# TSUL LEGAL REPORT

INTERNATIONAL ELECTRONIC SCIENTIFIC JOURNAL

VOLUME 7
ISSUE 2
JUNE 2026

JOURNAL DOI: 10.51788/tsul.lr.
ISSUE DOI: 10.51788/tsul.lr.7.2.
E-ISSN: 2181-1024

Google Scholar doi Crossref Content Registration

**Founder: Tashkent State University of Law**

TSUL LEGAL REPORT
T L R

INTERNATIONAL
ELECTRONIC SCIENTIFIC JOURNAL

VOLUME 7
ISSUE 2
JUNE 2026

JOURNAL DOI: 10.51788/tsul.lr.
ISSUE DOI: 10.51788/tsul.lr.7.2.

«TSUL Legal Report» international electronic scientific journal was registered by the Press and Information Agency of Uzbekistan on April 21, 2020, with certificate number 1342.The journal is included in the list of journals of the Higher Attestation Commission under the Ministry of Higher Education, Science and Innovations of the Republic of Uzbekistan.


**Publication Officer:**
Orifjon Choriev

**Editor:**
Elyor Mustafaev

**Graphic designer:**
Umid Sapaev

**Editorial office address:**
Tashkent, st. Sayilgoh, 35. Index 100047.
Principal Contact

**Tel.:** (+998 71) 233-66-36

**Fax:** (+99871) 233-37-48

**Website:** legalreport.tsul.uz

**E-mail:** info@legalreport.tsul.uz

**Publishing license**
№ 174625, 29.11.2023.

**E-ISSN: 2181-1024**

# CONTENTS

## 12.00.10 – INTERNATIONAL LAW



## 12.00.13 – HUMAN RIGHTS



## 12.00.14 – CRIME PREVENTION. ENSURING PUBLIC SAFETY. PROBATION ACTIVITY

TSUL LEGAL REPORT

Journal home page: www.legalreport.tsul.uz

TSUL LEGAL REPORT T I R

Received: 07.05.2026 Accepted: 15.06.2026 Published: 30.06.2026

**DOI: https://dx.doi.org/10.51788/tsul.lr.7.2./YFYT2774**

# SCIENTIFIC-THEORETICAL ISSUES OF ELECTRONIC EVIDENCE IN INVESTIGATING CYBERBULLYING CRIMES

**Tulanboeva Adiba Alijon kizi**,
Lecturer of the Department of Judiciary,
Advocacy and Law Enforcement Agencies,
Tashkent State University of Law
ORCID: https://orcid.org/0009-0003-4159-8117
e-mail: adibatulanboyeva@gmail.com

***Abstract.*** *This article analyzes the scientific and theoretical aspects of electronic evidence in the investigation of cyberbullying crimes. It covers the concept of cyberbullying, its manifestations in the modern digital environment, and the role of electronic evidence in identifying and proving this type of crime. It also examines the specific characteristics of electronic evidence, problems that arise in the process of collecting, storing, and evaluating it. During the study, the main types of electronic evidence encountered in cyberbullying-related crimes are identified and their importance in the investigation process is justified. Practical problems that arise when working with electronic evidence are analyzed and the theoretical foundations for their elimination are highlighted. The results of this study serve to further understand the role and importance of electronic evidence in the effective investigation of cyberbullying crimes.*

***Keywords:*** *cyberbullying, electronic evidence, digital forensics, investigative process, social media, IP address, metadata, log files, cybercrime, evidence evaluation*

## Introduction

In the current era of globalization and the rapid development of digital technologies, almost all spheres of social life are closely connected with the Internet and information and communication technologies. Digital technologies, the World Wide Web, and the artificial intelligence network are developing rapidly. These factors, which are contributing to the growth of social life to a new level, are creating broad opportunities. At the same time, these processes are causing the growth of new forms of offenses, in particular, crimes committed in virtual space. One of such crimes is cyberbullying, which manifests itself in the form of humiliation, intimidation, defamation, or psychological pressure on a person using information technologies.

A unique aspect of cyberbullying crimes is that they are often committed through anonymous user accounts, the offender and the victim may be located in different

countries, and there is a high probability that the information related to the crime will be deleted or changed in a short time. These factors make it exceptionally difficult to identify the offender and prove their guilt. Consequently, electronic evidence, such as social media correspondence, private messages, IP addresses, metadata, and audiovisual files, becomes the primary tool for investigating and proving cyberbullying crimes. Therefore, an effective solution to the problem of cyberbullying is directly linked to the ability to identify, preserve, and assess electronic evidence. Before examining this issue in greater detail or defining the scientific framework of the investigation, it is necessary to first define the term ‘cyber’:

Cyber is a term that refers to any technological tool or phenomenon related to computers, networks, and digital data. It is used in all areas related to the digital world and is closely related to processes that occur in virtual environments (Bandler, 2024).

Cyberbullying is the intentional, repeated, and negative behavior towards a person through digital information and communication media, such as threatening, insulting, defaming, or damaging their reputation. It occurs in technological tools – social networks, messengers, mobile applications, and online platforms. Also, its main essence is to expose the victim to negative consequences in terms of mental health, self-awareness, and social relationships. It is worth noting that the phenomenon of cyberbullying is characterized by its own negative characteristics, and unlike traditional bullying, it leaves a digital mark and occurs in the global information space (Bodova, 2025).

The Resolution of the President of the Republic of Uzbekistan “On measures to protect the rights of consumers of digital products (services) and strengthen the fight against crimes committed using digital technologies” also stipulates the organization of scientific and research activities to combat crime in the field of digital technologies. This resolution also indicates the relevance of the issue covered in the article.

According to UNICEF, cyberbullying is a set of behaviors that are intended to repeatedly harm, intimidate, or embarrass others through social media, instant messaging, or other online environments. Such behaviors include spreading misinformation, sending threatening or abusive messages, disclosing personal information, or damaging the victim’s online reputation (UNICEF, 2025).

Cyberbullying crimes are mainly committed through social networks, messengers and other digital platforms. The peculiarity of these crimes is that they are often committed secretly, through anonymous accounts, and the process of identifying and corroborating evidence is more complicated than in traditional crimes. Therefore, electronic evidence is of great importance as a primary means of proof in the investigation of cyberbullying crimes.

According to the Ministry of Internal Affairs and the Center for Cybersecurity, the number of crimes committed in cyberspace has increased fourfold in the last 3 years. The saddest thing is that about 65-70 percent of victims of cyberbullying are minors and young people. Global research by UNICEF confirms this, showing that one in three Internet users has been subjected to cyberbullying.

These figures prove that cyberbullying is not just a moral issue, but a serious criminal and legal phenomenon that threatens the mental health and safety of society and requires a fundamental reform of investigative methodology.

Today, the problem of cyberbullying is relevant not only as a socio-psychological, but also as a legal issue. Such actions committed in the digital space are associated with violations of human rights and freedoms, and the role of electronic evidence in the process of their identification, proof and legal assessment is of particular importance. Therefore, the scientific analysis of the concept of cyberbullying, its characteristics and legal aspects is one of the important tasks of modern legal research.

However, an analysis of current scientific sources and investigative practice shows that the issues of collecting, storing, authenticating and using electronic evidence in the investigation of cyberbullying crimes have not been sufficiently developed. In particular, some issues related to ensuring the integrity of electronic evidence, confirming its authenticity, and obtaining information stored on foreign platforms create certain difficulties in legislation and practice. This situation creates the need for in-depth research into the scientific and theoretical foundations of electronic evidence and identifying and eliminating existing gaps in this area.

This article analyzes the scientific and theoretical issues of electronic evidence in the investigation of cyberbullying crimes, its types, specific features, and importance in investigative practice. It also highlights the main problems that arise when working with electronic evidence and theoretical approaches to their elimination.

**Methods**

The electronic evidence system used in the investigation of cyberbullying crimes was chosen as the object of the study. The choice of this object is explained by the fact that cyberbullying crimes are committed directly in the digital environment and the traces of the crime are manifested in electronic form. From a legal point of view, electronic evidence is a source of information that embodies information about the crime, the identity of the offender and his actions and is important for solving a criminal case. In cases of cyberbullying, correspondence, electronic messages, audio and video files, IP addresses, log files and other digital data are the main sources of evidence.

The method of scientific and legal analysis was used to study the role of electronic evidence in the investigation of cyberbullying crimes, the concept of electronic evidence, its characteristics, and the scientific views of foreign and national scientists. With the help of this method, the role of electronic evidence as the main means of proof in cyberbullying crimes was determined, and the existence of certain theoretical and practical problems related to the storage and procedural strengthening of electronic evidence was identified.

As a result of the comparative analysis, it was found that in some foreign countries there are special procedural mechanisms for storing and authenticating electronic evidence, and in national legislation some aspects of these issues need to be further improved. In particular, the norms of national legislation were analyzed in comparison with the experience of foreign countries. In this process, only the objects that have common aspects were selected, that is, the procedures for collecting, storing and evaluating electronic evidence were compared. For example, the differences between the procedure for recognizing digital correspondence (messengers, social networks) as evidence in some countries and national practice were studied. In this way, existing problems in the procedural strengthening of electronic evidence and ways to overcome them were identified.

The structural elements of cyberbullying crimes and the specific characteristics of electronic evidence were studied separately. In particular, the main forms of cyberbullying (sending offensive messages, threats, spreading false information) were analyzed separately, and the types of electronic evidence (chat correspondence, audio-video files, IP addresses, log files) that arise in each case were studied using the analysis method. It was also analyzed how the characteristics of electronic evidence, such as its volatility, rapid disappearance or modification, affect the investigation process. For example, the issues of restoring or reinforcing an offensive post on a social network if it is deleted were considered separately.

The data obtained as a result of the analysis were summarized using the synthesis method and holistic scientific conclusions were formed. In particular, various elements

related to cyberbullying crimes and working with electronic evidence were considered in their interrelation and their role as a single system was justified. Using this method, the sequential stages of working with electronic evidence were systematized and the importance of rapid identification and preservation of evidence in the investigation of cyberbullying crimes was justified. For example, in cases of cyberbullying, the stages of rapid identification of evidence (taking screenshots, storing server logs), their procedural formalization and presentation as reliable evidence in court were considered as a single system.

“Electronic evidence is not stored for as long as traditional evidence, and is subject to modification, data formats becoming obsolete or disappearing over time, and the system in which the evidence is stored may fail.” These specific characteristics of electronic evidence were analyzed.

Also, during the research process, modern scientific sources on cyberbullying and electronic evidence were studied through the method of scientific literature analysis. This method served to strengthen the theoretical foundations of the study.

**Results**

When analyzing cyberbullying crimes, the focus is often on the direct victims, as they are seen as the individuals directly affected by the online attack. This approach is important for identifying the crime, assessing its negative consequences and developing appropriate measures. Cyberbullying has several characteristics that differ from traditional crimes: digital devices, virtual traces, social network profiles and online connections play an important role in its perpetration. For example, in traditional crimes, evidence found at the scene of the crime can be crucial in identifying the suspect; however, in cyberbullying, the perpetrator is identified through the device on which the crime was committed, its IP address, the time of the crime and other metadata. Electronic traces are also used to shed light on the context and mechanism of the crime. These aspects complicate the processes of collecting electronic evidence and its admissibility as reliable evidence in court. However, at the same time, they allow proving the commission of a crime and identifying the device on which the crime was committed.

When investigating cyberbullying crimes, it is important to pay special attention to the victim. It is precisely by studying the victim’s condition that it becomes possible to identify the crime in a timely manner, assess the extent of the harm caused to him, and analyze the full context of the incident.

At the same time, it is also necessary to identify and quickly analyze how cyberbullying spreads through social networks and other information systems. This will help increase the effectiveness of the investigation process.

Such an approach requires not only the detection of crime, but also the introduction of detection, corrective and preventive control mechanisms aimed at ensuring safety. The main goal of these measures is to reduce the harm caused by cyberbullying, strengthen the legal and psychological protection of victims, and prevent the recurrence of such crimes in the future.

Forensic science and digital forensics play a key role in implementing this approach, as these areas enable the identification of electronic evidence, its integrity and reliability, and its reasonable and credible presentation in court.

Digital traces, including IP addresses, metadata, chat logs, and timestamps, are essential in solving crimes. They can help identify the perpetrator, reconstruct the sequence of events, and assess the consequences of a crime.

In this regard, the role of electronic evidence is crucial in the legal assessment and investigation of modern types of crimes such as cyberbullying (Sobirova, 2025).

The Law of the Republic of Uzbekistan “On Cybersecurity” establishes legal mechanisms for combating cybercrime, protecting information systems and resources, and detecting cybersecurity incidents. Article 16 of the Law also stipulates that cybersecurity entities must notify the authorized state body about cybersecurity incidents and cybercrimes that have occurred, prevent the loss of digital traces, and ensure the permanent storage of information necessary for the investigation. This norm constitutes the legal basis for the process of storing, recovering, and analyzing electronic evidence in the investigation of crimes related to cyberbullying. In addition, Article 22 of the Law states that the investigation of cybersecurity incidents shall be carried out by an authorized state body, which indicates the need to use special technical and forensic methods in exposing cybercrimes.

The conducted analyses showed that with the increase in the number of cybercrimes, the importance of electronic evidence is also increasing. In the majority of crimes committed in the digital environment, evidentiary information is available in electronic form, and their timely identification and storage is one of the main conditions for exposing the crime. The main feature of these crimes committed in virtual space is that they are carried out directly through information and communication technologies, and the traces of the crime are also formed in the digital environment. Therefore, electronic evidence is the main source of evidence in identifying, proving and holding the guilty person accountable for cyberbullying crimes.

The study identified the most common electronic evidence in cyberbullying investigations. In particular, social media and messenger conversations, audio and video recordings, screenshots, technical information about user accounts, IP addresses, log files, and metadata were identified as important sources of information confirming the fact of cyberbullying. This evidence allows us to determine the time, method, and duration of the crime, as well as the psychological harm inflicted on the victim.

The results also clearly demonstrated the unique characteristics of electronic evidence. In particular, electronic evidence is a category of evidence that is volatile and prone to loss. For example, electronic evidence can be destroyed by deleting correspondence, closing accounts, editing data, or hiding virtual traces. Therefore, speed in identifying and procedurally strengthening electronic evidence in the investigation process is of paramount importance.

Overall, the results of the study showed that the role of electronic evidence in the investigation of cyberbullying crimes is important not only as a means of proof, but also as a source of information that fully reveals the mechanism of the crime. Proper identification, preservation and evaluation of electronic evidence is one of the key factors ensuring the effectiveness and fair completion of the investigation.

**Discussion**

In the context of the increasing importance of electronic evidence in the investigation of cyberbullying crimes, it is urgent to strengthen the scientific and theoretical foundations for their proper use. Without the development of clear legal mechanisms and effective methodological approaches to working with electronic evidence, it will be difficult to increase the effectiveness of the fight against cyberbullying crimes.

At the same time, cyberbullying crimes have specific features that distinguish them from traditional crimes. Such crimes are characterized by the fact that they are committed through information technologies, computer systems and the Internet. Technical and software tools are used to commit crimes, and the object of the crime is mainly information security, privacy and human dignity. Cyberbullying crimes are committed remotely and often anonymously. These crimes are distinguished by their national and transnational nature.

Cyberbullying crimes are committed using technological devices. These crimes are often aimed at humiliating a person, humiliating them in front of society and people. They can choose lonely, psychologically vulnerable people as their prey. In particular, this type of crime can be targeted not at technical systems, but at the human psyche, that is, at the actions, confessions and weaknesses of users. Therefore, relying only on technical solutions in the fight against cyberbullying crimes is not enough. In this regard, a comprehensive approach is needed that takes into account the human factor, the social environment and the culture of information security.

Many scholars have emphasized the need for substantial research to fully understand the complexities of cyberbullying on social media. Oksanen et al. discussed cyberbullying within workplace organizations and closed groups on social media and noted that young professionals in closed groups on social media reported high levels of cyberbullying victimization, with 17% of Finnish workers reporting victimization, and that victims in closed groups on social media reported high levels of psychological stress, burnout, and technostress (Oksanen et al., 2020).

Most studies examining the prevalence of cyberbullying have focused on high school-aged students. In addition, sociodemographic factors, particularly race, as well as the individual's life course, have been less studied than age and gender in the relationship between cyberbullying victimization and perpetration. This suggests that additional research is needed in this area (Kowalski, 2018).

A study by Abaido et al. examined the prevalence of cyberbullying among university students in an Arab community and their attitudes towards reporting it. The survey found that 91% of respondents confirmed that cyberbullying occurs on social media, with Instagram (55.5%) and Facebook (38%) being the most common platforms. Furthermore, the authors found that reporting cyberbullying incidents is a significant problem due to social and cultural constraints (Abaido, 2020).

Factors influencing the occurrence of cyberbullying on social media among university students were studied. In particular, the prevalence of cyberbullying is a serious problem on social media platforms, which has a long-term psychological impact on individuals. In the digital environment, people perform various social roles, which affects their subsequent communication. As a result, their behavior can become tied to certain restrictions and habits. For the study conducted among university students, only the Instagram platform was selected, while other social networks (e.g., Telegram, Facebook, TikTok, etc.) were not included in the scope of the study. In conclusion, cyberbullying is a serious social problem characterized by anonymity, prevalence, and continuous continuation. Cyberbullying occurs through intimidation, harassment, and the dissemination of harmful information through social networks. In order to prevent it and help victims, it is important to understand how this phenomenon occurs (Mtshali & Khubisa, 2019).

Explaining cybercrimes solely through the technological tools used to commit them is not a sufficient and sustainable approach. On the one hand, digital technologies are developing rapidly, and on the other hand, the human factors that give rise to such crimes – motives, psychological state and social environment – are becoming increasingly complex.

Also, the distinction between crimes committed using digital means and crimes that occur exclusively in the Internet and virtual environments is not always clear. Therefore, explaining cybercrimes solely in terms of technical means does not fully reveal their true nature (McGuire, 2019) .

The principle of protective jurisdiction means that even if the perpetrator of a crime is in the territory of another state, if he commits a crime against the citizens of a given state

or its essential interests, that state has the right to consider, investigate and prosecute the crime.

In cybercrime, if the harm is caused to the citizens or national interests of a state, the crime can be considered within the jurisdiction of that state, regardless of where it was committed. In particular, in some situations, several states simultaneously consider themselves competent for the crime. As a result, disagreements or conflicts between jurisdictions may arise over which state should handle the case.

The principle of universal jurisdiction applies to serious crimes that threaten all of humanity. Every state has the right to try these crimes, regardless of where they were committed or the nationality of the perpetrator (Rajabov, 2024).

The current Criminal Code does not provide a direct legal definition of concepts such as “cyberbullying,” “cyberstalking” or “insulting using digital technologies”. Investigative bodies are forced to qualify cyberbullying acts under Article 139 (Defamation) or Article 140 (Insult) of the Criminal Code. However, the aggravating factor “in the mass media or on the Internet” in these articles does not fully cover all the destructive features of cyberbullying (for example, group clinging, creation of fake content using artificial intelligence – deepfake).

The Criminal Procedure Code does not sufficiently interpret the concept of “Electronic evidence”, the specific procedures for its identification, seizure, examination and storage. There is no unified investigative practice in the procedural formalization of correspondence, screenshots and disappearing messages in messengers (Telegram, Instagram, etc.), which are the main evidence in cyberbullying. There are cases where screenshots are often rejected by courts as evidence that is “illegally obtained or can be easily altered.”

**Table**

| Years | To the list taken general cybercrimes number | On the Internet insult, slander and harassment (Cyberbullying) | Share of minors and youth (%) | Digital evidence forgery/no to do cases |
|---|---|---|---|---|
| **2021** | 2 214 | 432 | 48% | 89 |
| **2022** | 4 332 | 812 | 53% | 142 |
| **2023** | 8 110 | 1,654 | 59% | 310 |
| **2024** | 12,450 | 2,890 | 64% | 512 |
| **2025** | 16,200 | 4 120 | 68% | 745 |

The statistics show that from 2021 to 2025, the number of total cybercrimes increased by 7.3 times, and cases of direct cyberbullying (insults, defamation, violation of privacy on the Internet) increased by almost 9.5 times. This indicator confirms that cyberbullying is becoming the most dangerous socio-legal problem with a high level of latency (concealment) in society.

Also, the share of minors and young people among the victims of cyberbullying is increasing every year (from 48% in 2021 to 68% in 2025). The main reason for this is the younger generation’s active presence in the digital space and on social networks (Telegram, Instagram, TikTok) and their lack of awareness of cyber-hygiene rules.

One of the most dangerous trends for investigative practice is the sharp increase in cases of “falsification or deletion of digital evidence” (from 89 in 2021 to 745 in 2025).

Cyberbullying perpetrators are rapidly destroying electronic evidence using modern anonymizing tools (VPN, proxy), disappearing messages, and fake accounts. This scientifically and practically proves the need to introduce mechanisms for rapid fixation (sealing) of electronic evidence in criminal procedural legislation without delay.

In the investigation process, procedural deadlines are violated when collecting electronic evidence. Ensuring security when storing electronic evidence is important. In particular, information contained in electronic evidence may be lost or corrupted. There may be delays in identifying it. This leads to a decrease in efficiency. As a result, the need to strengthen cooperation between operational-search activities and investigative actions is evident.

International experience in working with electronic evidence in the investigation of cyberbullying crimes shows that in developed countries, the collection, storage and analysis of this type of evidence is carried out on the basis of strict standards. In particular, in international practice, maintaining the integrity and reliability of electronic evidence is recognized as a fundamental principle in the process of working with it (U.S. Department of Justice, 2024).

For example, the internationally accepted ISO/IEC 27037 standard clearly regulates the processes for identifying, collecting, retrieving, and preserving electronic evidence, and establishes a mandatory requirement for maintaining a “chain of custody” (Luthfi, 2024). This is important for ensuring the admissibility of evidence in court.

In addition, international experience distinguishes three main sources of electronic evidence: data stored on devices, data publicly available on the Internet, and data stored by service providers.[4] In particular, mutual legal assistance mechanisms are used between states to obtain the latter type of data, which is an important tool in investigating cybercrime at a transnational level.

At the same time, guidelines and recommendations developed by international organizations emphasize the need for careful assessment of the reliability of electronic evidence when using it in court. Since electronic evidence can be easily altered or destroyed, enhanced procedural control over it is required (Dmitrieva & Pastukhov, 2023).

Although the current legislation of the Republic of Uzbekistan does not distinguish the concept of “electronic evidence” into a separate legal category, in practice and in some regulatory documents there are concepts close to it – for example, expressions such as “electronic document,” “electronic information carriers,” “information resources.”

The concept of “electronic evidence” is mainly determined on the basis of theoretical approaches. According to M.V. Gorelov, electronic evidence is information about circumstances of importance in the case, reflected in digital, audio or video form. It also includes minutes of court hearings and minutes of procedural actions executed using electronic computing devices (Gorelov, 2005).

The specific characteristics of electronic evidence can be summarized as follows:

- Electronic evidence is not stored for as long as traditional evidence, and it is subject to changes, data formats becoming obsolete or lost over time, and the system in which the evidence is stored may fail.
- There is no level of protection for electronic evidence, it can be damaged by viruses, malware, and cybercriminals can break into the system.
- Electronic evidence always leaves a trace. Many electronic activities (e.g. logins, network traffic, chats) are recorded in log files.

Despite its intangible nature, electronic evidence always leaves some digital footprint. Even if criminals use information technology to commit crimes, take measures to hide their identity, protect their personal data, or anonymize their activities, their actions do

not remain completely untraceable. Because any digital activity is carried out through information systems, servers, network devices, and software, and in these processes, traces are created in the form of technical logs, metadata, IP addresses, time stamps, and other digital data.

In the practice of forensic science and forensic examination, these digital traces are identified as electronic evidence, analyzed and formalized in the appropriate procedural order. With the help of special technical means and expert methods, it is possible to identify hidden or encrypted data, recover deleted files, and determine the time, method, and person of the crime. Therefore, although the concealment measures taken by criminals may make the identification of electronic evidence difficult, they do not make it completely impossible.

Electronic evidence can also be divided into 3 types based on the form in which it appears. For example:

1. Evidence resulting from human factors (installed programs, additional programs, logins and passwords when entering the site, search history);

2. Evidence generated by the device. This type of evidence can include images (jpg, gif), videos (mp4, MOV), audio (mp3, MID), and office (Docx, PPT);

3. Evidence arising from cybercrime.

Electronic evidence can come in many forms, and it is important to understand the types when presenting a case in court. The most common types of electronic evidence are:

Email correspondence can be important and valuable evidence in legal proceedings because it contains important information about the relationship between the parties, the content of the communication, and specific circumstances. Lawyers can use emails as a means of confirming the existence of communication between the parties or as a means of proving a particular opinion, agreement, or legal position.

Text messages are similar in content to emails, they are generally shorter and less formal in expression. However, such messages can be valuable as evidence in court proceedings where intentions, agreements, or important matters are discussed between individuals via text communication.

Social media platforms like Facebook, Twitter, and Instagram are increasingly being used as evidence in court cases. Lawyers can use posts to prove a person’s mental state, location, or other relevant information.

Digital files, such as documents, images, videos, and audio recordings, can be admitted as evidence in court proceedings. They can be used to support arguments, provide context, and prove specific points. It is important to note that electronic evidence must meet specific requirements to be admissible in court. The investigator must ensure that the evidence is authentic, relevant, and reliable. They must also be careful to maintain the integrity of the electronic evidence so that it cannot be challenged or rejected in court (Jaiswal, n.d.).

Foreign scholars have classified electronic evidence into types and forms. There are different views on the classification of electronic evidence into types and forms.

1. File-based evidence includes Word, Excel, PDF documents, images, videos, and audio files. They can be existing on a computer or mobile device, created or modified by the user.

According to American expert Casey: “File-based evidence usually preserves traces of crime without hiding them, but technical means are required to detect them” (Casey, 2011).

2. Metadata is technical information about files such as creation date, author, last edited, and storage location. It can often be more important than the main evidence.

According to American expert and researcher Pollitt, “Metadata is crucial in verifying the reliability and consistency of electronic evidence” (Pollitt, 2008).

3. System and log files are logs automatically created by the operating system, web server, router, or applications. They clearly show the time of user activity or an event.

4. Emails and messages (e-mails, messages) – messages on email servers, correspondence in messengers, text messages – are considered important as means of communication used in the commission of a crime.

5. Evidence on mobile devices – SMS, GPS location data, call history, camera recordings, and activities on mobile apps fall into this group.

According to American academic and journalist Garfinkel, “Mobile devices embody a wealth of evidence related to personal life, so analyzing them requires ethical and legal caution” (Garfinkel, 2010).

6. Evidence in the cloud – documents, photos, and recordings stored in services like Google Drive, OneDrive, and iCloud. Retrieving them often requires international cooperation (SWGDE, 2022).

There are several forms of electronic evidence, including:

1. Static electronic evidence is information that exists in an unchanged state and is not in contact with an active network at the time of its acquisition. (Documents on a USB flash drive, files on a CD/DVD, undeleted documents on a hard drive)

According to Casey, “Static data exists primarily on stationary devices and is best studied using classical forensic methods” (Casey, 2011).

2. Live /Volatile electronic evidence is data that exists while the system is running. It is usually in random access memory (RAM), network traffic, or open sessions and is temporary in nature. (Program processes in RAM, files transferred in real time over the Internet, system session logs).

According to US scientist Simson Garfinkel, the biggest problem with working with volatile electronic evidence is that such data can be instantly lost as a result of a minor system failure or power outage, making it extremely difficult to identify and preserve (Garfinkel, 2010).

3. Logical copy is a version of electronic evidence that is visible to the operating system but structured at the file system level. This is often done in the form of a copy of documents, photos, or emails.

As American scholar Mark M. Pollitt has noted, the use of logical copies greatly simplifies the analysis process. However, these copies may in some cases not contain important information that is hidden or previously deleted. Therefore, they should not always be considered a complete source of evidence (Pollitt, 2008).

4. Bit-level image format is a complete copy of the entire memory, including any files, including deleted, hidden, or inconsistent data. It is the most suitable format for forensic investigations.

American legal scholar Carrier argues that a full digital copy of a disc is the most reliable and legally protected form of evidence, because it is archived in an exact replica of the original media.

5. Hash-verified form is a copy of the evidence (either static or image) verified using a hash function. This is used to prove its integrity.

Investigating cyberbullying crimes is one of the most complex processes. In particular, this is due to the specific characteristics of such crimes and the use of advanced technologies in them. Although cyberbullying crimes may contain similar features to traditional crimes – for example, insults, extortion, fraud or defamation, they are fundamentally different in content and form. Therefore, the role and significance of the

place where the crime was committed is important. Unfortunately, most of the existing research has not paid sufficient attention to the digital environment in which the crime was committed. However, it is in this environment that electronic evidence is formed and is the main tool for proving the crime. Electronic evidence must be reliable, accurate and in a form that meets legal requirements, since it forms the basis of court decisions and plays an important role in punishing the guilty person (Yeboah-Ofori & Brown, 2020).

**Conclusion**

In the modern era, as information technologies penetrate deeply into all aspects of our lives, the number and scale of cybercrimes are also increasing. This poses new challenges for law enforcement agencies, in particular, the problems of working with electronic evidence in the investigation process, its collection, evaluation, and most importantly, its reliable storage have become a pressing issue.

In conclusion, in the investigation of cyberbullying crimes, electronic evidence is emerging as an integral and decisive element of modern criminal procedure. Such offenses committed in the digital space have their own characteristics, unlike traditional evidence, and the processes of their identification, recording, storage and evaluation require a special approach. Therefore, a deep scientific and theoretical analysis of the legal nature of electronic evidence, its role in the evidentiary system and its procedural status is of great importance.

## REFERENCES

Association of Chief Police Officers. (2011). *ACPO good practice guide for digital evidence* (4th ed.). https://library.npia.police.uk/docs/acpo/digital-evidence-2011

Bandler, J. (2024, December 16). *Cyberlaw: An area of law for all of us.* Reuters Legal News. https://www.reuters.com/legal/legalindustry/cyberlaw-an-area-law-all-us-2024-12-16/

Chandra, D. (2025). Examining the contours and challenges of the national cybercrime reporting portal in countering digital financial frauds. *Journal of Victimology and Victim Justice, 8*(1), 251–266. https://doi.org/10.1177/25166069241306546

Council of Europe. (2001). *Convention on cybercrime* (ETS No. 185). https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Dmitrieva, A. A., & Pastukhov, P. S. (2023). Concept of electronic evidence in criminal legal procedure. *Journal of Digital Technologies and Law, 1*(1), 1–25.

European Commission. (2021). *Proposal for a regulation on electronic evidence in criminal matters.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

European Commission. (2025, January 21). *E-evidence: New rules to facilitate acquisition of electronic evidence.* https://digital-strategy.ec.europa.eu/en/policies/e-evidence

Europol. (2023). *Digital evidence: Guidelines for law enforcement and judicial authorities.* https://www.europol.europa.eu/publications-documents/digital-evidence-guidelines

Federal Rules of Evidence, 28 U.S.C. app. (2017). Rule 902(14): Self-authentication of data copied from electronic devices, storage media, and files. https://www.law.cornell.edu/rules/fre/rule_902

Gorelov, M. V. (2005). *Elektronnye dokazatelstva v grajdanskom sudoproizvodstve Rossii (voprosy teorii i praktiki)* [Electronic evidence in Russian civil proceedings (theoretical and practical issues)] [Doctoral dissertation, Yekaterinburg].

Granja, F. M., & Rafael, G. D. R. (2017). The preservation of digital evidence and its admissibility in the court. *International Journal of Electronic Security and Digital Forensics, 9*(1), 1–18.

Gulomovna, Y. N. (2025). Foreign experiences in preventing cybercrime. *Critical Thinking, Analytical Thinking and Innovative Ideas, 1*(5), 159–164.

Guttman, B., White, D. R., & Walraven, T. (2022). *Digital evidence preservation: Considerations for evidence handlers.*

Holt, T. J. (2019). *The human factor of cybercrime.* Routledge.

Indian Computer Emergency Response Team (CERT-In). (n.d.). *Organization homepage.* https://www.cert-in.org.in/

International Organization for Standardization. (2012). ISO/IEC 27037:2012 – *Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence.* https://www.iso.org/standard/44381.html

International Organization for Standardization. (2023, November 21). *ISO/IEC 27402:2023 – Cybersecurity – IoT security and privacy – Device baseline requirements.* https://www.iso.org/standard/83506.html

INTERPOL. (2020). *Digital forensics guidelines.* https://www.interpol.int/en/Crimes/Cybercrime/Digital-Forensics

Jain, R., & Sonowal, B. (2025). Analyzing the procedure for investigation in cybercrime and admissibility of electronic evidence. *In Cybercrime unveiled: Technologies for analyzing legal complexity* (pp. 265–289). Springer Nature.

Jaiswal, A. (n.d.). *Electronic evidence. Medium.* https://medium.com/@jaiswalamulya3/electronic-evidence-cd349aed85ba

Kamal, R., Hemdan, E. E. D., & El□Fishway, N. (2022). Forensics chain for evidence preservation system: An evidence preservation forensics framework for internet of things-based smart city security using blockchain. *Concurrency and Computation: Practice and Experience, 34*(21), e7062.

Kim, D., Ihm, S. Y., & Son, Y. (2021). Two-level blockchain system for digital crime evidence management. *Sensors, 21*(9), Article 3051. https://doi.org/10.3390/s21093051

Luthfi, A. (2024). Comparison study of NIST SP 800-86 and ISO/IEC 27037 standards as a framework for digital forensic evidence analysis. *Journal of Information Systems and Informatics, 6*(2), 701–718.

Lyle, J. R., Guttman, B., Butler, J., Sauerwein, K., Reed, C., & Lloyd, C. (2022). *Digital investigation techniques: A NIST scientific foundation review.*

Marcella, A., Jr., & Menendez, D. (2010). *Cyber forensics: A field manual for collecting, examining, and preserving evidence of computer crimes.* Auerbach Publications.

Mason, S., & Seng, D. (2017). *Electronic evidence.* University of London Press.

McGuire, M. (2019). It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime. *In The human factor of cybercrime* (pp. 3–28). Routledge.

NATO Cooperative Cyber Defense Center of Excellence. (2022). *Cyber forensics toolkit.* https://ccdcoe.org/library/publications/cyber-forensics-toolkit/

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic Sciences, 2*(2), 379–398.

Pirmatov, O. (2023). Problems of evaluation of digital evidence based on blockchain technologies. *Janus, 14*(1).

President of the Republic of Uzbekistan. (2023, November 30). *On measures to protect the rights of consumers of digital products (services) and strengthen the fight against violations committed using digital technologies* (Resolution No. RP 381). Lex.uz.

Rajabov, U. (2024). Cybercrime law: New trends in cybercrime activity and international cooperation in combating cybercrime. *Innovative Developments and Research in Education, 3*(32), 128–135.

Republic of Uzbekistan. (2022, April 15). *On cybersecurity* (Law No. LRU 764). https://lex.uz/docs/5970546

Safitri, I. (2023). Protection of victims of deep fake pornography in a legal perspective in Indonesia. *International Journal of Multicultural and Multireligious Understanding, 10*(1), 384–385.

Scientific Working Group on Digital Evidence (SWGDE). (n.d.). *Documents.* https://www.swgde.org/documents

Shkurova, P. D. (2017). *Elektronnyy dokument kak samodostatochnoye sredstvo dokazatel'stva v grazhdanskom i administrativnom sudoproizvodstve* [Electronic document as a self-supporting means of proof in civil and administrative legal proceedings]. *Juridicheskie Isledovaniya*.

Sibe, R. T., & Kaunert, C. (2024). Digital evidence, digital forensics, and digital forensic readiness. *In Cybercrime, digital forensic readiness, and financial crime investigation in Nigeria* (pp. 57–83). Springer Nature.

Skorobogatov, A. V. (2020). *Tsifrovye dokazatel'stva v ugolovnom protsesse: Teoretiko-pravovoi analiz* [Digital evidence in criminal proceedings: Theoretical and legal analysis]. Yustitsinform.

Tavani, H. T. (2000). *Ethics and technology: Controversies, questions, and strategies for ethical computing.* Wiley.

U.S. Department of Justice. (n.d.). *Forensic examination of digital evidence: A guide for law enforcement.* https://www.ojp.gov/library/publications/forensic-examination-digital-evidence-guide-law-enforcement

Yeboah-Ofori, A., & Brown, A. D. (2020). Digital forensics investigation jurisprudence: Issues of admissibility of digital evidence. *Journal of Forensic, Legal & Investigative Sciences, 6*(1), 1–8.


# TSUL LEGAL REPORT

INTERNATIONAL ELECTRONIC SCIENTIFIC JOURNAL

VOLUME 7
ISSUE 2
JUNE 2026