illegal Access to Personal Data (Hacking)

Illegal access, commonly referred to as hacking, consists of entering a computer system, database, or electronic network without authorization, with the aim of accessing personal data. This offense may target public institutions, private companies, or individual users. In many cases, the offender exploits technical vulnerabilities or stolen credentials to bypass security measures.

From an evidentiary perspective, illegal access is rarely proven through traditional means such as witness testimony or physical objects. Instead, investigators depend on digital evidence such as access logs, authentication records, IP addresses, and system activity reports. These technical elements make it possible to establish that access occurred, determine the date and time of the intrusion, and sometimes identify the device or network used.²

¹ **Bourtal**, A. (2024). Proving Electronic Crime With Digital Evidence According to Algerian Legislation. *Algerian Journal of Legal and Political Sciences*, p.p. 48–49.

² **Eoghan Casey**, *op cit*, p. 176.

In Algerian criminal procedure, the use of such digital evidence must comply with strict legal conditions. The electronic traces obtained during investigations are admissible only if they are collected lawfully and under judicial supervision, especially when they involve private systems or personal data¹. This shows that while digital evidence is indispensable in hacking cases, its legal value depends on respect for procedural guarantees.

2. Digital Espionage Involving Personal Data

Digital espionage refers to the secret and continuous collection of personal data without the knowledge of the data subject. Unlike hacking, which may occur in a single act, espionage often takes place over an extended period. It may involve the use of spyware, key loggers, or remote surveillance tools that allow the offender to monitor activities and extract sensitive information.

The digital evidence associated with espionage cases is often complex and technical. It may include traces left by malicious software, abnormal data transfers, communication records with external servers, and forensic reports identifying hidden programs. These elements help demonstrate that personal data was collected covertly and transmitted to unauthorized parties.²

One of the main difficulties in espionage cases is attributing the offense to a specific person, as offenders frequently use anonymization techniques or operate remotely.

This difficulty increases the importance of expert analysis and reinforces the need for judges to carefully assess the reliability and coherence of digital evidence presented before the court.

¹ **Abderahmane Khalfi**, op cit, p.p 310-314

² **Brenner süssan**, op cit, p. 57

3. Unlawful Modification of Personal Data

Unlawful modification occurs when personal data is altered, deleted, or falsified without legal authorization. This crime directly affects the integrity and accuracy of personal information, which may lead to serious consequences for individuals, such as identity fraud, financial loss, or administrative problems. The offense may be committed by external attackers or by insiders who misuse their access rights.¹

Digital evidence is crucial in proving unlawful modification. Investigators rely on system logs, modification histories, digital timestamps, backup files, and audit trails to show that data was changed and to identify the moment and method of the alteration. These technical records allow a reconstruction of events and help distinguish lawful operations from criminal acts.

Digital timestamps and system records have strong evidentiary value because they are automatically generated and difficult to falsify without leaving traces².

In Algerian practice, such evidence supports the judge's personal conviction, provided that it is collected and analyzed in accordance with legal procedures.

4. Illegal Disclosure of Personal Data

Illegal disclosure involves the communication or sharing of personal data with third parties without a lawful basis or without the consent of the person concerned. This crime is increasingly common due to the widespread use of social networks, messaging applications, and electronic communication platforms. Disclosure may occur intentionally, for profit or revenge, or as a result of serious negligence.

⁻¹ Bourtal, A. (2024)., p48-. 51

⁻² Eoghan Casey, op cit, p 176

To establish illegal disclosure, digital evidence such as screenshots, email exchanges, transmission logs, metadata, and platform records is commonly used. These elements help prove that the data was communicated, identify the recipient, and determine the responsibility of the person who disclosed the information.

Courts must apply the principle of proportionality when assessing digital evidence in disclosure cases, in order to avoid unnecessary violations of privacy¹. This approach is consistent with Algerian law, which seeks to repress unlawful disclosure while ensuring respect for fundamental rights and procedural fairness.

Section One showed that digital evidence has a unique legal nature and specific characteristics that distinguish it from traditional evidence. It also demonstrated the close relationship between digital evidence and personal data crimes under Algerian law.

Section Two: Principles and Legal Controls Governing Digital Evidence

The use of digital evidence in criminal cases cannot be separated from legal principles and procedural safeguards. While digital evidence is essential for uncovering personal data crimes, its use may seriously affect individual rights, especially the right to privacy and the right to a fair trial.

For this reason, criminal law imposes several principles and legal controls that govern how digital evidence is collected, preserved, and used. These principles aim to balance two objectives: the effectiveness of criminal justice and the protection of fundamental rights.

¹ Mostefaoui Abdelkade, *op cit* , p. 135.

In Algerian law, this balance is ensured through the principle of legality, procedural admissibility rules, and institutional supervision, notably by the authority responsible for personal data protection. International standards also play an important role in shaping modern approaches to digital evidence.

This section examines these principles and controls in detail.

Subsection One: Principle of Legality and Procedural Admissibility

The principle of legality is a cornerstone of criminal procedure. It requires that any evidence used against an accused person must be collected and used according to the law. This principle is particularly important in the digital context because investigative measures often involve intrusion into private life.⁸

Procedural admissibility ensures that only lawful and reliable evidence is accepted by courts. In digital cases, admissibility depends on strict respect for legal conditions, judicial authorization, and procedural documentation.

Sub-branch One: Importance of Legality in Criminal Evidence

1. Meaning of the Principle of Legality

The principle of legality in criminal evidence requires that all proof used in criminal proceedings be obtained in strict conformity with the law. This principle limits the powers of investigative authorities and ensures that criminal investigations are conducted within a legal framework. In criminal justice, the goal is not only to establish the truth, but to ensure that this truth is reached through lawful and fair methods.

In Algerian criminal procedure, legality governs all stages of the evidentiary

¹ Beladjeraf, S. (2021). The Authority of the Criminal Judge to Accept and Appreciate Digital Evidence. *Journal of Comparative Legal Studies*, p.p 677-678

Chapter one: Conceptual and Legal Framework of Digital Evidence in Personal Data Crimes.

process. It applies from the opening of the investigation to the presentation of

evidence before the court. Every investigative act, such as searches, seizures, interceptions, and recordings, must respect the conditions defined by law. If these conditions are violated, the evidence may lose its probative value, regardless of its relevance.

Legality also contributes to legal certainty by establishing clear and predictable rules. Investigators know the limits of their powers, and individuals are protected against arbitrary interference. This framework strengthens confidence in criminal justice and reinforces the authority of judicial decisions.¹

Furthermore, the principle of legality reflects the idea that justice must respect both public order and individual rights. Criminal repression cannot be effective if it relies on unlawful practices. The credibility of criminal justice depends on the respect of legal procedures at every stage.²

2. Legality as a Guarantee Against Arbitrary Use of Power

Criminal investigations grant the state significant powers that may seriously affect individuals. These powers include searching private spaces, accessing personal information, and monitoring communications. Without legal limits, such powers could easily be misused. The principle of legality acts as a safeguard that prevents arbitrary or excessive investigative practices.

In practice, legality requires investigators to act only within the scope defined by law. Prior judicial authorization is often required, especially when investigative measures interfere with private life. The duration, purpose, and methods of

¹ Beladjeraf, S. op cit.

² Titouche, R. (2018). Territorialité du droit pénal et cybercriminalité. Review of the Voice of Law, p. 538.

investigation must also respect legal limits. These requirements apply equally to traditional investigations and to digital investigations.

Legality also allows for judicial and defense control. Evidence obtained through unlawful means may be challenged before the court. This possibility strengthens procedural balance and reinforces the right of defense. It also encourages investigators to strictly respect legal procedures.

By limiting the discretionary power of authorities, legality ensures that criminal investigations remain justified, proportionate, and controlled. This contributes to the legitimacy of the criminal justice system and prevents abuses of power.¹

3. Legality and the Protection of Fundamental Rights

The principle of legality is closely connected to the protection of fundamental rights and freedoms. Criminal investigations often interfere with private life, secrecy of correspondence, and protection of personal data. These interferences are particularly significant in cases involving digital evidence, where large amounts of personal information may be accessed, stored, or analyzed.

The Algerian Constitution guarantees the protection of private life. Any limitation of this right must therefore be legally justified and proportionate to the seriousness of the offense. Legality ensures that investigative measures do not exceed what is strictly necessary for the needs of the investigation.²

In digital investigations, legality requires strict control over electronic surveillance, interception of communications, and access to digital data. These measures must be carried out under judicial supervision and within precise legal

⁻¹ **ABDERAHMANE Khalfi**, op cit, p.p 288–292.

⁻² Constitution of the People's Democratic Republic of Algeria (2020), Articles 47 and 48

conditions. This legal framework protects individuals from unjustified intrusion into their personal lives.

Respect for legality also reinforces fair trial guarantees. When evidence is obtained through lawful means, the parties can trust the judicial process. Conversely, violations of legality may weaken confidence in the fairness and legitimacy of criminal proceedings.

4. Consequences of Illegality in Criminal Evidence

Illegality in the collection of evidence has serious procedural consequences. Evidence obtained in violation of legal rules may be excluded from the case file or assigned limited probative value by the judge. This consequence reflects a fundamental principle of criminal justice: unlawful methods cannot be used to establish lawful convictions.

The exclusion of illegal evidence plays an important preventive role. It encourages investigators to respect legal procedures and discourages the use of unlawful investigative practices. This contributes to improving the quality and professionalism of criminal investigations.

Illegality also affects the credibility of evidence. Even when the factual content of the proof appears convincing, its unlawful origin may raise doubts about its integrity and authenticity. Judges must therefore assess not only the substance of the evidence, but also the conditions under which it was obtained. This approach reinforces the idea that justice must be fair in both its objectives and its methods. The search for truth cannot justify the violation of legal safeguards.¹

¹ **Beladjeraf, S.** (2021). The Authority of the Criminal Judge to Accept and Appreciate Digital Evidence. *Journal of Comparative Legal Studies*, 7(1), p.p. 679–680

5. Enhanced Importance of Legality in Digital Evidence

In criminal investigations, the value of digital evidence depends on how it is collected and handled. Digital data is fragile and can be modified easily, sometimes without leaving any trace.

For this reason, it is essential that any collection of electronic evidence follows strict legal procedures, including obtaining proper authorization, documenting actions carefully, and maintaining the chain of custody. These measures help ensure the integrity of the data and make it possible for the court to evaluate its reliability, respecting legal and technical standards is critical to guarantee both the authenticity and the credibility of digital evidence.¹

6. Legality and the Formation of Judicial Conviction

Legality plays a decisive role in the formation of the judge's personal conviction. Judges must base their decisions on evidence that is both legally obtained and factually convincing. Any violation of legality may weaken the persuasive force of the evidence, even if it appears technically reliable.

In Algerian criminal procedure, the judge enjoys freedom in assessing evidence, but this freedom is exercised within the limits imposed by law. Respect for legality strengthens judicial confidence in the evidence and contributes to reasoned and fair decisions.

Legality therefore represents a substantive guarantee of justice. It protects individual rights, ensures procedural fairness, and reinforces the credibility and legitimacy of criminal justice as a whole.²

⁻¹ Eoghan Casey, op cit, p. 26.

⁻² Abderahmane Khalfi, op cit p.p 288–292.

Sub-branch Two: Legal controls for collecting digital evidence

The collection of digital evidence raises serious legal concerns due to its technical nature and its direct impact on private life and personal data. Because digital investigations may involve accessing communications, devices, and sensitive information, Algerian criminal law imposes strict legal controls to regulate these practices. These controls aim to prevent abuse, protect fundamental rights, and ensure that digital evidence remains reliable and admissible before the courts.

1. Judicial Authorization

Judicial authorization is one of the most important legal controls in the collection of digital evidence. Many investigative measures affecting digital data cannot be carried out freely by investigators. Measures such as interception of communications, access to stored electronic data, and online surveillance require prior authorization from a competent judicial authority.

This requirement ensures that intrusive investigative actions are not conducted arbitrarily. Judicial authorization allows an independent authority to verify the necessity and proportionality of the measure in relation to the seriousness of the offense. It also limits the scope and duration of the investigative action, reducing the risk of excessive intrusion into private life.

In Algerian criminal procedure, judicial authorization functions as a protective mechanism that balances the needs of criminal investigation with the protection of individual rights. Without such authorization, digital evidence obtained through intrusive measures may be contested and lose its evidentiary value.¹

¹ **Abderahmane Khalfi**, *ibid* p.p 293–207.

2. Respect of Procedural Formalities

The collection of digital evidence in criminal investigations presents unique challenges due to the intangible, volatile, and easily modifiable nature of electronic data. Unlike traditional physical evidence, digital evidence can be altered by seemingly minor actions, sometimes leaving no visible trace. For this reason, judicial oversight and strict procedural safeguards are essential. Investigators must obtain prior judicial authorization, issue written orders, respect statutory time limits, and precisely identify the devices or systems targeted. These steps are not mere formalities; they constitute fundamental guarantees that protect the integrity of the evidence and the rights of individuals.¹

Adhering to procedural safeguards also ensures transparency and accountability. Written judicial orders provide a clear legal basis for investigative measures, helping to prevent arbitrary actions. Time limits limit unnecessary or prolonged interference with private life, while the careful identification of devices avoids overly broad searches that might compromise data unrelated to the alleged offense. Failure to comply with these procedures may seriously undermine the credibility and probative value of digital evidence, potentially leading to exclusion from court proceedings or a reduction in evidentiary weight.²

Beyond legal compliance, procedural rigor reinforces technical reliability. Digital evidence collected under proper legal conditions can be confidently analyzed and presented in court, whereas irregularly obtained data is vulnerable to challenge and dispute. Combining strict legal procedures with careful technical handling is essential to ensure that digital evidence is both admissible and trustworthy. In this way, adherence to formal procedures protects not only the integrity of individual

¹ Ghribi Abdelkader, op cit, p. 153

² Kadri, S., & Abbar, O. (2024). p. 238.

investigations but also the broader fairness and legitimacy of the criminal justice system.¹

3. Chain of Custody

The chain of custody is a fundamental legal and technical control in the handling of digital evidence. It consists of documenting every step in the collection, transfer, storage, and analysis of electronic data. This documentation allows the court to verify that the evidence has not been altered or manipulated.

Digital evidence is particularly vulnerable due to its intangible nature. A single unauthorized action may modify data without visible traces. The chain of custody provides assurance that the evidence presented before the court is the same as the evidence originally collected during the investigation. Any break or inconsistency in the chain of custody may raise doubts about the integrity of the evidence. Such doubts weaken the evidentiary value of digital data and may affect the judge's confidence in its reliability.²

4. Documentation and Transparency

Documentation and transparency are essential legal controls in the collection of digital evidence. Investigators must clearly document the technical methods used to extract, copy, and analyze electronic data. This documentation allows judicial authorities to review the legality and reliability of the investigative process.

Transparency also plays a key role in protecting the rights of the defense. When investigative methods are documented and accessible, the defense can challenge the legality or accuracy of the evidence.

¹ Eoghan Casey, op cit, p. p19.26

This possibility reinforces procedural fairness and equality of arms. Without proper documentation, digital evidence may appear opaque or unreliable. Transparency therefore contributes to judicial trust and ensures that digital investigations remain subject to legal control and adversarial debate.¹

Subsection Two: Role of Supervisory Authorities and International Standards

Beyond judicial control, modern criminal justice relies on institutional supervision and international norms. In cases involving personal data, specialized authorities play a key role in protecting individuals.

International standards also influence national law by setting minimum guarantees for legality, proportionality, and fair trial.

Sub-branch One: Powers of the ANPDP and Its Procedural Role

The protection of personal data in Algeria is ensured through both criminal law mechanisms and administrative supervision. In this context, the ANPDP occupies an essential place. Its role is not limited to prevention, but also extends to supporting the detection of violations that may later become criminal matters. Although the ANPDP does not exercise judicial power, its activities influence criminal procedure in cases involving personal data crimes.

1. Legal Status of the ANPDP

The ANPDP is an independent administrative authority created by Law No. 25-11 on the protection of personal data. Its independence allows it to act objectively,

¹ **Beladjeraf, S.** (2021). The Authority of the Criminal Judge to Accept and Appreciate Digital Evidence. *Journal of Comparative Legal Studies*, p. 686.

without being subject to direct political or judicial pressure. This status reinforces its credibility and effectiveness in supervising data processing activities.

The main mission of the ANPDP is to ensure that personal data is processed in a lawful, transparent, and secure manner. This mission reflects the preventive dimension of data protection. By acting upstream, the authority aims to limit violations before they result in serious harm or criminal liability.¹

Although the ANPDP is not a judicial body, it plays an important role in identifying illegal practices. Its interventions may reveal behaviors that constitute criminal offenses under Algerian law. In this way, the authority contributes indirectly to the protection of personal data through the criminal justice system.

The establishment of the ANPDP demonstrates the legislator's intention to strengthen personal data protection by combining administrative oversight with criminal repression. This dual approach enhances the overall effectiveness of the legal framework.²

2. Supervisory Powers of the ANPDP

The ANPDP is entrusted with several supervisory powers designed to ensure compliance with personal data protection rules. These powers include monitoring data processing activities carried out by public institutions and private entities, receiving complaints from individuals, and issuing warnings or recommendations in case of violations.

⁻¹ Articles 44 and 45, Law No. 18-07 .

⁻² **Mostefaoui Abdelkader**, op cit, p. 142.

Through monitoring activities, the authority verifies whether data controllers respect legal obligations such as consent, purpose limitation, and data security. This supervision helps identify unlawful practices that may affect a large number of individuals.

The power to receive complaints is particularly important. Individuals whose personal data has been misused may report violations to the ANPDP. These complaints provide valuable information about illegal data processing practices and may reveal patterns of misconduct.

Warnings and recommendations issued by the ANPDP encourage compliance and allow entities to correct irregular practices. Although these measures are administrative in nature, they may play a decisive role in preventing criminal behavior or highlighting serious violations that require judicial intervention.

3. Procedural Impact of Supervisory Powers on Criminal Evidence

The supervisory powers of the ANPDP have an indirect but significant impact on criminal evidence. When the authority identifies unlawful data processing, this information may indicate the existence of personal data crimes. Such findings can serve as a basis for alerting judicial authorities.

Reports and observations produced by the ANPDP may help investigators understand the technical and legal context of the violation. They may also assist in identifying the actors involved and the methods used to process personal data unlawfully.¹

While the ANPDP does not collect criminal evidence in the strict sense, its activities contribute to the detection of criminal offenses. This cooperation strengthens the effectiveness of criminal investigations while respecting the separation between administrative and judicial functions.

Institutional coordination between administrative authorities and judicial bodies ensures a coherent response to personal data violations. It allows each institution to operate within its legal mandate while contributing to the protection of personal data.¹

4. Cooperation with Judicial Authorities

Cooperation between the ANPDP and judicial authorities is essential in cases involving personal data crimes. While judicial authorities are responsible for conducting investigations and assessing criminal responsibility, the ANPDP provides technical and regulatory support.

Information communicated by the ANPDP may trigger criminal investigations or support evidentiary analysis. This cooperation helps judicial authorities deal with the technical complexity of digital environments and personal data processing systems.

Such collaboration must respect procedural guarantees and the rights of the defense. The role of the ANPDP remains supportive, ensuring that criminal proceedings are based on reliable and legally obtained information.

Effective cooperation contributes to a more efficient and balanced criminal justice system, particularly in cases involving complex digital evidence.¹

5. Limits of the ANPDP's Procedural Role

Despite its importance, the ANPDP has clear limits. It does not possess judicial powers and cannot conduct criminal investigations or impose criminal sanctions. Criminal proof remains exclusively under the authority of judicial bodies.

¹ Article 49 and 51, Law No. 18-07,.

This separation of roles protects procedural fairness and prevents the concentration of powers in a single institution. Judicial authorities retain full control over evidence assessment, prosecution, and sentencing.

The ANPDP's role is therefore complementary. It strengthens prevention, detection, and cooperation without interfering with judicial independence. This balance ensures respect for fundamental rights and reinforces confidence in the legal system.¹

Sub-branch Two: Influence of International Standards

1. The Budapest Convention

The Budapest Convention on Cybercrime represents the first international effort to create common legal tools to fight crimes committed through digital technologies. It was adopted to respond to the growing use of computers and networks in criminal activities, including offenses involving personal data. The

¹ **Beladjeraf, S.** (2021). The Authority of the Criminal Judge to Accept and Appreciate Digital Evidence. *Journal of Comparative Legal Studies*, p.p. 675–676.

Convention focuses not only on defining cybercrimes but also on procedural rules that help authorities collect and preserve digital evidence in a lawful way.

One of the most important contributions of the Convention is the introduction of procedural measures adapted to the digital environment. These measures include the rapid preservation of stored data, the lawful access to electronic systems, and the collection of traffic and content data under judicial supervision. Such tools are essential because digital evidence can be easily deleted, altered, or transferred across borders within seconds.

Even though Algeria is not formally bound by the Budapest Convention, its principles have an indirect influence on national legal thinking. Many of the issues addressed by the Convention, such as judicial authorization, proportionality, and international cooperation, are also present in Algerian criminal procedure. Personal data crimes often involve foreign servers, international platforms, or cross-border communications, which makes cooperation between states unavoidable.

The Convention also emphasizes the need to balance effective investigation with the protection of fundamental rights. This balance is particularly important in cases involving personal data, where investigative measures may interfere with privacy and data protection. For Algerian lawmakers and judges, the Budapest Convention offers a useful comparative framework that helps understand international best practices in dealing with digital evidence.¹

3. Fair Trial Guarantees

¹ **Boutemedjet**, Djalal., & **Aliouche**, Kamel..Comparing Algeria's Personal Data Transfer Rules with General Data Protection Regulation. The Journal of Teacher Researcher of Legal and Political Studies,02,2025, p. 936.

International human rights law places fair trial guarantees at the center of criminal justice. These guarantees include the principle of legality, the requirement of proportionality, and the right of defense. They apply to all forms of evidence, including digital evidence, regardless of its technical nature.

In cases involving digital evidence, fair trial guarantees play an even more important role. Digital data can be complex, technical, and difficult to understand for non-specialists. Without proper safeguards, there is a risk that such evidence may be accepted without sufficient scrutiny. This situation could weaken the rights of the accused and affect the balance between the prosecution and the defense.

The right of defense requires that the accused be able to examine digital evidence, challenge its authenticity, and understand how it was collected. This implies transparency in investigative methods and clear documentation of technical procedures. Judges must also be able to assess the reliability of digital evidence without relying blindly on technical experts.

For the Algerian legal system, international fair trial standards reinforce constitutional principles related to due process and judicial protection of rights. They remind courts that digital evidence must not be treated as infallible simply because it appears technical or scientific. Respecting fair trial guarantees strengthens the credibility of criminal justice and ensures that digital evidence serves justice rather than undermines it.¹

¹ **Meguellati**, Sabrine. Hadjer Tebakh. Digital Evidence and its Role in Criminal investigations, faculty of law and political Sciences. University of Bourdj Bouariridj, 2024, p. 58.

Chapter Two:
**Nature and Characteristics of Digital
Evidence.**

Chapter Two:Procedural Regulation of Digital Evidence under Criminal Procedures Law No. 25-14

After studying the conceptual and legal framework of digital evidence in personal data crimes, it is necessary to analyze how this evidence is regulated at the procedural level. Criminal procedure plays a decisive role in determining whether digital evidence can be lawfully collected, preserved, and assessed by the courts.

In Algeria, Criminal Procedures Law No. 25-14 provides the legal framework governing criminal investigations and trials. Although this law was originally designed for traditional crimes, it has gradually been adapted to deal with cybercrime and digital evidence.

Personal data crimes often require intrusive investigative measures, such as searching electronic devices or intercepting digital communications. These measures must be carried out under strict procedural conditions in order to protect individual rights and ensure the admissibility of evidence.

This chapter examines the procedural regulation of digital evidence under Algerian law. It focuses first on investigation and inquiry procedures, and then on how digital evidence is assessed during trial, including the challenges faced by judges and legislators 1

Section One: Investigation and Inquiry Procedures

The investigation stage is the foundation of criminal proceedings. It is during this stage that evidence is discovered, collected, preserved, and documented. In cases involving personal data crimes, the investigation phase is even more important because digital evidence may disappear quickly if not handled correctly.

Digital evidence is fragile, invisible, and technical. For this reason, criminal procedure must provide clear rules that regulate how investigators act when dealing with electronic systems, devices, and digital data. These rules aim to ensure two main objectives: effectiveness of criminal investigation and protection of individual rights.

In Algerian law, Criminal Procedures Law No. 25-14 provides several mechanisms that allow judicial authorities to collect digital evidence. However, these mechanisms must be applied with caution because they often involve intrusion into private life and personal data.

This section examines the powers of judicial authorities during investigation and inquiry, as well as the essential role played by technical expertise in handling digital evidence.¹

Subsection One: Judicial Powers and Collection Procedures

Judicial authorities are responsible for directing and supervising criminal investigations. In digital cases, their role becomes more complex due to the technical nature of evidence and the speed at which data can be altered or destroyed.

The collection of digital evidence requires specific procedural measures, such as searching electronic systems, seizing devices, and intercepting communications. These measures must always be conducted under legal conditions and judicial supervision.

This subsection analyzes the main investigative powers related to digital evidence in personal data crimes.

Sub-branch One: Search and Seizure of Electronic Systems and Devices

1. Legal Basis of Digital Search and Seizure

Search and seizure are traditional investigative measures that aim to discover material elements connected to a criminal offense. In the past, these measures were limited to physical objects such as documents, weapons, or tools used to commit a crime. However, the digital transformation of society has significantly expanded the nature of evidence. Today, criminal activity, especially personal data crimes, often leaves traces in electronic systems rather than in physical spaces.

Under Algerian criminal procedure, Criminal Procedures Law No. 25-14 provides the general legal framework governing search and seizure operations. This law authorizes judicial authorities to seize any object that may contribute to establishing the truth. Electronic devices, such as computers, mobile phones, tablets, servers, and digital storage media, are included within this concept when they contain data related to a criminal offense.

In personal data crimes, electronic devices frequently constitute the primary source of evidence. Emails, databases, browsing histories, digital images, and application data may all contain traces of illegal access, modification, or disclosure of personal information. Treating these devices as objects of proof reflects the necessary adaptation of Algerian criminal procedure to modern forms of crime, while maintaining the principle of legality.

This legal recognition ensures that digital search and seizure are not arbitrary actions but are grounded in clear procedural rules. It also provides a legal basis for judges to assess the admissibility of digital evidence during trial.¹

¹ Abderahmne Khalfi, *op cit*, p.p 330–334.

2. Scope of Digital Search

Digital search differs significantly from traditional physical search due to the nature of electronic data. A digital search is not limited to what is immediately visible on the device. It may extend to internal memory, external storage devices, removable media, and data stored remotely on cloud platforms, provided that such data is accessible through the seized system.

This extended scope reflects the reality of modern data storage. Personal data is often fragmented across multiple locations and platforms, even when accessed through a single device. For example, a smartphone may provide access to email accounts, social media platforms, cloud storage, and professional databases, all of which may contain personal data relevant to an investigation.

However, this wide scope creates serious legal concerns. Digital searches may expose large amounts of personal information that are unrelated to the alleged crime. This includes data belonging to family members, colleagues, or other third parties. Such situations increase the risk of disproportionate interference with private life.

Because digital data is not confined by physical boundaries, investigators must clearly define the limits of their search. The challenge lies in identifying relevant data while avoiding excessive intrusion. This issue is particularly sensitive in personal data crimes, where the protection of private information is a core legal objective.¹

¹ **Masa Galič**, (Defence rights in the context of huge data sets and big data forensic tools in criminal Proceedings), boom strafblad, Amesterdam, 2021, p.p 4–5.

3. Conditions and Guarantees

To ensure legality and protect individual rights, digital search and seizure must respect strict procedural conditions. These conditions are designed to prevent abuse and to guarantee that investigative measures remain under judicial control. One of the most important safeguards is prior judicial authorization, which limits the discretionary power of investigators.

Judicial authorization defines the scope, purpose, and duration of the digital search. It helps ensure that investigative actions are proportionate to the seriousness of the offense. In addition, legal time limits must be respected to prevent prolonged or unjustified interference with private life.

Other procedural guarantees include the proper identification of the devices being searched or seized and, in certain cases, the presence of the suspect or a legal representative. These formalities contribute to transparency and allow later verification of the legality of the operation.

In digital investigations, these guarantees take on increased importance. Because electronic devices often contain intimate and sensitive personal data, any procedural irregularity may result in serious rights violations. Moreover, failure to respect these safeguards may lead to the exclusion or weakening of digital evidence before the court.¹

4. Seizure and Preservation of Digital Evidence

Once electronic devices are seized, preserving the integrity of digital data becomes a central concern. Unlike physical evidence, digital evidence is highly

¹ Ghribi Abdelkader, op cit, p. 153.

fragile. Simple actions, such as turning on a device, updating software, or connecting to a network, may alter or destroy valuable data.

To prevent such risks, investigators apply specific preservation techniques. One common method is the creation of forensic copies, which are exact replicas of the original data. These copies allow experts to analyze the content without modifying the original device. The original data is preserved in a secure condition to ensure its integrity throughout the proceedings.

Preservation also requires careful documentation. Every step taken during seizure, copying, storage, and analysis must be recorded. This documentation helps demonstrate that the evidence has not been altered and allows judicial authorities to verify the reliability of the investigative process.

In the absence of proper preservation measures, digital evidence may lose its probative value. Courts may doubt its authenticity or integrity, which can weaken the prosecution's case and undermine confidence in the judicial process.¹

5. Legal Risks and Challenges

Despite the existence of legal safeguards, digital search and seizure continue to raise important challenges. One of the main risks is the collection of excessive or irrelevant personal data. Because electronic devices centralize many aspects of an individual's life, separating relevant evidence from unrelated private information is often difficult.

This situation creates a constant tension between investigative efficiency and respect for fundamental rights. Investigators may be tempted to collect large

¹ **Bouguerra** Khaled., & Kebaili Mohamed, Requirements for Adapting Algerian Auditing Standards in Collecting Electronic Evidence in the context of the digital operating Environment in Algeria. An Analytical Study on a Sample of Accounting, Experts and External Auditor, Eco research,02,University of Blida, 2025 p. 155.

amounts of data to avoid missing relevant evidence. However, such practices risk violating the principle of proportionality and undermining trust in criminal justice.

In personal data crimes, these risks are even more pronounced. The offense itself concerns protected information, which requires heightened caution during investigative measures. Limiting the scope of digital searches to what is strictly necessary is therefore essential.

Judicial oversight plays a crucial role in addressing these challenges. Judges must ensure that digital searches remain lawful, proportionate, and justified. Respecting these principles strengthens the legitimacy of criminal proceedings and ensures that digital evidence contributes to justice rather than threatening individual freedoms.¹

Sub-branch Two: Interception and Recording of Communications and Digital Data

1. Concept of Interception in the Digital Context

Interception refers to the monitoring and recording of communications, either in real time or after they have been transmitted. In the digital environment, interception may concern emails, instant messages, phone calls, social media communications, or other forms of online exchange. In personal data crimes, such communications often contain important information about illegal access, disclosure, or misuse of personal data.

Unlike traditional investigative measures, interception directly targets private communications. It allows authorities to access information that individuals

⁻¹ **Nadia Lakli,, & Amina Chenaa.,** (Mechanisms for Protecting the Personal Data of the Electronic Consumer in Algerian Law between legal texts and actual application), Journal of Law and Sustainable Development, 02miami,2025, p. 12.

normally expect to remain confidential. For this reason, interception is considered one of the most intrusive tools available in criminal investigations. It interferes not only with private life but also with the secrecy of correspondence.

In Algerian criminal procedure, interception is treated as an exceptional measure. Its use is justified only when other investigative methods are insufficient and when the offense under investigation is serious. This exceptional nature reflects the need to protect fundamental rights while allowing effective investigation of complex digital crimes.¹

2. Legal Conditions for Interception

Because of its intrusive character, interception is subject to strict legal conditions. One essential requirement is prior judicial authorization. This authorization ensures that interception is not carried out arbitrarily and that it serves a legitimate investigative purpose. Judicial control limits the discretion of investigative authorities and provides a legal framework for the measure.

Another important condition relates to the seriousness of the offense. Interception is generally reserved for serious crimes, including complex offenses involving personal data and cybercrime. It cannot be used for minor violations, as this would create a disproportionate interference with individual rights.

The duration of interception must also be limited. Unlimited or prolonged monitoring would amount to constant surveillance, which is incompatible with the principles of legality and proportionality. Clear time limits help ensure that interception remains targeted and justified by investigative needs.

¹ **Abderahmane Khalfi**, op cit, p.p 338–342.

These conditions aim to maintain a balance between effective criminal investigation and respect for fundamental rights guaranteed by both Algerian constitutional principles and international human rights standards.¹

3. Recording and Storage of Intercepted Data

Once communications are intercepted, the way data is recorded and stored becomes crucial. Intercepted digital data must be preserved in a secure and reliable manner to prevent loss, alteration, or unauthorized access. Any technical failure or improper handling may affect the integrity of the evidence.

Secure storage is necessary because digital data is fragile and can be easily modified, intentionally or unintentionally. Proper technical procedures must be applied to ensure that intercepted communications remain identical to the original transmissions. This is especially important when digital evidence is later examined by experts or presented before the court.²

Recording and storage also require careful documentation. Investigators must keep clear records of how the data was collected, stored, and accessed. This transparency allows judicial authorities and the defense to verify the reliability of the evidence and assess whether legal procedures were respected.

Without proper recording and storage, intercepted data may lose its evidentiary value, even if the interception itself was lawfully authorized.³

4. Admissibility of Intercepted Evidence

¹ Ghribi Abdelkader, op cit, p. 154.

² Bouguerra, K., & Kebaili, M. op cit p. 157.

³ Eoghan Casey, op cit, p. 320

The admissibility of intercepted communications depends primarily on respect for legal conditions. If interception is conducted without proper authorization, outside the legal scope, or in violation of procedural guarantees, the resulting evidence may be excluded or given reduced probative value.

Judges play a central role in assessing the legality of interception measures. They must verify whether authorization was granted, whether the duration was respected, and whether the interception remained within the limits defined by law. Any irregularity may cast doubt on the legitimacy of the evidence.

In digital cases, unlawful interception may also undermine confidence in the criminal justice system. The exclusion of illegally obtained evidence serves as a reminder that respect for rights is not optional, even in the fight against serious crime.

For this reason, strict legality is a key condition for the admissibility of intercepted digital evidence in Algerian criminal proceedings.

5. Balance between Investigation and Privacy

Interception can be a powerful investigative tool, especially in complex personal data crimes. However, its use must remain exceptional. Transforming interception into a routine practice would risk creating a system of generalized surveillance incompatible with democratic values.

The challenge lies in finding a balance between the needs of criminal investigation and the protection of privacy. While authorities must be able to investigate serious offenses effectively, individuals must also be protected against excessive intrusion into their private communications.

In the digital age, where communication is constant and diverse, the risk of overuse of interception is real. For this reason, legal systems must remain vigilant and ensure that intrusive measures are justified, limited, and strictly controlled.

Respecting this balance strengthens the legitimacy of criminal justice and preserves public trust, especially in cases involving sensitive personal data.¹

Subsection Two: Role of Technical Expertise

Digital evidence cannot be understood or evaluated without technical knowledge. For this reason, technical experts play a central role in digital investigations.

Experts assist judicial authorities in extracting, analyzing, and documenting digital data. However, reliance on expertise also raises legal and procedural questions.

This subsection examines the importance of technical experts and the challenges related to authenticity and attribution of digital evidence.

Sub-branch One: Importance of Technical Experts in Extraction and Documentation

1. Role of Technical Experts

In modern criminal investigations, especially those involving digital evidence, technical experts play an essential role. Digital evidence does not exist in a visible or physical form like traditional evidence. It is stored in electronic systems, often hidden within complex software, databases, or encrypted devices. Because of this technical nature, judicial authorities cannot access or interpret such data without specialized assistance.

¹Kadri, S., & Abbar, O. op cit p. 238

Technical experts are responsible for extracting digital data from electronic devices such as computers, mobile phones, tablets, servers, and external storage media. This extraction must be carried out carefully, using appropriate forensic tools and methods. Any mistake during extraction may result in the loss, alteration, or contamination of data, which could seriously affect the reliability of the evidence.

Beyond extraction, experts analyze electronic systems to identify relevant digital traces. These traces may include access logs, metadata, timestamps, deleted files, communication records, or system activity histories. In personal data crimes, such traces are often decisive in proving illegal access, unlawful modification, or unauthorized disclosure of personal information.

Another crucial task of technical experts is the preparation of expert reports. These reports present technical findings in a structured and understandable way for judges, prosecutors, and lawyers. Since legal professionals are not usually trained in computer science, expert reports translate complex technical operations into legal facts that can be discussed during judicial proceedings. Without this mediation, digital evidence would remain inaccessible and unusable in court.¹

2. Legal Framework of Expertise

The intervention of technical experts is governed by a legal framework that aims to ensure fairness, neutrality, and respect for procedural rules. In Algerian criminal procedure, experts are appointed by judicial authorities and act under their supervision. This appointment gives expertise an official and regulated character, distinguishing it from private or informal technical opinions.

¹ Bouguerra, K., & Kebaili, M. op cit p.p. 150–151.

Experts are required to act independently and objectively. Their mission is not to support the prosecution or the defense, but to provide a neutral technical assessment of the facts. This neutrality is particularly important in digital cases, where technical conclusions may strongly influence the judge's personal conviction.

The legal framework also defines the limits of the expert's mission. Experts must restrict their work to the questions formulated by the judicial authority and avoid exploring data unrelated to the case. This limitation is essential in personal data crimes, where electronic devices often contain sensitive information unrelated to the alleged offense.

By imposing rules on appointment, mission scope, and neutrality, the legal framework ensures that technical expertise serves the search for truth without violating individual rights. Respect for these rules strengthens the credibility of expert findings and reinforces trust in digital evidence presented before the court.¹

3. Documentation of Technical Operations

Documentation is a fundamental element of technical expertise in digital investigations. Because digital operations are invisible and highly technical, every step taken by the expert must be clearly recorded. This includes the methods used to access devices, the tools employed for extraction, and the procedures followed during analysis.

Proper documentation allows judicial authorities to understand how digital evidence was obtained and to verify that legal and technical standards were respected. It also enables the defense to examine the expert's work and raise

¹Abderahmane Khalfi., *op cit*, p.p 344-347.

challenges if irregularities are suspected. Without detailed documentation, it becomes difficult to assess whether the evidence has been handled correctly.

In digital investigations, documentation also helps protect the integrity of the evidence. Recording each operation creates a traceable history of how data was handled, which reduces the risk of manipulation or accidental alteration. This traceability is essential when disputes arise regarding the authenticity or reliability of digital evidence.

Furthermore, documentation contributes to transparency in criminal proceedings. It reassures all parties that technical expertise was conducted professionally and lawfully. In personal data crimes, where the protection of privacy is a central concern, transparent documentation plays a key role in maintaining procedural fairness and judicial confidence.¹

Sub-branch Two: Challenges of Authenticity and Attribution

1. Authenticity of Digital Evidence

Authenticity is one of the most important challenges related to digital evidence. It refers to the question of whether digital data is genuine and whether it has remained unchanged from the moment it was created until it is presented before the court. In criminal proceedings, especially those involving personal data crimes, the value of digital evidence depends largely on its authenticity.

Digital evidence is particularly vulnerable to alteration. Data can be modified, deleted, copied, or fabricated using simple technical tools. Even unintentional actions, such as opening a file or connecting a device to the internet, may change

⁻¹ Bouguerra, K., & Kebaili, M. op cit p. 155.

metadata or system information. This fragility creates constant doubts about whether the evidence truly reflects the original facts.

Because of these risks, courts must be careful when assessing digital evidence. The authenticity of data must be supported by technical guarantees, such as proper preservation, documentation, and forensic methods. Without these safeguards, digital evidence may lose its credibility and fail to convince the judge.

In personal data crimes, where the offense itself concerns protected information, ensuring authenticity is even more important. Any doubt regarding alteration may undermine the entire evidentiary process.¹

2. Attribution of Evidence to the Accused

Attribution refers to the process of linking digital evidence to a specific individual. In criminal law, it is not enough to prove that illegal digital activity occurred; it must also be shown that the accused person is responsible for that activity. In the digital environment, this task is often complex.

Many technical factors complicate attribution. Devices may be shared by several users, such as family members or colleagues. Internet connections may be accessed by multiple, and IP addresses do not always identify a single individual. In addition, anonymous accounts, false identities, and virtual private networks make it difficult to associate digital actions with a specific person.

In personal data crimes, attribution problems are frequent. Unauthorized access or disclosure may be carried out remotely, automatically, or using stolen credentials. This creates uncertainty about who actually performed the illegal act.

¹ **Abdullah, H. O., Maqsood, M., & Nadeem, A.** (Digital Evidence in Criminal Proceedings: Legal Standards, Chain of Custody, and Evidentiary Reliability in The Digital Era), *Research Journal for Social Affairs, Pakistan*, 2025, p.p. 800–801.

As a result, digital evidence must be supported by additional elements, such as usage patterns, timestamps, or contextual information.

Because attribution is uncertain, judges must carefully examine the link between the evidence and the accused. Weak or indirect attribution may not be sufficient to establish criminal responsibility.¹

3. Legal Consequences of Uncertainty

When doubts arise regarding the authenticity or attribution of digital evidence, important legal consequences follow. Criminal law is based on the principle that guilt must be proven with certainty. If evidence is unreliable or ambiguous, it cannot serve as a solid basis for conviction.

In Algerian criminal procedure, uncertainty benefits the accused. If the judge is not convinced that digital evidence is authentic or that it can be clearly attributed to the accused, the evidence must be interpreted with caution. This principle protects individuals from wrongful conviction based on fragile or doubtful proof.²

Uncertainty may result in reduced evidentiary value or even exclusion of digital evidence. This encourages investigators and experts to respect technical and procedural safeguards during collection and analysis. It also reinforces the importance of legality and proper documentation.

In cases involving personal data crimes, respecting this principle is essential to maintain fairness. Digital evidence should support justice, not replace careful judicial reasoning. Doubt remains a fundamental protection within criminal proceedings.³

¹ Galič Masa. Op cit, p. 8.

² Brenner susan. Op cit, p. 38.

³ Abderahmane Khalfi, *op cit*, p.p 348–350.

Section Two: Trial Assessment and Procedural Challenges

The trial stage represents the final and most sensitive phase of criminal proceedings. It is during this stage that the judge examines the evidence collected during the investigation and decides on the criminal responsibility of the accused. In cases involving personal data crimes, the trial stage is often complex because digital evidence plays a central role.

Digital evidence is rarely self-explanatory. It usually requires interpretation through expert reports and technical explanations. This situation creates difficulties for judges, lawyers, and defendants, especially when the case involves sensitive personal data and complex digital systems.

In Algerian criminal law, the judge enjoys freedom of assessment based on personal conviction. However, this freedom must be exercised within the limits of legality, procedural fairness, and respect for the rights of defense. Digital evidence challenges these principles because of its technical nature and potential impact on privacy.

This section studies how digital evidence is assessed during trial and analyzes the main procedural challenges raised by its use. It also discusses the need for legislative development and alignment with international standards.

Subsection One: Evidentiary Value of Digital Evidence at Trial

The evidentiary value of digital evidence depends on several factors, including legality, authenticity, reliability, and the manner in which it is presented before the court. Unlike traditional evidence, digital evidence is not directly observable and must often be explained by technical experts.

In personal data crimes, digital evidence is often decisive. However, its evaluation requires careful judicial reasoning to avoid injustice. This subsection examines how digital evidence is presented and discussed during trial and how the rights of defense and the judge's personal conviction are protected.

Sub-branch One: Presentation and Discussion of Digital Evidence before the Judiciary

1. Forms of Digital Evidence Presented at Trial

During criminal trials involving personal data crimes, digital evidence may be presented before the court in various forms. These forms are adapted to the technical nature of digital data and to the practical needs of judicial proceedings. Common examples include expert reports, printed documents derived from electronic files, screenshots, system logs, and audio or video recordings.¹

In practice, judges rarely deal directly with raw digital data, such as original databases or complete system files. Raw data is often too complex and technical to be examined in its original form during a public hearing. Instead, digital evidence is presented through summarized, structured, and interpreted materials that highlight the elements relevant to the case.

This method of presentation allows the court to focus on the legal meaning of the evidence rather than its technical complexity. However, it also means that judges depend heavily on interpretation, especially when digital evidence is filtered or explained by experts. For this reason, the way digital evidence is presented plays a decisive role in shaping judicial understanding and assessment.²

⁻¹ Bouguerra, K., & Kebaili, M. op cit p. 160.

⁻² Galič, Masa. op cit, p. 9.

2. Role of Expert Reports in Judicial Understanding

Expert reports are central to the presentation of digital evidence before the judiciary. These reports translate technical findings into clear and accessible language that can be understood by judges, prosecutors, and defense lawyers. Without such reports, most digital evidence would remain incomprehensible to legal professionals.

Expert reports explain how data was extracted, what methods were used, and what conclusions can be drawn from the analysis. In cases involving personal data crimes, experts often clarify issues such as unauthorized access, data modification, or illegal disclosure. Their work helps the court understand the technical context of the offense.

However, expert reports do not bind the judge. Judicial authority remains responsible for assessing the evidentiary value of expert conclusions. The judge must examine whether the expert's reasoning is logical, whether procedures were respected, and whether the conclusions are supported by the facts. Blind reliance on expertise may weaken judicial independence and undermine the principle of free evaluation of evidence.¹

3. Principle of Contradiction

The principle of contradiction is a fundamental rule of criminal procedure. It requires that all evidence presented before the court be discussed openly and fairly by both parties. Digital evidence is no exception to this rule, even when it is highly technical or complex.

¹ Ghribi Abdelkader, op cit, p. 159.

Both the prosecution and the defense must have access to expert reports, technical documents, and any other materials related to digital evidence. This +access allows the defense to examine the methods used, question the reliability of the data, and raise objections if irregularities are suspected.

The discussion of digital evidence during trial ensures procedural fairness and equality of arms. It allows the judge to hear different interpretations of the same technical facts and to form a balanced opinion. Without contradiction, digital evidence may appear unquestionable, which risks undermining the rights of the accused.¹

4. Public Debate and Transparency

Public discussion of evidence is an essential element of criminal justice. It strengthens the legitimacy of judicial decisions and reinforces public confidence in the courts. Even in cases involving technical digital evidence, explanations must be provided in a clear and understandable manner.

Transparency requires that the reasoning behind judicial decisions be visible and comprehensible. When digital evidence plays a central role in a conviction, the court must explain how it was evaluated and why it was considered reliable. This clarity is important not only for the parties but also for appellate courts reviewing the decision.

In personal data crimes, transparency helps demonstrate that intrusive investigative measures were justified and lawfully used. It also shows that digital

⁻¹ Galič Masa, op cit, p. 6

evidence was not accepted blindly but carefully examined within the framework of legal safeguards.¹

5. Risk of Overvaluation of Digital Evidence

Digital evidence often appears precise, objective, and scientific. This appearance may lead to its overvaluation during trial. Judges and jurors may be tempted to give greater weight to digital traces than to other forms of evidence, assuming that technology is neutral and infallible.

In reality, digital evidence is not immune to error or misinterpretation. Technical data may have several explanations, and digital traces do not always clearly reflect human intent. Errors in collection, analysis, or interpretation may affect the reliability of digital proof.

Overvaluation of digital evidence creates the risk of unjust conclusions, especially when other elements of the case are weak. Courts must therefore approach digital evidence with caution and maintain a critical perspective. Treating digital evidence as one element among others helps preserve balanced judicial reasoning and protects against technological illusion.²

Sub-branch Two: Guarantees of the Right of Defense and the Judge's Personal Conviction

1. Right of Defense in Digital Cases

¹ Kadri, S., & Abbar, O. op cit, p.p. 245–246

² Galič Masa, op cit, p. 10.

The right of defense is one of the most important principles of criminal procedure. It guarantees that the accused can know the evidence used against them, examine it, challenge its validity, and present arguments in response. This right applies at all stages of criminal proceedings, including investigation and trial.

In cases involving digital evidence, exercising the right of defense may become more difficult. Digital evidence is often technical, complex, and based on specialized methods that are not easily understood without technical knowledge. Defense lawyers may face challenges in accessing digital files, understanding forensic reports, or verifying how data was extracted and analyzed.

Despite these difficulties, the right of defense applies fully to digital cases. The accused must be able to examine digital evidence under conditions that allow effective defense. This includes access to expert reports, technical documentation, and procedural records related to the collection and handling of digital data.

Ensuring effective defense in digital cases helps maintain procedural fairness and prevents convictions based on evidence that cannot be properly challenged.¹

2. Right to Counter-Expertise

To guarantee equality of arms between the prosecution and the defense, criminal procedure allows the defense to request counter-expertise. This right is particularly important in cases involving digital evidence, where expert opinions often play a decisive role.

Counter-expertise allows the defense to verify the methods used during data extraction and analysis. It also makes it possible to identify technical errors,

¹ **Abderahmane Khalfi**, op cit, p.p 367-371.

procedural irregularities, or alternative interpretations of the same digital traces. This process helps avoid one-sided technical conclusions dominating the trial.

In digital cases, counter-expertise contributes to transparency and fairness. It ensures that expert reports are not accepted automatically and that technical findings are open to discussion. Allowing counter-expertise strengthens confidence in the judicial process and protects the rights of the accused.

Without this possibility, digital evidence could become unchallengeable, which would contradict the basic principles of criminal justice.¹

3. Judge's Personal Conviction

In Algerian criminal law, the judge decides cases based on personal conviction. This principle means that the judge is free to assess the value of evidence, without being bound by rigid rules of proof. Personal conviction applies equally to traditional and digital evidence.

However, personal conviction is not arbitrary. It must be formed through lawful evidence that has been properly collected, presented, and debated during trial. In digital cases, this requirement is particularly important because of the technical nature of the evidence.

The judge must be able to understand the meaning and limits of digital evidence. Expert reports assist in this task, but they do not replace judicial reasoning. Personal conviction must remain rational, reasoned, and based on clear explanations that connect technical facts to legal conclusions.

⁻¹ **Friedrich cyrielle**, (Science and Technology as Means of Evidence in Criminal Procedure), PhD Thesis, University of Geneva, 2013, p. 340.

This approach preserves judicial independence while ensuring that decisions are grounded in evidence that respects procedural guarantees.¹

4. Presumption of Innocence and Doubt

The presumption of innocence is a fundamental principle of criminal law. It requires that any doubt regarding guilt must benefit the accused. This principle applies fully to cases involving digital evidence.

When doubts exist concerning the authenticity of digital data or its attribution to the accused, the evidentiary value of such data is weakened. Digital evidence may appear precise, but it is not immune to uncertainty, technical error, or misinterpretation.

In these situations, judges must exercise caution and avoid basing convictions on fragile or ambiguous proof. Respecting doubt protects individuals from wrongful convictions and reinforces confidence in the justice system.

In personal data crimes, where evidence is often technical and indirect, the presumption of innocence remains a crucial safeguard against excessive reliance on digital traces.²

Subsection Two: Procedural Challenges and Legislative Solutions

Despite legal progress, the use of digital evidence in Algerian criminal procedure raises several challenges. Traditional procedural rules were designed for physical evidence and are not always suitable for digital realities.

⁻¹ Kadri, S., & Abbar, O. op cit, p.p. 235–236.

⁻² Brenner Susan, op cit, p. 205.

This subsection identifies the main procedural difficulties and proposes legislative reforms inspired by doctrine and international standards.

Sub-branch One: Integration of procedural provisions within incriminating legal texts

1. Absence of a Clear Legal Category

One of the main difficulties with digital evidence is that it does not fit clearly within traditional categories of criminal evidence. Classical criminal procedure usually distinguishes between written evidence, material evidence, and testimonial evidence. Digital evidence does not fully correspond to any of these categories. It is not purely material because data itself is intangible, and it is not purely written because it exists through electronic systems and technical processes. This lack of classification creates uncertainty when judges must decide how digital evidence should be treated and evaluated during criminal proceedings. In Algerian criminal procedure, the legal classification of evidence plays an important role in determining its admissibility and evidentiary value, which makes this issue particularly sensitive in digital cases.¹

2. Consequences for Judicial Consistency

The absence of a clear legal category for digital evidence has direct consequences for judicial consistency. When the law does not clearly define the nature of digital proof, courts may adopt different approaches in similar cases. Some judges may treat digital data as written evidence, while others may consider it technical or material evidence. This diversity of approaches can lead to inconsistent judicial decisions and unpredictable outcomes. Such inconsistency weakens legal certainty and makes it more difficult for parties to anticipate how digital evidence

¹ Eoghan Casey, op cit, p. 38.

will be assessed. Comparative criminal law also shows that traditional evidentiary systems face similar difficulties when integrating technological proof into existing legal frameworks.¹

3. Need for Legislative Clarification

Because of these difficulties, many legal scholars argue that legislative clarification is necessary. Explicitly defining digital evidence in Algerian criminal procedure would help determine its legal nature and clarify the rules governing its collection, examination, and evaluation. Clear regulation would also reduce judicial uncertainty and provide investigators and judges with a stable legal framework. In cases involving personal data crimes, where digital traces often play a decisive role, the absence of clear rules may affect both the effectiveness of prosecution and the protection of individual rights. Legislative intervention would therefore contribute to legal certainty and procedural fairness.

4. Impact on the Rights of the Parties

The difficulty of classifying digital evidence also affects the rights of the parties, especially the right of defense. When the legal nature of evidence is unclear, the defense may face challenges in determining how to contest its admissibility or probative value. Clear classification would allow the defense to better understand the applicable procedural rules and prepare effective arguments. At the same time, it would help judges justify their decisions more clearly and transparently. Adapting traditional evidence systems to digital realities is therefore necessary to ensure fairness and maintain trust in the criminal justice system.²

¹ Friedrich Cyrielle, op cit, p. 88.

² Abderahmane khalfi, op cit, p.p 374-376.

Sub-branch Two: Integration of procedural provisions within incriminating legal texts

With the emergence of complex forms of offences requiring specific procedural mechanisms, the current legislative trend consists in incorporating procedural aspects within incriminating legal provisions. This approach enables the establishment of procedures specifically related to the administration and collection of digital evidence.¹

The criminal legislation is generally based on two categories of legal norms: substantive legal texts, which include incriminating provisions, the definition of the offence, its constituent elements, and the prescribed penalties; and procedural legal texts, which govern criminal proceedings proper. Traditionally, the application of these legal norms did not raise significant difficulties, particularly with regard to the administration of evidence.²

However, with the emergence of new forms of criminality, especially those related to information and communication technologies, it became evident that traditional procedures for the administration of evidence were no longer adequate. One of the main challenges lies in the intangible and volatile nature of digital evidence, which can be easily altered, deleted, or remotely accessed, thereby requiring highly technical investigative tools and accelerated preservation mechanisms.³

In this context, legal systems have progressively moved toward the development of hybrid legislative techniques, whereby substantive criminal law increasingly integrates procedural safeguards. This evolution reflects a functional approach to criminal law, aiming not only to define offences but also to ensure their effective prosecution in digital environments, particularly through measures such as data

retention orders, electronic surveillance, and cross-border cooperation in electronic evidence gathering.⁴

This legislative tendency has been adopted by the Algerian legislator through several recently enacted criminal laws, particularly those relating to the protection of personal data and the prevention of technology-related offences. Through this approach, the legislator seeks to remedy the shortcomings of traditional evidentiary procedures by introducing legal provisions adapted to emerging forms of crime and digital evidence.⁵

- *Convention on Cybercrime (Budapest Convention)*, 2001, Council of Europe, arts. 14–21

— ² **Jean Pradel**, *Procédure pénale*, 19th ed., Cujas, Paris, 2017, p.p. 45–52.

— ³ **Olivier Leclerc, Étienne Vergès & Géraldine Vial**, (Scientific and Technological Evidence)”, *open science, France, 2020*, , p.p. 3–9.

— ⁴ **Mireille Delmas-Marty**, *Le flou du droit : du code pénal aux droits de l’homme*, PUF, Paris, 2004, p.p. 112–118.

— ⁵ Law No. 09-04 of specific rules on the prevention and fight against information technologies and communication’s crimes, of 16 aout 2009, Official Gazette of the People’s Democratic Republic of Algeria No47 .

Conclusion

Conclusion

This research focused on the role of digital evidence in personal data crimes under Algerian law. It started from the observation that the rapid development of technology has changed the way crimes are committed and, at the same time, the way criminal proof is produced and evaluated.

Today, many personal data crimes take place in digital environments. These crimes are often committed without physical contact and do not leave traditional traces. Because of this reality, digital evidence has become essential in criminal investigations and trials. In many cases, it is the only way to identify offenders and establish criminal responsibility.

The first chapter showed that digital evidence has a specific legal nature. It is intangible, fragile, easy to alter, and highly technical. These characteristics clearly separate it from traditional forms of evidence and explain why general procedural rules are sometimes insufficient. The chapter also highlighted that personal data enjoys legal protection in Algerian law, especially through Law No. 18-07 and the intervention of the ANPDP, which plays an important preventive and supervisory role.

The second chapter examined the procedural treatment of digital evidence under Criminal Procedures Law No. 25-14. It showed that investigative measures such as digital search, seizure, interception of communications, and technical expertise are necessary to fight personal data crimes. However, these measures are also highly intrusive. For this reason, they must always be carried out within a strict legal framework that respects judicial authorization, proportionality, and individual rights.

At the trial stage, the research identified several important challenges. Judges often rely on expert reports to understand digital evidence, which may create a

risk of excessive dependence on technical analysis. While the judge's personal conviction remains the foundation of criminal justice, it must be based on lawful, transparent, and clearly explained evidence. In this context, the right of defense and equality of arms remain essential guarantees, especially in complex digital cases.

The study also showed that Algerian criminal procedure still lacks clear and explicit rules specifically dedicated to digital evidence. The difficulty of classifying digital evidence within traditional evidentiary systems creates legal uncertainty and may affect judicial consistency. International standards, such as the Budapest Convention and the GDPR, offer useful guidance that can help inspire future legislative reforms without ignoring national legal principles.

In conclusion, digital evidence has become unavoidable in the fight against personal data crimes. However, its use must always be balanced with the protection of fundamental rights, particularly privacy and the right to a fair trial. Algerian law is therefore called upon to continue evolving by clarifying procedural rules, improving judicial and technical training, and strengthening cooperation between judicial and administrative authorities. Only a balanced and cautious approach can ensure both effective criminal justice and real protection of personal data.

Results :

- Digital evidence has become an essential element in combating personal data crimes, given that these offenses are closely linked to the digital environment and rely on electronic means.

- Digital evidence is characterized by a specific nature that distinguishes it from traditional forms of evidence, as it is intangible, fragile, easily alterable, and dependent on advanced technologies, which necessitates a special legal and procedural treatment.

-The Algerian legislator has established legal protection for personal data through specific legal provisions, most notably Law No. 25-11, while assigning a significant role to the National Authority for the Protection of Personal Data.

-The National Authority for the Protection of Personal Data plays a central role in ensuring compliance with data protection rules through its preventive and supervisory functions.

-Criminal Procedure Law No. 25-14 regulates the procedures for collecting digital evidence through mechanisms such as digital searches, seizure, and interception of communications; however, these measures require strict compliance with legal safeguards.

-The collection of digital evidence is subject to a set of legal constraints, primarily the principle of legality, the necessity of prior judicial authorization, and respect for the principle of proportionality, all of which aim to protect fundamental rights and freedoms.

-Technical expertise plays a pivotal role in interpreting digital evidence; however, excessive reliance on it may affect the judge's independence in forming their conviction.

-The judge enjoys discretionary power in assessing digital evidence, yet this power remains limited by the requirement to respect legality and the credibility of the evidence.

Recommendations :

In light of the findings reached, a set of recommendations can be proposed to enhance the effectiveness of digital evidence in personal data crimes, as follows:

Updating the legislative framework in line with the rapid development of digital technologies, through the introduction of more precise and clear legal provisions regulating digital evidence and its procedures.

Strengthening specialized training for judges and judicial police officers in the field of digital evidence, in order to enable them to better understand its technical aspects.

Providing adequate technological resources to judicial police officers and agents of the National Authority for the Protection of Personal Data, in order to assist them in tasks related to investigation, inspection, and inquiry into cybercrimes.

Reducing excessive reliance on technical expertise by equipping judges with the necessary knowledge and technical tools to understand and independently assess digital evidence.

Enhancing international cooperation in combating cybercrime, particularly with regard to the exchange of digital evidence and mutual legal assistance.

List of References

List of references:

- _ Constitution of the People's Democratic Republic of Algeria. (2020).
- _ *Convention on Cybercrime (Budapest Convention)*, 2001, Council of Europe, arts. 14–21.
- _ Abderahmane khalfi, *algerian criminal procedures*, 8 ed, Dar belkis, Algiers, 2025.
- _ Brenner susan, *Cybercrime and the Law: Challenges, Issues, and Outcomes*, Northeastern University Press, 2012.
- _ Eoghan Casey, *Digital Evidence and Computer Crime*, forensic science, computers and the internet, 3ed, amesterdam, 2011.
- _ Jean Pradel, *Procédure pénale*, 19th ed., Cujas, Paris, 2017.
- _ Lotfi, K. H. A. *Digital evidence and its role in proving information technology crimes*. Dar El Fikr Al Jamia'I, 2019.
- _ _ Friedrich cyrielle, *(Science and Technology as Means of Evidence in Criminal Procedure)*, PhD Thesis, University of Geneva, 2013.
- _ _ Meguellati, Sabrina. Hadjer Tebakh. *Digital Evidence and its Role in Criminal investigations*, master's, faculty of law and political Sciences. University of Bourdj Bouariridj, 2024.

- _ Abdullah, H. O., Maqsood, M., & Nadeem, A. (Digital Evidence in Criminal Proceedings: Legal Standards, Chain of Custody, and Evidentiary Reliability in The Digital Era), *Research Journal for Social Affairs*, Pakistan, 2025
- _ Beladjeraf, S. (2021). The authority of the criminal judge to accept and appreciate digital evidence. *Journal of Comparative Legal Studies*.
- _ Bourtal Amina, (Proving Electronic Crime With Digital Evidence According to Algerian Legislation), *Algerian Journal of Legal and Political Sciences*, 01, university of ain temouchent, 2026.
- _ Boutemedjet, Djalal., & Aliouche, Kamel..Comparing Algeria's Personal Data Transfer Rules with General Data Protection Regulation. *The Journal of Teacher Researcher of Legal and Political Studies*, 02, 2025, p. 936.
- _ Bouguerra, K., & Kebaili, M. Requirements for Adapting Algerian Auditing Standards in Collecting Electronic Evidence in the context of the digital operating Environment in Algeria. *An Analytical Study on a Sample of Accounting, Experts and External Auditor*, Eco research, 02, University of Blida, 2025.
- _ Masa Galič, (Defence rights in the context of huge data sets and big data forensic tools in criminal Proceedings), *boom strafblad*, Amsterdam, 2021.
- _ Ghribi abdelkader, (Legal Value of Forensic Digital Evidence : Between the Requirements of the Legal Text and _the Demands of the Digital Environment), *journal of legal and economic research*, 02, research center for Islamic sciences and civilization, laghouat, Algeria, 2025.
- _ Olivier Leclerc, Étienne Vergès & Géraldine Vial, (Scientific and Technological

Evidence)”, *open science,France,2020*.

_Kadri Saoucen., & Abbar Omar, (Digital evidence between a personal conviction of the criminal judge and Supreme Court control),*Algerian Journal of comparative public law, 01university of belabes , 2024*.

_ Nadia Lakli., & Amina Chenaa., (Mechanisms for Protecting the Personal Data of the Electronic Consumer in Algerian Law between legal texts and actual application), *Journal of Law and Sustainable Development, 02miami,2025*.

-Titouche, Radia. The territorial principal of criminal law and cybercrime, voice of Law Magazine 02, University of tizi ouazou ,2018 .

—

_ Meguellati, S. *Digital evidence and its role in criminal proof* (Master's thesis, University of Mohamed El Bachir El Ibrahimi), 2024

_ Mostefaoui Abdelkader, (La protection de la vie privée à l'épreuve de l'extension des pouvoirs d'enquête), *Journal of Law and Human Sciences*, 2, algeries, 2021.

_ Titouche, R, Territorialité du droit pénal et cybercriminalité. *Review of the Voice of Law* , 2018.

_ Law No. 25-11 relating to the protection of individuals in the processing of personal data of 10 july 2025, Official Gazette of the People's Democratic Republic of Algeria No48 .

_ Law No 25-14 amending the code of criminal procedures, on August 13, 2025 Official Gazette of people's democratic of Algeria, No. 54 .

_ Law No. 09-04 of specific rules on the prevention and fight against information technologies and communication's crimes, of 16 aout 2009, Official Gazette of the People's Democratic Republic of Algeria.

Table of Contents

Introduction	2
CHAPTER ONE: Conceptual and Legal Framework of Digital	
Evidence in Personal Data Crimes	7
Section One: Nature and Characteristics of Digital Evidence	8
Subsection One: Concept and Characteristics of Digital Evidence	9
Sub-branch One: Definition (Linguistic, Legal, and Doctrinal)	9
Sub-branch Two: Distinctive Features of Digital Evidence	16
Subsection Two: Application of Digital Evidence in	
Personal Data Crimes.....	21
Sub-branch One: Concept of Personal Data and	
Scope of Legal Protection	21
Sub-branch Two: Major Types of Personal Data Crimes	
(Hacking, Espionage, Unlawful Modification, Disclosure)	27
Section Two: Principles and Legal Controls Governing	
Digital Evidence	31
Subsection One: Principle of Legality and	
Procedural Admissibility.....	31
Sub-branch One: Importance of Legality in Criminal Evidence	32
Sub-branch Two: Legal Controls for Collecting Digital Evidence.....	36
Subsection Two: Role of Supervisory Authorities and	
International Standards	39

Sub-branch One: Powers of the ANPDP and Its Procedural Role.....	39
Sub-branch Two: Influence of International Standards.....	43
CHAPTER TWO: Procedural Regulation of Digital Evidence	
Under Criminal Procedures Law No. 25-14	47
Section One: Investigation and Inquiry Procedures	48
Subsection One: Judicial Powers and Collection Procedures.....	49
Sub-branch One: Search and Seizure of Electronic Systems and Devices	49
Sub-branch Two: Interception and Recording of Communications and Digital Data	54
Subsection Two: Role of Technical Expertise	58
Sub-branch One: Importance of Technical Experts in Extraction and Documentation.....	58
Sub-branch Two: Challenges of Authenticity and Attribution.....	61
Section Two: Trial Assessment and Procedural Challenges	64
Subsection One: Evidentiary Value of Digital Evidence at Trial.....	64
Sub-branch One: Presentation and Discussion of Digital Evidence before the Judiciary	65
Sub-branch Two: Guarantees of the Right of Defense and The Judge's Personal Conviction.....	68
Subsection Two: Procedural Challenges and Legislative solutions	71

Sub-branch One: Difficulty of Classifying Digital Evidence

Within Traditional Evidence Systems 72

Sub-branch Two: Integration of procedural provisions within incriminating legal texts..... 74

Conclusion..... 79

List of References 81