ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

Digital Evidence Authentication in Criminal Justice System "An Anglo-Saxon and Latin Criminal Law Perspectives"

Dr. Fahil Abdulbasit Abdulkareem
Dept. of Legal Administration, Technical College of Administration, Duhok Polytechnic University, Duhok, Kurdistan Region, Iraq
Email:fahil.abdulbasit@dpu.edu.krd

ID No. 3094	Received: 16/11/2024	Keyword:
(PP 169 - 179)	Accepted: 13/04/2025	digital evidence, criminal justice system, algorithmic criminology, democracy of justice.
https://doi.org/10.21271/zjlp.23.sp.10	Published: 29/04/2025	

Abstract

Criminal justice system now faces significant procedural and substantive issues as a result of the development of the internet and the pervasive use of information systems. Since digital evidence is technological scientific proof that is impossible to dispose and replicable, it offers several benefits. Regarding the evidence's probative value, the criminal judge has considerable authority when assessing digital evidence. Three conditions must be satisfied for digital evidence to be admitted in court: the evidence's legitimacy, the judge's degree of certainty, and the evidence's discussion. The existing legal framework determines the judge's ability to accept digital evidence. The Latin system, also called the system of free evidence, and the Anglo-Saxon system, often called the system of restricted evidence, are the two primary legal systems. The importance of the study stems from the fact that many crimes of a digital nature cannot be detected or proven using the traditional criminal laws in the Iraqi criminal system, while the study of digital evidence has started to replace and play a role in criminal evidence globally in order to control crimes and prevent offenders from impunity. Therefore, by presenting the legal framework of the authenticity of digital evidence from a Latin and Anglo-Saxon perspectives, the research's backdrop stems from its correspondence with global criminal legislative advancements in the techno-legal area. The research's challenge is to use descriptive and analytical methods to explain the probative value of digital evidence in relation to criminal evidence.

1. Introduction

Forensic evidence is the core of proof and a means of attributing or denying a criminal incident to the defendant. Therefore, it is important at all stages of the trial (The pre-trial, trial, and verdict process) and through it, the truth is known. Forensic evidence is aimed at proof, and this is defined as the proof of a legally significant fact to the authorities responsible for criminal proceedings using the methods provided by law following the regulations to which it is subject.

Scientific and technological progress has given rise to the so-called information system, with its databases, programs and information, which has reached a large proportion of people in the form of information networks and the undeniable benefits they bring to all

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

cultural, scientific and political levels. On the other hand, it has also opened up a space for considerable risks, as the information system has become a place and a means for committing so-called information crimes (cybercrimes). Law enforcement authorities have been forced to use modern digital technologies and technical tools in their proven (collection process) due to the specific digital nature of electronic crimes (information crimes) and the impact this has on the evidence that can be used to prove them under criminal law. This has resulted in the emergence of a new category of evidence, namely digital evidence.

For traditional forensic evidence to be accepted in court, it must be specific, direct, and probative to prove the incident. To be accepted in court, digital evidence must also meet certain criteria. In the context of this topic, the following question therefore arises: What is meant by digital evidence and what authenticity does it have before comparative justice (Latin and Anglo-Saxon criminal justice?)

2. Definition of Digital Evidence

The definitions of digital evidence varied between broadening its concept and narrowing it down. The Conference of International Investigators (CII 2021) defined it as "information and data of potential value to an investigation that is stored or transmitted in digital form. Digital evidence differs from traditional evidence in multiple ways:

A. It is often highly complex, frequently scattered among different physical or virtual locations, and requires expertise and tools to collect.

B. It can easily be altered, accidentally or intentionally, possibly without leaving any trace.

C. It can easily be copied and distributed, presenting challenges to preserving confidentiality.

D. It can be temporary in nature: network logs, Internet browsing history, social media posts, instant messages, cached data and deleted data can be lost if not preserved in a timely manner."

Digital evidence can be described as information retrieved from computers in the form of magnetic or electrical files or pulses. This data can be collected and analysed using specialised programs, applications, and technology. The findings can then be presented as evidence that is admissible in court. Information that originates in the digital world and can be used as evidence in a court of law (jurisdiction court) in the form of physical extracts or documentation can be referred to as a digital evidence (Horsman, 2023.(

3. Characteristics of Digital Evidence

Digital evidence has many advantages over traditional forensic evidence. It is a type of scientific evidence that is invisible and difficult to dispose of. This evidence can be easily retrieved with a high degree of accuracy (Stoykova, 2023). Additionally, digital evidence can be characterised by several features, including those listed below:

A. Invisible Evidence refers to data and information in an intangible electronic form (Morelato, Cadola, Bérubé, Ribaux, & Baechler, 2023), which is realised using computer hardware and software systems.

B. Digital evidence is scientific evidence, which means it must adhere to scientific rules. In comparative judiciary, the law seeks justice while science seeks the truth.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

C. The evidence in digital form is technical in nature. As technology produces digital pulses, its value lies in the ability to work with the solid components that make up the computer (Forte, 2003). This data is dynamic, high-speed, and transmitted from one location to another through communication networks.
D. Reproducibility, or copying, of digital evidence, is a crucial feature that reduces the risk of damaging the original evidence (Choi & Yang, 2021). This is because the process of copying is identical to the method of creation, which creates an effective guarantee for preserving the evidence from loss and damage by utilising exact copies of the evidence .
E. The digital evidence is difficult to remove as retrieval programs can recover it even after an order is issued to delete it.

4. The Common Types of Digital Evidence

4.1. Digital Messages

Written communications between two or more parties have been considered some of the most reliable pieces of evidence in the history of law. These communications not only help investigators gain new insights into a crime, but also define relationships between suspects, validate statements, and establish a timeline of events (Sokol et al., 2023). Investigators cannot disregard the source of a digital message, despite their primary interest in its content. A vast range of communication methods may be submitted as evidence in our digital age, including Text messages that can be sent through smartphones, social media platforms, instant messaging software, and emails. In addition, digital memos and documents can also be used for communication purposes.

4.2. Browser and Search History

It is a known fact that people spend more than six hours per day on the Internet. This makes browsers a valuable source of evidence for investigators. Every search and website visit leaves a trail that can be followed and browsing history usually provides the easiest path. Some people may clear their browsing history to protect their privacy, but there are still ways to obtain this information. For instance, several websites and platforms, such as Google, store search history data for each user under their account (Sokol, Rózenfeldová, Lučivjanská, & Harašta, 2020). A warrant can be obtained data, which can provide a significant amount of information to support an investigation or be used as evidence in a trial .

4.3. Digital Photographs and Video Footage

Digital images and videos are crucial pieces of evidence in criminal trials. However, this type of evidence is easily manipulated, and people may not be aware that they are doing it. Simple actions such as playing the video with the wrong software, compressing the video to share, or converting the files to a playable format can alter their contents (Pedapudi & Vadlamani, 2023). Therefore, agencies and law firms need to follow the correct procedures for acquiring, storing, and presenting evidence. Agencies must obtain and examine original, unmodified digital files as evidence. The sources of evidence generated and stored by law enforcement, such as body-worn and dashboard cameras are particularly valuable as they are under complete oversight. However, third-party sources (Holt & Dolliver, 2021), such as digital video files, CCTV cameras, and smartphone camera photographs, must be gathered, stored, and analysed using

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

forensically sound procedures. This ensures that they can be presented objectively in a courtroom (Dolliver, Collins, & Sams, 2017).

4.4. Log files

Computer software typically generates activity logs that document various processes and errors, from operating system functions to video game glitches. Although these logs are primarily intended for maintenance purposes (Dolliver et al., 2017), they can also serve as evidence to confirm the activities of specific individuals or reveal additional information for investigators. The contents and location of each log file can vary depending on the software (Cheng, Shi, Gong, & Guan, 2021). However, some common examples of digital evidence that are utilised include :

A. Phone logs: Smartphones keep comprehensive records of daily activities, including call frequency and location data. They can also confirm the time a photo or video was captured (Domingues, Andrade, & Frade, 2021).

B. IP logs: IP addresses are used to identify devices and users accessing a website, and their physical location can be determined using IP logs (Sokol et al., 2020).

C. Transaction logs: These logs are used to track changes made to files, enabling administrators to revert to a previous state. These logs are commonly utilised by servers, databases, and cloud-based document processors such as Google Docs (Choi & Lee, 2023).

D. Event logs: Computer software and operating systems maintain event logs to track system activities, identify errors and diagnose crashes. These logs also help to identify whether a human or a computer process triggered a specific event (Khan, Parkinson, & Murphy, 2023).

E. Message logs: Most communication software, including messaging and gaming chat, saves conversations for future retrieval (Forte, 2004).

5. The Basic Conditions of Digital Evidence

The criminal judge is obligated to meet three basic conditions in assessing digital evidence as scientific (technological) evidence before the criminal court:

A. The first condition for digital evidence to be considered legitimate is that it must be obtained through legal means within the criminal system. If the procedures used to obtain the digital evidence are not based on a legal basis, they will be invalidated, and the evidence will not be considered legitimate. For example, using physical or moral coercion, or fraudulent methods against the perpetrator, such as deceiving them to reveal their entry code to their system, will make the evidence invalid (Scanlon, Breitinger, Hargreaves, Hilgert, & Sheppard, 2023). The legality of evidence is deemed an essential aspect of the criminal procedure reform movement. Recommendation No. 18 of the Fifteenth International Conference of the International Penal Law Association, held in Brazil in September 1994, states that: "Any evidence obtained by violation of a fundamental right, including any derivative evidence thereof, is invalid and inadmissible with respect to any stage of the procedure.". The principle of legitimacy is crucial when investigating digital evidence in both information crimes as well as traditional and hybrid crimes in the digital environment. Any violation of this principle will render the procedure invalid. Additionally, this principle determines the responsibility of law enforcement officers for their actions under the law.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

B. The second condition for digital evidence is the judge's level of certainty when convicting an offender. It is constitutionally crucial for a judge to have a high level of certainty, regardless of whether the evidence is traditional, digital, or a combination of both. According to Article 19, paragraph 5 of the Iraqi Constitution of 2005, when there is doubt in a criminal case, it is always interpreted in favour of the accused. To reach a state of certainty in traditional crimes, a judge can scrutinise the evidence, analyse it, and draw a conclusion. However, when it comes to digital crimes, the judge must possess technical knowledge of information matters to determine certainty. Without sufficient technical knowledge, the judge may have doubts about the digital evidence, which could lead to the release or acquittal of the defendant. Therefore, any defendant in a digital case can benefit from doubts generated by the judge. According to the majority of comparative criminal law experts, computer outputs are considered to have a high level of certainty. This is why the American criminal justice system recognises copies of data extracted from computers as evidence with significant probative value.

C. The third condition for digital evidence is that it should be presented and discussed during court sessions. This means that the evidence must have a legal basis established in the case papers, and the parties involved must be given sufficient opportunity to view and discuss it. This applies to all types of evidence, as stated in article 212 of the Iraqi Criminal Procedure Code 23 of 1971. The discussion of digital evidence follows two fundamental rules. Firstly, the opponents have the right to access and respond to the digital evidence until a legal decision is reached, guaranteed by articles 123 and 124 of the Iraqi Criminal Procedure Code 23 of 1971. This statement emphasises the importance of allowing individuals to have the right to defend themselves and confront the evidence presented against them. Secondly, for the judge's verdict to be legally valid, the evidence must originate from official case documents.

6. The Judge's Discretion in the Admission of Digital Evidence

The admissibility of digital evidence is at the discretion of the criminal judge and depends on the prevailing evidence system (Makulilo, 2016; Prashant Bhadu, 2021). These systems include the Latin system and the Anglo-Saxon system:

A. The Latin System is a legal framework where the legislature doesn't specify the evidence and means of proof but rather leaves the freedom to the judge to establish their judgment according to their discretion without imposing any specific evidence on them. With the advancement of scientific and digital evidence, judges in this system have to deal with new kinds of evidence to discover crimes. As a result of this principle, the judge is not bound by the evidence presented by the parties to the case because they have the right to initiate themselves and take all measures in search of evidence necessary to form their conviction (Tatulych, 2020). To obtain digital evidence, the individual in charge, typically the criminal judge, can issue orders to the internet service provider. These orders may require the collection of information related to the websites that the accused person visited, the files and conversations in which they participated, as well as the messages they sent and received. Furthermore, the person in charge may instruct the system operator to provide them with the necessary details to access the system, which may include disclosing passwords and codes for various programs. They may also order an inspection of the computer in question. However, the criminal judge must ensure that any evidence they accept is valid and credible according to the relevant

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

laws before admitting it. Both Algerian and Egyptian legislations, in addition to French legislation, have adopted this system (Oparnica, 2016).

B. The Anglo-Saxon System is also known as the system of specific proof or the system of legal evidence. In this system, the legislator determines the evidence in advance and the judge is not allowed to deviate from it. Therefore, if the evidence is available for conditions that were specified and restricted by the legislator, the judge is obligated to establish his ruling even if the judge is not convinced. The evidence in this system is governed by two rules: The first is the rule of excluding hearing testimony, and the second is the rule of best evidence (Bierekoven, Bazin, & Kozlowski, 2014).

1. The rule of excluding hearing testimony states that it cannot be used as evidence if the witness who gave it only heard it and did not participate in its creation using any of their senses. Such testimony is usually collected outside the court and thus excluded from being used as evidence. However, there are some exceptions to this rule, especially when it comes to data and information obtained through a computer. The English judiciary has accepted this type of evidence on numerous occasions. For instance, the case of R v. Wood (1983) (Harvey, 2019) showed that direct evidence produced by a computer is not subject to the hearsay rule and can be accepted as direct testimony .

2. The rule of best evidence provides that the original of a writing, recording, or photograph is required to prove the contents thereof. In the United States, this rule has been approved as part of the Evidence Act ("Rule 1002. Requirement of the Original," n.d.), which allows electronic materials to receive the same recognition as other forms of evidence. Furthermore, the American legislator has gone a step further by stating that the writing inside an electronic device is similar to the original. This means that to copy it, the print output or any other output can be read, and if it accurately reflects the data, it is considered original data ("Rule 1003. Admissibility of Duplicates," n.d.). Therefore, electronic documents do not conflict with the rule of best evidence .

7. Conclusions and future work

Digital evidence is legally highly suitable to be used in criminal cases due to its strong probative value, despite being non-material evidence that can be easily concealed. However, using digital evidence in cases involving multiple countries can present a challenge due to conflicts in jurisdiction. The situation becomes even more complicated when the countries involved have different criminal justice systems, as each country will adhere to its judicial sovereignty. There is a need for technical expertise especially judges and investigators, in the field of justice due to the digital reality. Additionally, the Iraqi criminal system lacks legislative provisions for investigating digital crimes and handling digital evidence. Our research has focused on identifying the types, characteristics, and basic requirements of digital evidence. It is worth mentioning that the Iraqi criminal legislator has adopted the free evidence system in its penal approach, which is based on the Latin system .

We urge the Iraqi criminal legislature to update its system to accept digital evidence as original and reliable evidence that cannot be challenged except through illicit means (illegitimacy). We also recommend incorporating modern technical requirements into the Iraqi criminal system, specifically by creating a legal mechanism for investigation and collection procedures for analysing digital evidence. This is necessary to prevent digital criminals from acting with impunity.

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

8. Recommendations

Finally, we offer the Iraqi criminal legislature a number of suggestions, including:

A. Specify unequivocally and explicitly that digital evidence is considered authentic evidence in criminal proceedings, as well as the conditions and procedures that must be followed to guarantee that the authenticity of digital evidence is preserved in terms of how closely it resembles the original in the event of reproduction or retrieval. This will help to establish the evidence's validity before the criminal judge .

B. Focus on the preparation and qualification of digital (IT) expertise based on modern scientific (digital) methods in the field of digital forensic investigation. In this way, digital crime forensic investigation teams with technical (digital) competencies would be established to investigate digital (information) crimes and eventually collect digital evidence using state-of-the-art techniques that guarantee the achievement of justice .

C. Prepare digital awareness training programmes for individuals and institutions that use the Internet for their work, particularly for national security-related financial, scientific, and intelligence services. These programmes should teach participants how to update the protection systems used in their line of work and take the necessary precautions to protect their data and information systems .

D. Establish an efficient system for law enforcement agencies and internet service providers to collaborate digitally, both during the information collection process and when taking proactive steps to maintain the integrity of digital evidence .

References

- Articles

German, in Signatures Electronic .(2014) T. Kozlowski, & P., ,Bazin C., Bierekoven, French Electronic and Evidence Digital Perspective. Law Polish and French https://doi.org/10.14296/deeslr.v1i0.1719 .(0)1 Review, Law Signature

Extracting LogExtractor: .(2021) .Y Guan, & Z., N. Gong, C., Shi, C., C. C. Cheng, analysis. taint and string via messages log android from evidence digital .301193 ,37 Investigation, Digital International: Science Forensic https://doi.org/10.1016/j.fsidi.2021.301193

in log transaction server SQL of alysisan Forensic .(2023) S. Lee, & H., Choi, Digital International: Science Forensic system. file of area unallocated https://doi.org/10.1016/j.fsidi.2023.301605 .301605 ,46 Investigation,

digital the in recaptu media and journalism Investigative .(2021) S. Yang, & P., J. Choi, .100942 ,57 Policy, and Economics Information age. https://doi.org/10.1016/j.infoecopol.2021.100942

forensic digital to approaches Hybrid .(2017) B. Sams, & C., Collins, S., D. Dolliver, Digital context. utionalinstit an in analysis comparative A investigations: https://doi.org/10.1016/j.diin.2017.10.005 .137–124 ,23 Investigation,

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

Phone Your Microsoft's .(2021) M. Frade, & M., L. Andrade, P., Domingues, International: Science Forensic perspective. forensic digital a from environment https://doi.org/10.1016/j.fsidi.2021.301177 .301177 ,38 Investigation, alDigit

–6 ,(12)2003 Security, Network collection. evidence digital of Principles .(2003) D. Forte, 0-00006(03)4858-https://doi.org/10.1016/s1353 .7

Security, Network forensics. digital in searches text of importance The .(2004) D. Forte, 4-00067(04)4858-https://doi.org/10.1016/s1353 .15–13 ,(4)2004

Digital and Sciences Forensic in Research of Importance The .(2023) D. Franco, Sciences, icForens of Journal International Society. Contemporary in Forensics 16000336-https://doi.org/10.23880/ijfsc .2–1 ,(4)8

Electronic SSRN Issues. Some Admissibility: Evidence Digital .(2019) J. D. Harvey, https://doi.org/10.2139/ssrn.3505611 Published. Journal.

-front among recognition evidence ldigita Exploring .(2021) S. D. Dolliver, & T., Holt, Science Forensic scenes. crash fatal at officers enforcement law line .301167 ,37 Investigation, Digital International: https://doi.org/10.1016/j.fsidi.2021.301167

examinations. science forensic aldigit for strategies evidence Digital .(2023) G. Horsman, https://doi.org/10.1016/j.scijus.2022.11.004 .126–116 ,(1)63 Justice, & Science

detection activity irregular based-Context .(2023) C. Murphy, & S., Parkinson, S., Khan, Expert approach. mining itemset An investigations: forensic for logs event in .120991 ,233 Applications, with Systems https://doi.org/10.1016/j.eswa.2023.120991

rules new Tanzania: in evidence electronic of admissibility The .(2016) B. A. Makulilo, .(0)13 Review, Law Signature Electronic and Evidence Digital law. case and https://doi.org/10.14296/deeslr.v13i0.2302

Forensic .(2023) S. Baechler, & O., Ribaux, M., Bérubé, L., Cadola, M., Morelato, international An education: higher in learning and teaching intelligence .111575 ,344 International, Science Forensic approach. https://doi.org/10.1016/j.forsciint.2023.111575

Evidence Digital education. forensic digital and evidence Digital .(2016) G. Oparnica, .(0)13 Review, Law Signature Electronic and https://doi.org/10.14296/deeslr.v13i0.2305

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

audio handling for approach forensics Digital .(2023) N. lamani,Vad & M., S. Pedapudi, .100860 ,29 Sensors, Measurement: files. video and https://doi.org/10.1016/j.measen.2023.100860

An Evidence: Digital Of Perplexity And Admissibility .(2021) Bhadu. Prashant .20–10 IV),)5 Development, searchRe Legal Overview. https://doi.org/10.53724/lrd/v5n4.03

.(2023) J. Sheppard, & N.,-J. Hilgert, C., Hargreaves, F., Breitinger, M., Scanlon, the and bad, the good, The investigation: forensic digital for ChatGPT .301609 ,46 Investigation, Digital rnational:Inte Science Forensic unknown. https://doi.org/10.1016/j.fsidi.2023.301609

.(2023) S. Krajči, & K., Kováčová, E., Marková, O., Krídlo, Ľ., Antoni, P., Sokol, relationships. evidence digital understand to approach analysis concept Formal .108940 ,159 Reasoning, Approximate of Journal rnationalInte https://doi.org/10.1016/j.ijar.2023.108940

the in Addresses IP .(2020) J. Harašta, & K., Lučivjanská, L., Rózenfeldová, P., Sokol, Slovak eth of Law Case Civil and Criminal the in Evidence Digital of Context .300918 ,32 Investigation, Digital International: Science Forensic Republic. https://doi.org/10.1016/j.fsidi.2020.300918

digital for framework conceptual a as trial fair a to right The .(2023) R. Stoykova, ,49 Review, Security & Law Computer .investigations criminal in rules evidence https://doi.org/10.1016/j.clsr.2023.105801 .105801

Law proceedings. civil in evidence of means a as evidence Electronic .(2020) I. Tatulych, -g/10.36695/2219https://doi.or .219–215 ,1 Law, of University Kyiv of Review 5521.1.2020.43

Webpages

from Retrieved n.d.).) Original. the of Requirement .1002 Rule https://www.law.cornell.edu/rules/fre/rule_1002

from Retrieved n.d.).) Duplicates. of Admissibility .1003 Rule

https://www.law.cornell.edu/rules/fre/rule_1003

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

ڕەسەنایەتی بەڵگەی دیجیتاڵی لە سیستەمی دادوەری تاوانکاریدا
"ڕوانگەی یاسای تاوانکاری لاتینی و ئەنگلۆساکسۆن"

دکتۆر ڤەهیل عبدالباسط عبدالکریم
بەشی کارگێڕی یاسایی، کۆلێژی تەکنیکی کارگێڕی، زانکۆی پۆلیتەکنیکی دهۆک، دهۆک، هەرێمی کوردستان، عێراق
ئیمێل: fahil.abdulbasit@dpu.edu.krd

پوختە

ئێستا، سیستەمی دادوەری تاوانکاری لە ئەنجامی پەرەسەندنی ئینتەرنێت و بەکارهێنانی بەربڵاوی سیستەمی زانیاری ڕووبەڕووی کێشەی بەرچاوی ڕێکار و جەوهەری دەبێتەوە. بەو پێیەی بەڵگەی دیجیتاڵی بەڵگەی زانستی تەکنەلۆژییە کە فرێدانی مەحاڵە و دووبارە دەکرێتەوە، چەندین سوودی هەیە. سەبارەت بە بەهای سەلماندنی بەڵگەکان، دادوەری تاوان دەسەڵاتێکی بەرچاوی هەیە لە کاتی هەڵسەنگاندنی بەڵگە دیجیتاڵییەکان. دەبێت سێ مەرج جێبەجێ بکرێت بۆ ئەوەی بەڵگەی دیجیتاڵی لە دادگادا وەربگیرێت: شەرعیەتی بەڵگەکان، پلەی دڵنیایی دادوەر و باسی بەڵگەکان. چوارچێوەی یاسایی ئێستا توانای دادوەر بۆ وەرگرتنی بەڵگەی دیجیتاڵی دیاری دەکات. سیستەمی لاتینی کە بە سیستەمی بەڵگەی ئازادیش ناودەبرێت و سیستەمی ئەنگلۆساکسۆن کە زۆرجار پێی دەوترێت سیستەمی بەڵگەی سنووردار، دوو سیستەمی یاسایی سەرەتایین. گرنگی لێکۆڵینەوەکە لەوەوە سەرچاوەی گرتووە کە زۆرێک لە تاوانەکان بە سروشتی دیجیتاڵی ناتوانرێت دەستنیشان بکرێن یان بسەلمێنرێن بە بەکارهێنانی یاسا تاوانکارییە تەقلیدییەکان لە سیستەمی تاوانەکانی عێراقدا، هاوکات لێکۆڵینەوە لە بەڵگە دیجیتاڵییەکان دەستپێکردووە بۆ جێگرەوە و ڕۆڵ بینین لە بەڵگەی تاوان لە ئاستی جیهانیدا بە مەبەستی کۆنترۆڵکردنی تاوانەکان و ڕێگریکردن لە بڕ سزایی تاوانباران. بۆیە بە خستنەڕووی چوارچێوەی یاسایی ڕەسەنایەتی بەڵگە دیجیتاڵییەکان لە ڕوانگەیەکی لاتینی و ئەنگلۆساکسۆنەوە، پاشخانی توێژینەوەکە لە هاوتابوونی لەگەڵ پێشکەوتنە یاساییە تاوانکارییە جیهانییەکان لە بواری تەکنۆ-یاساییدا سەرچاوە دەگرێت. تەحەدای توێژینەوەکە بریتییە لە بەکارهێنانی شێوازی وەسفکردن و شیکاری بۆ ڕوونکردنەوەی بەهای سەلماندنی بەڵگەی دیجیتاڵی لە پەیوەندی لەگەڵ بەڵگەی تاوانکاریدا.

کلیلە ووشەکان: بەڵگەی دیجیتاڵی، سیستەمی دادوەری تاوانکاری، تاوانناسی ئەلگۆریتم، دیموکراسی دادپەروەری، سیستەمی دادوەری تاوانکاری عێراق

ISSN-Print: 2079-3901
ISSN-Online: 3005-396X

حُجِّية الدليل الرَّقْمِيّ في نِظَامِ العَدَالَةِ الجِنَائِيةِ
" وِجْهَاتِ نَظَرِ الْقَانُون الْجِنَائِيّ الْأَنْجُلُو- سَاكْسُونِيّ وَاللَّاتِينِي"

الدكتور فهيل عبدالباسط عبدالكريم
قسم الإدارة القانونية، الكلية التقنية الإدارية، جامعة دهوك التقنية، دهوك، إقليم كردستان العراق
البريد الالكتروني: fahil.abdulbasit@dpu.edu.krd

ملخص

حاليا، يواجه نظام العدالة الجنائية قضايا إجرائية وموضوعية كبيرة نتيجة لتطور الإنترنت والاستخدام الواسع النطاق لأنظمة المعلومات. وبما أن الدليل الرقمي هو دليل علمي تقني من المستحيل التخلص منه، حيث يمكن طبعه مجددا، فإنه تقدم كثير من الفوائد فيما يتعلق بالقيمة الثبوتية للأدلة، وبذلك يتمتع القاضي الجنائي بسلطة كبيرة عند تقييم الأدلة الرقمية. بوجهٍ عام يجب استيفاء ثلاثة شروط لقبول الأدلة الرقمية في المحكمة: شرعية الدليل، ودرجة يقين القاضي، ومناقشة الدليل. يحدد الإطار القانوني القائم في الدولة قدرة القاضي على قبول الأدلة الرقمية. النظام اللاتيني، المسمى أيضًا بنظام الدليل الحر، والنظام الأنجلو- ساكسوني، المسمى غالبًا بنظام الدليل المقيد، هما النظامان القانونيان الأساسيان. تنبع أهمية الدراسة من حقيقة مفادها أن كثيراً من الجرائم ذات الطبيعة الرقمية لا يمكن اكتشافها أو إثباتها باستخدام القوانين الجنائية التقليدية في النظام الجنائي العراقي الحالي، في حين بدأت دراسة الأدلة الرقمية تحل محل الأدلة الجنائية التقليدية، وتؤدي دورًا عالميًا من أجل السيطرة على الجرائم ومنع الجناة من الإفلات من العقاب. لذلك، من خلال تقديم الإطار القانوني لحجية الدليل الرقمي من منظور لاتيني وأنجلو- ساكسوني، تنبع خلفية البحث من توافقه مع التقدم التشريعي الجنائي العالمي في المجال التقني-القانوني. ويتمثل التحدي الذي يواجهه البحث في استخدام الأساليب الوصفية والتحليلية لشرح القيمة الثبوتية للدليل الرقمي في نظام العدالة الجنائية.

الكلمات المفتاحية: الدليل الرقمي، نظام العدالة الجنائية، علم الإجرام الخوارزمي، ديمقراطية العدالة، نظام العدالة الجنائية العراقي