Journal of Law, Policy and Globalization
ISSN 2224-3240 (Paper) ISSN 2224-3259 (Online)
Vol.54, 2016

Knowledge and How It Helps in Validating Cyber Crime

Ali Al – Zubi * Ahmed Al_Nuemat *
Department of law, Al-Balqa Applied University, Al-Salt, Jordan, P.O. Box: Al-Salt 19117

Abstract

The internet has been subjected to cyber crime because it is hard to detect where the offense was instigated, and this is ascribed to the class and features of the data presented by the computer, official substances, which are usually vague due to the possibility of the information being corrupted and concealed. These official substances add to the difficulty of the proof of the committed cyber crime which cannot be validated just by capability, which contradicts the official command that, "the proof in offensive situations by all procedures of collecting evidence." Establishing cyber crime with the help of official knowledge is very hard, as the information and proof available is usually uncertain, unconvincing and hard to tell if real or fake. This is because of the uncertainty of the proofs involved, as there is always a chance of them being interfered, so that they are unable to offer any real data regarding the matter so no serious steps can be taken. Thus, this uncertainty encourages the suspect which is because of the official grounds according to which the law of board magistrate must be by private assurance, depending on undisputed testimony, and that the board requirements are dependent on declaration and inevitability, instead of uncertainty and estimation.

Introduction

This study makes it an objective of elucidating the suitable official progression to certify the cyber crime, and deliberate some of the issues that harm the chance of demonstrating cyber crime, and exposed the individuality of the executor, these issues might be official as rule and law, and technical subjects may cause issues and hindrances in the way of examining these type of offences. Thus, the procedure of this study aims to explain the practical subjects concerned with cyber crime and the part played by these offenders as proof, throughout the distribution, employing texts, official codes and legal clarifications of pertinent and assertive in the area concerned with the evidence in offensive situations.

This study is separated into three parts; the first part involves of an overview of the cyber crime laws in Jordan and exemplifies the common official and customary subjects that are confronted when trying to establish cyber crime and to trail the offenders. The second part on the other hand, involves of an explanation of how to verify cyber crime, with the help of employment and distribution of scripts and official laws and clarifications concerned with confirming the offenders. Part three concentrates on the topic of evidence in the offending cases, and the part played by the board judge in this division, and the most noticeable characteristics of this case, the suitable opinion of the judge and the limitations linked with this verdict. It also concerns with the proof available in situations involving of cyber crime with the help of specialized skill, the significance of capability, and the efficiency of proficiency in evidencing cyber crime in case of incorruptibility and procedural subjects backed with evidence.

The main motive behind selecting the topic "Knowledge and its part in proving cyber crime" for this study, is due to the fact that the Cyber Crime Law No. 27 of 2015[1], that exchanged the provisional Act of information systems crime No.30 for the year 2010, is a new addition to the Hashemite Kingdom of Jordan, as there are numerous queries regarding the evidence against cyber crime with the lack of laws in this division, alongside the lack of Jordanian cassation court determinations in such cases. This will help subsidize the elimination of doubt concerned with those queries and supplement the technical and official understanding to verify cyber crime.

First Part: Jordanian Cyber Crimes Law

Internet is a fictional world that enables to connect more than just an information system so as to offer information and statistics. Considering the significance of the Internet in the current age and the enhanced movement of people on this system, the attitude and the actions of the consumers of Internet did not dodge a rule, where some of the laws in the cyber crimes law No 27 of 2015 were organized, that control the actions and attitude of the internet system consumers and defends the rest from the actions that cause cyber offence on the Internet. [2]

It was explained that the offences committed over the Internet that make up the Cyber Crimes Laws, that force punishments on the offenders, access without permission or infringement, or surpassing approval so as to

[1] Jordan Cyber Crimes Law No. 27 Year 2015.
[2] Ibid., Article 3.

cancel or delete, add, obliterate, reveal, indistinct, alter, transform, move, copy or inactivate information, statistics or data on networking sites.[1] The crimes concerned with eavesdropping, obstruction, alteration of the sender of information,[2] actions linked with sexual development, acceptability, advertising of prostitution, and actions associated with slander, malign and abuse being deliberately used without certification or disruption,[3] or Authorization to surpass the data network or system in some way so as to acquire information or statistics that are inaccessible to the community,[4] which influences the national refuge or international associations of the Kingdom, communal security or the domestic economy and similar offences.[5] These offences performed over the Internet came to an agreement with the board fundamentalism base, which signifies that there is no offence and its sentence without there being an official specification of the offensive acts committed.[6]

The extremely significant characteristic of the cyber crime law is that it is passed up to the official police after gaining the authorization of the district attorney or the court, admission to anywhere signs are applied to compel any of the offences specified in this Law, as the same law sanctioned to the official police examination hardware, tools, software, operating systems, network information and the channels through which the proofs can be collected against the offence performed, that in all situations, the worker who has to establish the examination documentation in this respect and propose it to the capable district attorney.[7] The electronic crimes law also gave official permission to the district police to confiscate the items, objects, tools, equipment, systems, networking data and the channels employed by the offenders to commit that particular crime and the finances acquired from them, arrangement data and information concerned with the instruction of any of them.[8] The electronic crimes law also specified to the court to seize the devices, equipment, substances and detain the work, data or site associated with the crime performed by the offender that fall under this law, the finances obtained from this crimes to also be captured, and the court to have the power to eliminate the defilement on the criminal's behalf. [9]

Lastly, the Jordanian cyber crime law notifies the variance in the interests of laws and regulations regarding the actions performed somewhere away from the Kingdom, but its influence proceeds inside the Hashemite Kingdom of Jordan, as it is expressed by this law that the communal interest and private rights are considered and are brought before the Jordanian courts, in case you have performed any offence that is mentioned in this law, by employing information systems inside the Kingdom, helped in disrupting any part or individual of this area, or any of this happened from the impact of your offence thoroughly or in fragments, or if performed by any of the inhabitants of that area.[10]

1- Laws Conflict and Jurisdiction

The relevant competence law and regulation of the main lawful substance that associated with the cyber crimes performed by the offenders on the internet particularly when they are performing these offences outside the kingdom or with the help of a system which is situated outside the kingdom. These subjects raise concerns about the local courts situated inside the kingdom having legal authority to handle disagreements that are linked with these offenses, also regulating which laws should be implemented to these offences. It should be observed that the Jordanian cyber crime law only notifies the concerns of laws and authority regarding the offences performed outside the kingdom, with them impacting the area inside the kingdom too, as is claimed by this law, that he considered the communal interest and private rights on the claimant at Jordanian courts, in case you have performed any offence that is specified in this law, by employing information systems inside the Kingdom, helped in disrupting any part or individual of this area, or any of this happened from the impact of your offence thoroughly or in fragments, or if performed by any of the inhabitants of that area. Hence, any individual who is affected by a cyber crime performed outside the kingdom, has the authority to determine a communal interest lawsuit and personal right before the capable Jordanian courts are experienced in such offences. [11]

---

[1] Ibid., Article 5.
[2] Ibid., Article 9-10.
[3] Ibid., Article 11.
[4] Ibid., Article 12.
[5] Ibid., Article 4-6,7-8,14-16.
[6] See Cassation Court Decision, Act Number 430/1997, 17/8/1997.
[7] Jordan Cyber Crimes Law No. 27 Year 2015, Article 13/ A.
[8] Ibid., Article 13/B.
[9] Ibid., Article 13/C.
[10] Ibid., Article 17.
[11] Christopher Hooper, Ben Martini, Kim-Kwang and Raymond Choo, 'Cloud Computing and its Implications for Cyber Crime Investigations in Australia' (2013) 29(2) Computer Law & Security Review 152.

The type of the computing assistance system permitted to implement actions from all over the world and no uncertainty of the probability of performing internet offence with the help of this system from outside the kingdom and this raises concerns associated with authority and the official evidence and the application of legal choices in the countries that have been involved in the crime. Even though the law to the concern of legality that these offences affected the kingdom as stated by Article 17 of the law, the difficulty of implementing the conditions of these courts outside the kingdom may make these conditions a custom as the application of international, laws could form an expansion of regional legality of the overseas courts. For instance, the Lucas film Ltd v Ainsworth situation was handled after the Supreme court in England determined that the disruption of logical stuff, rights by Internet from somewhere out of England does not cause a local expansion of the power of the courts of the country which supported the person that performed that offence. Other concerns that oppose the regulations of the states, because of the variances existing between the law system, there is a chance that the a specific act is considered as an offence in the country that is subjected to endure the effects of the crime, but the country that the offence is committed it, does not consider the act as an offence, for whatever reason, like the lack of a permissible transcript.[1]

The difference between the laws and regulations cannot be avoided when discussing cyber offences, the internet users apply some assistance or system in the digital world, where accessible, like enabling the work from outside the geographical site where the system is placed, that offers these assistances. It usually exists outside the regulation of the country, not just outside its conditions, where the user is working. Also, the system of the supplier of the processing assistance must be situated in more than one geographical division in one time, which would cause official concern regarding the security of the consumer availing this assistance. Thus, the consciousness of the global society has become obvious due to the trouble offered by the examination in the electronic offences performed online as the aptitude to compel from other states. With respect to this, it has pursued associates of the global society to accomplish polygonal contracts to improve collaboration between these associates to battle internet offence, like the Convention on cyber crime specifies that there is a requirement for collaboration between countries and the private divisions in order to confront the cyber crime and the requirement to shield genuine concerns when using and improving the information technology. [2]

2- Problems Confronted when Exploring Internet Offences

The laws and regulations may evade or restrict the capability to examine the cyber crime, along with the substantial stowage of the information on the systems of the new assistance in the world of electronic devices, which makes this study harder due to the impracticality of classifying digital proof.[3] For instance, the calculation on the concept of stowing information, statistics and functioning requests to the system without the requirement of a particular position for the procedure of stowing in systems that can provide assistance that is situated outside the area of the kingdom, which constraints the capacity to examine the unlawful actions developing from the use of processing, even if such information and statistics is saved on systems situated inside the area of the kingdom and the class of processing expertise causes problems in examination for dispersing and stowing this information on a number of mechanisms.

The actual contest for the cyber crime examination is to search for the precise data that they require, since it is not as easy as it may appear, to recognize the offender in the inquiries being made regarding the Internet. This is hard in case of the crimes committed over the internet because the processing assistance deliverers are firms that are normally situated in other countries, rather than the same one as the consumer exists in. Hence, assistance deliverers are to accomplish the agreements with the consumers, to control the appropriate law and regulation in case of any arguments regarding the utilization of this assistance provider like the storage and utilization of the information and confidentiality , that these arrangements tackle the concerns of academic property rights in association with the information and statistics, that are saved in the computer system by the consumers, as these contracts provide the assistance providers with benefits regarding the use of the saved data and statistics on processing.[4] For instance, if the annual record of Facebook illustrates that the Jordanian government requested data three times in the year 2014, for the duration of one month (7) and (12) on the offences performed on Facebook, but the firm only reacted to them only once by sending one request. The firm accountable for Facebook site specified that they react to only the requests that are concerned with misconduct

[1] David W. Chadwick and Kaniz Fatema, ' A Privacy Preserving Authorization System for the Cloud' (2012) 78(5) Journal of Computer and System Sciences 1359.
[2] Convention on Cyber Crime, opened for signature 23 November 2011 (entered into force 1 July 2004).
[3] Christopher Hooper, note 13 above.
[4] Da-Yu Kao and Shiuh-Jeng Wang, "The IP Address and Time in Cyber-Crime Investigation (2009) 32(2) *Policing: An International Journal of Police Strategies & Management* 194.

and that each request is checked against the appropriateness of the official explanation for such an application and there is a good chance that this application might be ignored, the applicant needs to deliver the matter and things that support it alongside.[1]

Second Part: Proof in Criminal Cases

The official explanation of proof or evidence is the validation of the crime committed, it is gathered to prove the violation of the law, which help to figure out if the offence was actually committed or not and allocated to the respondent or release.[2] The verification could be viewed on the measures and processes performed by the Public Prosecutor's Office and its supplementary forms after the committed offence is reviewed and the proof is collected, reviewed and initial study is performed so as to demonstrate the offence committed by the respondent or emission, taking into consideration that the proof being accumulated in the numerous phases of offence reports are the grounds where the judge is persuaded with the probability of the performed offence, and the offender is accused of the crime committed by him.[3]

The obtain ability and presentation of the proof in front of the board of the judges in a specific case ascertains and strengthens his sentence in the supervision of justice and the penalty of the criminal, this cannot reflect without the proof and measures that certify the offences committed, which is the associated with the offender who is presented in front of the judge, where the proof is examined with the help of the study performed and the search of the reality in all real ways, where originating proof from the genuine proof denotes that the accessible components help determine the offence and the situation around them to commit and how it could be applicable on the offender, thus the evidence of the offence and evidence collected alongside it, is essential. Or else, the criminal is known to get away without getting punished for his acts.[4]

This part of the study will concentrate on the subject of evidence which is normally gathered against an offence, and collect the laws and rules concerned with the digital offences, that the main motive behind this tendency is that the law of the digital offences in Jordan is a new law, which is because of the lack of expert suppliers and legal views on this subject. While the unsettled troubles that will be adopted in this respect is to attain appropriate official route on the basis of cyber crime, the kind of proof that can appear as a testimony of conviction in contradiction of the alleged indication, along with elucidating the official and practical ambiguities that can be manipulated to exemption on the cyber crimes performed.

1- the part played by the judge in the way of proof of the offence

In offensive situations, the proof accumulated to support the offences, breaches and infringements by all ways of evidences and the part played by the judge by giving his own private opinion and if the law text regarding a specific matter is followed and in case the proof does not appear then the judge gives the verdict to release the alleged defendant of the crime that he was being held accountable for. Hence, the trail court has the legitimate power and authority to follow the requirements of Article 147 of the Criminal Procedure Code devoid of the restriction in the Court of Cassation, providing the discoveries made from the official confirmation offered in the situation and abstract them acceptably, specifically because the judge in offensive situations are dominated by private opinion and he may morally consider the proof and not inquire anyone else.

Even though the legality of the board judge in establishing his own opinion based on ethical proof, but not all of the proof is acceptable for this reason. The proof should be linked to the crime supposedly committed and be according to the rule of doubt and should elucidate the actions of the defendant instead of stating his guiltlessness against the blames pinned on him regarding the offence. This tendency is in accordance with the rule that claims that severe conditions must be made on the declaration of inevitability and not of disbelieve and deduction.[5]

The Court of Cassation once stated that the trial court under Article 147 of the Criminal Procedure [6]is completely free to take whatever verdict through proof and leave all the rest without accuser by the Court of

[1] Denis Reilly, Chris Wren & Tom Berry. 'Cloud Computing: Pros and cons for computer forensic Investigation' (2011) 1(1) *International Journal Multimedia and Image Processing* 26.
[2] Christopher Hooper, note 13 above.
[3] Gvernment Requests Report, Jordan July 2014 -December 2014, accessed 23rd August 2016, https://govtrequests .facebook.com/country/Jordan/ 2014-H2/#
[4] *Ibid.*
[5] Mohammed al-Halabi, The Mediator in Explaining Criminal Procedure Code, Part II, P. 266.
[6] Code of Criminal Procedure No. 9 Year 1961, Article 147.

Cassation in such essential concerns, providing the result acquired was agreeable and satisfactory, with the desire to leave and not to consider it as grounding on proof, which manages the sensible uncertainty to subsidize the hesitation, clarifies the detail that the suspect penal establishments should be based on the conviction, instead of the estimation, and there should be no uncertainty regarding the association of the suspect with the offence he is being held accountable against, which in the end demands statement of innocence, which is given to him by the charges placed against him. [1]

Similarly, the jib of the penal judge is to confirm the reality with the help of his judgement, taking into consideration the proof presented and taking the solid proof that arose from the stipulations, as the penal judge is required to demonstrate the reality that must be backed with solid proof, and should be clear. Therefore, the penal judges dependent on the independence of the judge in evaluating the proof in the trails and examining them, in case he fails to be persuaded and is not comforted, he may put it before the panel and seek help from others, which is then again, dependent on his belief to express the motive behind the crime committed by him, as this is thoroughly based on the persistence without restriction, provided that it is acceptable to express the disadvantages of consuming, which is not corrupted by the verdict established. [2]

Conclusively, the judge in the penal events ruled by the private sentence constructed as stated by the proof and ignore everything else on the condition that the conclusion gained was agreeable and satisfactory, and that the proof that was presented had no hint of uncertainty, as the uncertainty elucidates the significance of the suspect that the penal conditions should maintain the declaration of inevitability and not doubt and estimation. Appropriately, the assurance of the illegal court that the offender is the one who performed the crime on the internet endorsed to him which must be dependent on the official proof which should not have any sign of doubt, as the doubt and uncertainty works to help the suspect, which demanded him to fulfil his duty which cleared him of all the things he was held responsible for.

2- Burden of Proof in Criminal Offenses

Normally, the weight of evidence in offensive situations is at the district attorney, whereas the trial judge in penal cases implemented his widespread foresight to expose the reality and form equilibrium between proofs. The General Prosecutor's Office and its figures commended to examine offences and gather proof consistent with Article seven of the Code of Criminal Procedure with the help of exploratory processes and gathering information and review the offensive situation, along with the district attorney to the initial attorney to take the necessary measures to guarantee capture, examination and call upon the witnesses that attest the case. [3]

In case of the offender, it is trusted to form proof regarding the shortage of the charge of the crime of the one that is held to demonstrate his innocence against the offences that he is held responsible for, as the incorruptibility supposition and sentence must be documented, contingent on the base and the official belief that the criminal is blameless until proved to be responsible, it monitors, the district attorney is held responsible for verifying a sentence. But this does not pardon the charge on the offender to disapprove the proof that the district attorney handed to the court and deliberated it before deciding that it was fake, and that regardless of depending on the evidence to prove his innocence, but he is qualified to appeal to the court with proof that refers to his incorruptibility of performing a said offence and refutation against the blame of performing the offence.[4] Also the fact that the accuser had to be denied the validity and cogency of all accounts connecting to the proof, performances and details of the examination by the district attorney is considering the illegitimacy of the declarations gained whilst under pressure and the inaccuracy of examination processes and shortage of validity, along with the imprecision of affirmations which have been arranged by the digital equipment pursuers, to the general action, and the detail that it is not controlled inside the restrictions of practical and spatial authority, as either it does not fulfil the formal hand or it was performed by a worker who was not an expert. [5]

Incidentally, the penal judge perform inspection of the proof provided by the district attorney and untangle the secrecy of the offence and then the determination dispensed to convict the offender or assert his virtue of the accusations filed against him, as they consider the proof offered whose appropriateness is on the criminal judge

[1] See Cassation Court Decision, Act Number 48/2015, 1/2015.See also 2159/2014,2175/2014,2149/2014.
[2] Mohammed al-Halabi, note 22 above, P. 267.
[3] *Ibid,* P.268.
[4] *Ibid*, 269.
[5] *Ibid*, 272.

to prove, this proof as legality not withstanding any other matters, as he has the authority to contest illegal data or proof acquired from unlawful ways, it is similar with the law that conditions that an opinion of the penal judge must be dependent on the declaration and inevitability, instead of uncertainty and guesswork, the proof that has even the slightest flaw cannot be considered as the grounds to base the final verdict on. [1]

Therefore, the authority of giving a final verdict based on the proof is in the hands of the trail judge in case of an offence against the suspect, while the judge is examining the investigation file, which is proved and verified by the proof, and gives a review of the legality and genuineness of the case, along with deliberating the resistances provided by the suspect, and also the last inspection with no interference of the district attorney or anyone else, and is only persuaded by the proof offered, it is entirely up to him to consider or ignore them, but in case of an uncertainty, there is a need to present and take word of the spectators, and the identification of the suspect in front of the district police, and excusing him, and when the judge is assured of the proof available in the investigation file, he can depend on it, and base his final decision on the evidence and data inside the file, in the best way to prove that the suspect did actually perform that particular offence.[2]

Thus if the suspect or offender of cyber crime finds it expensive to demonstrate his virtue due to the fact that the supposition and belief of virtue must be documented, as there is an official law that states that the suspect is guiltless until proven otherwise, which is taken further and the district attorney or the accuser are allotted the right to give a private opinion to prove someone accountable. Stress should be laid on the offender to disprove the proof brought forward by the district attorney and submitted to the court and deliberated if it was fake and that regardless of grounding the offender on the assumption of incorruptibility, but he is qualified to appeal to the court with proof that refers to his incorruptibility of performing a said offence and refutation against the blame of performing the offence.[3]

3- Limitations That Are Based on Verdict of Penal Judge

The subject of approval of proof by the penal judge is of great significance and is outside the control of the Court of Cassation that its part is restricted to the implementation of the law material, and this evaluation should be gained after the fixed inevitable conviction depending on the proof before the penal judge along with the proof held in the case file, which may be restricted to the part of the judge to assess and test proof offered by the charges, but when the judge starts to examine the proofs in the file, it should be known that the penal judge appreciates caution, and should be able to persuade the judge after offering proofs that are approved by the law, as the supplies acquired the declaration of inevitability and not grounding on the doubt, deduction, estimation or clarification.[4]

Regardless of the cautiousness of the panel judge, the admiration of proof and statement are placed by a few limitations, as some evidence are taken into consideration, while the rest have to be produced on conventional grounds, and on appropriate bases by stressing the truths of the situation evidently, by trusting on the unsure proof decisively, as the verdict of a sentence is not produced only on the conviction of the resolution.[5] When the proof is not according to the demands of the judge, he fails to discover the truth due to the uncertain facts present in it, it is this doubt that expresses to be beneficial for the suspect instead of his statement of innocence for the crime that he was being held responsible against, or else the final declaration was considered to be faulty.[6] The verdict should also be dependent on the rock-hard evidence offered in between the trails which was done to convict the suspect out in the open, and that this proof should be acceptable and inside the outline sketched by the mind, should be wise and in order, and it should also be kept in mind that it cannot only be that the verdict of the penal judge was based on fake information, as all that is produced on fake data is untrue, particularly in case of a sentence where it is probable to be a statement of incorruptibility grounding on the proof made for a wrong decision that is against the law, this proof of the judge giving his verdict on untrue proof should be proof enough to be presented in front of the judge in the trail as the judge cannot be held accountable on his personal data. [7]

Depending on what has been going on, the source and the community demonstrate that the penal judge gave

[1] *Ibid*, 274.
[2] *Ibid*, 277.
[3] *Ibid*, 278.
[4] *Ibid*, 279.
[5] *Ibid*, 280.
[6] *Ibid*, 282.
[7] *Ibid*, 285.

his verdicts governing on the independence of sentence given, but there are some exemptions to this concept, as they confine the independence of the judge in the sentence, thus, the sentence of the judge is not always independent because of the acknowledgement of specific limits on it.[1] One restriction, confines the judge in ways that constrain the evidence provided regarding the non-offensive materials, where it is considered in offensive issues as holding all the proof required, according to Article 147 of the Code of Criminal Procedure, there is also a requirement to have specific proof to charge the suspect, like when the law necessitates particular evidence, you must abide by it.[2]

Therefore, the statement of the Criminal Court of holding the suspect responsible against the cyber crime allegedly committed by him, which should be created on some permissible proof which must be free of any doubt, as the uncertainty benefits the suspect, and impulses the verdict to be not guilty, against whatever he was held accountable for, by the illegal actions he performed. And then there is the weight of verifying that the suspect is the same individual who performed that crime, and is lying to the district attorney, as it is his duty to prove the suspect as not guilty, which is already assumed, but the sentence must be reassured by the lawful proofs which claim the suspect to be blameless until proven otherwise. The penal judge appreciates caution, and should be able to persuade the judge after offering proofs that are approved by the law, as the supplies acquired the declaration of inevitability and not grounding on the doubt, deduction, estimation or clarification. Hence, the standards that consider the uncertainty and estimation in the proof should be deliberated, which is one of the many restrain registered on the optional authority allotted to the judge of the criminal based on the proof and approval of the hard proof, as the presentation of the particular proof and request other to create and record satisfactory basis and sensible motives, by stressing the evidences of the case undoubtedly and unmistakably, by depending on doubtful verdict, as the verdict of the sentence or virtue can only be maintained on the inevitability of the conclusive sentence. When the proof is not according to the demands of the judge, he fails to discover the truth due to the uncertain facts present in it, it is this doubt that expresses to be beneficial for the suspect instead of his statement of innocence for the crime that he was being held responsible against, or else the final declaration was considered to be faulty, it is lawfully intolerable to sentence the suspect of performing a cyber-offense by employing digital devices that are uncertain, and it is hard to regulate if the presented proof is real or devised, and this is because of the unsteady electronic information that cannot be trusted or is not appropriate enough to offer data that can be depended on when sentencing someone in the courts.

Third Part: Evidence Regarding Cyber Crime with Help of Skill

This part deliberates the fact that the cyber crime is one of the offences that cannot be validated by practical proficiency. This problem is confronted when the suspect does not admit to his crimes that he committed on the internet, but if the suspect admits to his crimes, there is no explanation to further analyse the situation cause that is all the acceptance that the court requires.

As the acceptance in illegal subjects is an component of deduction which the trial court has the independence to evaluate the right and worth of the proof providing it obeys the fact and actuality, and that the argument protects the rationality of this gratitude is an impartial disagreement against the trial court in evaluating the proof of the case, which may not be discussed or deleted of the proof by the Court of Cassation, provided the judge has declared the truth and the proof has no uncertainty issues, and there is also a probability that her court planned to not acquire professional to form a verdict.[3]

1- **Mechanical Skill and Its Significance**

Knowledge is considered in technical science understanding, a technical way that the court assumes to choose this way where a technical clarification is required to reveal the hidden truth and secrecy, and the experiences of the experts in this area helps the situation with their widespread understanding of the case which is associated with the subjects of arts and sciences, where one of those experts is employed to plan on the mechanical problems that are a part of the case, to figure out what their experience says about the case, the logic is required more than anything else, so as to complete the data required by the judge on problems that the judge has no understanding of.

2- **Knowledge in Examination and Interpretation Initial Examination**

The Jordanian penal provision law handles the knowledge as the process with which to demonstrate the initial examination in the Articles 39-41 phase, where Article 39 denotes the biased class of the crime and the

[1] *Ibid*, 286.
[2] Da-Yu Kao and Shiuh-Jeng Wang, note 17 above.
[3] See Cassation Court Decision, Act Number 258/1993 on 11/1993

situations that include subjects like Arts or Trade, which makes the General Attorney involve one or more experts of the art and workmanship. Depending on this, the inspection experts must look for the services of the knowledgeable, particularly in cases which are based on the crimes that can only be sentenced after the understanding of Arts and Trades help solve them.

In the stage of inspection, the information concerned with the offence and its discovery must be gathered, like where it happened and such, and its collateral damage too, like what and where the crime impacted, and as a result of this study, the suspect should be seized, where the District Police should take charge under the order of the Attorney General, this phase further stretches to the phases that were obeyed until the last order is passed to explain some of the uncertainties, the inspections, and the analysis, which are very significant phases of the offensive events, which make up the ground for other phases. The Attorney General should set himself to the task of questioning the suspect, confiscating the devices employed by the suspect when committing the crime, and look into his house for other items that are believed to expose the reality, and also preserve the papers that provisions the crime and help manage the record. The Attorney General also looks into trails and acquires criticisms and records, and also has the authority to stop any individual who was found in the place where the crime was committed, and the Article 53 of the Code of Criminal Procedures claims that the Attorney General should be capable enough to handle the objections reported to him. The Attorney General should also admit the claimant, the suspect and their representatives when performing the initial inspection, and has the right to perform the inspection all alone. Hence, this phase helps classify the components of the offence and form the character statement of the criminal from the situations, settings, doubt report and the accumulated proof.

The inspection and analysis is the most significant stage if the trails of the offender, that cover the track for the illegal lawsuit, to accumulate influences and physical proof of the illicit actions, and take actions that help reveal the situations of the offence and figure out the settings and reasons behind the commitment of the crime, to help the inspection operations and to refrain the offenders from bolting and absconding and seize them before they do. The District Police succeeds when their expertise help capture and uncover the offence, seizes the individuals who have offensive characteristics before they unleash their qualities who only do not perform those offences with the fear of getting caught in the act, such individuals should be stopped, captured and punished, this is what helps stop the crimes and to ensure safety and steadiness. The district police also help emotionally and indirectly to battle against the fraud and discovery, also cornering the criminals and getting them punished. [1]

The authenticity and legality of a criminal procedure in a court of law is often indicated by the extent of information obtained during the proceedings, and shared before the audience. Correspondingly, the importance of the investigation carried out in this regard can seldom be impressed enough to the degree and required extent, considering how this is amongst the preliminary processes to convict a criminal and bring the unlawful deed to its logical conclusion. It is therefore the responsibility of the police to investigate the circumstances of a crime committed, and after compiling the relevant facts, place it for subsequent prosecution to enable justice to the victims.[2]

It is very important and crucial that the investigating officers be upright and truthful during their investigations, enabling discovering the motives and circumstances of the crime committed. Otherwise, the facts of the case would be blurred and this would go towards making it difficult to prosecute the case and uncover the criminals. This would also contribute towards hindering the conviction of the criminals, besides impacting the judgement ultimately pronounced towards successfully concluding the proceedings conducted.[3] It is therefore important that all legal aspects should have been adhered to in the course of the investigation conducted, since shortcomings in this regard risk nullifying the judgement ultimately pronounced during the course of the proceedings undertaken. On a preliminary basis, the defendant and the prosecution both have to initially lay out the broad parameters of the proceedings and the facts related to the case towards determining whether the case is justified and worthy to be considered for a full-fledged investigation and subsequent judgement by the competent authorities. [4]

The investigation should proceed in a manner so as to carefully compile the available physical evidence

[1] Mohammed al-Halabi, note 22 above, P. 309.
[2] *Ibid,* P.311.
[3] *Ibid,* 313.
[4] Dr. Mohammed Ali Salem Ayad al-Halabi, the mediator in explaining Criminal Procedure Code, Part 1, P.31.

related to the crime committed, so that over a period of time, all ambiguities and queries related to the crime committed is appropriately answered and explained. It is therefore important to ensure that the integrity of the evidence collected and compiled is maintained at all times, and the crime site is preserved in its original state to the extent possible. This would certainly facilitate the investigators in successfully conducting their investigations. [1]

On the other hand, shortcomings in this regard would risk the loss of often key and crucial evidence, including smudging fingerprints. This could often lead to difficulties in successfully concluding an investigation and bringing the perpetrators to justice with regard to the criminal acts performed and concluded by them. An untouched crime scene provides a wealth of information to investigators and shortcomings in this regard can often upend the entire course of the investigations undertaken in the course of an investigation. [2]

The process through which the Attorney General is empowered to review and revise the proceedings of a case passing through a trial court is seriously impacted in consideration of the accompanying evidences presented in support of all statements made by both the defence and the prosecution. Overall, the trial courts have significant liberty and freedom to review the facts of the case and pronounce their judgements while tracking and recording the proceedings of the evidences presented. The courts have the independent authority to decide on exactly what kind of evidence would be permissible in the course of the trail, and what would be inadmissible. This is also guided by various manuals available in support thereof to ensure that proceedings conducted do not needlessly be adversely impacted by the misrepresentation of the evidence presented. [3]

In consideration of the aforementioned explanations, it can be reasonably concluded that both the initial enquiries and subsequent investigations made constitute key aspects of an investigative process. The same holds true for modern day electronic crimes too. It is supposedly considered a lot more simplified to tamper with modern day electronic evidence, and successes in this regard could surely impact the course and the direction of the subsequent investigation concluded. Often, the perpetrator of the crime would be considered to be highly skilled, to the extent that the individual hardly leaves any trace of the crime committed. This is so considering the ease and convenience with which most digital files can be changed, manipulated and amended, which makes the authenticity of such evidence often controversial. Hence, this in turn often contributes to presiding judges to be often hesitant in relying completely on electronic evidences alone for testimony in the course of the court proceedings conducted. Often adopting a shortened response time in compiling electronic data and related evidences could reduce the possibility of such data being tampered with, raising the threshold of authenticity associated with such information. In any event, the process and compilation of electronic data and information could also entail certain drawbacks in that the researcher would perhaps not be able to fully decipher the complete suite of hardware and software utilized and deployed within the system under evaluation and review. Therefore, such systems or processes could include the likes of various routers and the related, often utilized or deployed by the accused towards compiling certain information and data. The use of such systems within modern cyber crimes surely adds to the complications often faced by investigators in tracing the process employed vis-à-vis the crime, considering that such processes are often interlinked through the Internet. Nevertheless, considering that most routers used are equipped to maintain logs and records of their functions and operations, it is possible to obtain certain information irrespective of whether they are or are not connected with each other through the Internet.[4]

3- **Technical Experience in Front of Panel Judge**

An article 39-41 seemingly does provide ample leverage to the courts to determine the progression of a criminal investigation. Nevertheless, it still remains the prerogative of the judicial authorities to hire competent technical resources if there is perceived to be a genuine need for such personnel. It is important to note that complex technical issues can seldom be adequately handled and processed without the input, cooperation and assistance of qualified personnel since the multiple and complex parameters involved are often beyond the understanding of only the judge or the staff in the court. Hence, if faced with such quandaries and predicaments, the judge should resort to input from relevant personnel to ensure that the true state of affairs of the case being investigated is laid out for open scrutiny by all stakeholders. The court could decide to hire technical and qualified experts either on its own initiative, or on a plea from the defence team. When such a need is perceived or if the opposing party makes a formal request for relevant technical input, the same should not be over-ruled or

[1] Mohammed al-Halabi, note 27 above, P. 311.
[2] *Ibid,* 312.
[3] *Ibid,* 313.
[4] Ahmed Nashaat, A Message of Proof, Part I, 7th ed. , Alhalbi publication.

rejected as being inadmissible. Instead, allowing the same would contribute to ensure that the transparency of the proceedings is maintained. Perhaps, it is recommendable for the court to reject a need for such technical input and guidance only if the court takes it upon itself to bear full and complete responsibility for declining a request for the same. Alternatively, the courts may determine that the current merit of the case does not require the input a relevant technical input from a qualified practitioner.[1]

It is relevant to note and mention herein that as long as the proceedings are going on within the trial courts, the onus is not necessarily upon the presiding judge to answer and respond to each and every enquiry petitioned by the individual stakeholders. This is further intended to safeguard the interests of both the prosecution and the defendant to the proceedings, and to ensure that the proceedings are able to be undertaken without needless interference from any party to the dispute. The Court of Cassation is of the valued opinion that every accused has the right to a fair trial wherein they should have ample opportunities to defend themselves against all allegations made. Hence the defence should not be compelled to provide evidence to necessarily incriminate them. Even confessions made to investigators during the course of the investigations are allowed to be denied by the defence when the court actually takes up the case for hearing in its presence. Seemingly, this is a legal lacuna enabling the defence to make false confessions to legal authorities. In truth, this provision ensures that the defence team is provided due and ample opportunity to present their side of the case, and further to ensure that they are not compelled to provide evidence would be otherwise detrimental to their interests. In such cases and instances, it is often considered advisable to appoint a specialist to determine the truth. This would enable the court to determine the true state of affairs and make an appropriate ruling regarding each case presented to it for judgement. [2]

The Court of Cassation is of the opinion that the legal system should try and separate the facts of the case taken under review, using appropriate scientific and technical aids wherever required to ensure the impartiality of the judgements ultimately presented. This would contribute to ensuring that the judgements hold their weight in the event of review petitions. Under ordinary circumstances, this would be possible by hiring the services of related specialists who could provide their valued technical input regarding the issue under consideration.[3] Dr. Mohammed al-Halabi has duly indicated the shortcomings in processing issues in the context of the Criminal Procedure Act.[4] The law is correspondingly ambiguous on the specifics on how the proceedings are to be conducted in the given scenario, except for the fact that the technical advisor's input should be relied upon to a significant extent to lend credence to the final judgement pronounced by the courts. If necessary, multiple technical experts could be hired by the courts to ensure that the experts all provide similar advice regarding the issue under consideration. In the alternative, judgements provided upon weak arguments could often run the risk of the initial outcome being revoked upon appeal to a higher court. [5]

Cyber crimes are complex issues and entail multiple technical aspects for resolution and perception, which is often not something the courts can address on their own. Hence, to overcome the shortcomings perceived in this regard, it is important that the judges have recourse to necessary technical input from experts conversant with the intricacies of the systems and processes under consideration. Without such input from experts, judges are hindered in executing their duties towards the cases they are dealing with, since each cyber crime case being decided upon has its own set of unique properties to contend with. In the alternative, if the judge decides to handle things on their own initiative but are ultimately concluded not to be conversant with the relevant processes, they would be observed to be faced with issues against which they would not be able to rule upon. In such situations, it is but compulsory to hire the services of a technical expert, conversant with the issue at hand so that the appropriate judgement could be provided. At times, despite input from experts on the field, they may fail to realise the complete issue, and therefore fail to comprehend the multiple dimensions involved. The input and advice received would be incomplete in such scenarios and could be cause for earlier judgements to be overturned when subsequently reviewed with more comprehensive input from additional experts.[6]

If a court is not satisfied with the degree of support being received from a given technical resource, it is important that they hire the services of professionals they are more comfortable with towards ensuring that the

[1] Jondi Abdul Malik, Criminal Encyclopedia, Dar Alelem Leljamea Beirut Lebanon, Part I, P. 224.
[2] See Cassation Court Decision, Act Number 754/2011 on 5/2011.
[3] See Cassation Court Decision, Act Number 689/2010 on 5/2010.
[4] See Cassation Court Decision, Act Number 159/1983.
[5] See Cassation Court Decision, Act Number 159/1983.
[6] Mohammed al-Halabi, note 22 above, P 313.

input received adequately addresses the technical and scientific challenges being faced. In the event that a litigant to a specific court proceeding requests the services of a technical expert, the court should normally allow the same to be presented to ensure that all aspects of the case is correctly perceived and understood. If the court still decides to reject the advice provided by such an expert, it is justifiable to expect that the court would have genuine and due reason for rejecting the counsel received. It is important that the reason provided by the court should hold up to subsequent scrutiny in a higher court of law.[1]

4- **Importance of Expertise**

Article 147 stated within the Criminal Procedure Code is of the recommendation that all convictions issued by the court should hold up to subsequent legal scrutiny. The legislation enacted vis-à-vis a given issue provides generalized guidelines, with the onus of implementing the law lying with the courts. To this end, the courts are tasked with reviewing the information available and exercise whatever allowable penalty they deem appropriate. While normal issues placed before the court for review would be mostly decided through in-house input, at times the issues being debated would be complicated to the extent of requiring technical and scientific input from third-party professionals. This would contribute to the integrity of the judgement ultimately provided in this regard.[2]

The court may therefore refer to a doctor of medicine in judging upon murder and cases dealing with death. Alternatively, the services of a psychiatrist would be referred to for judging the mental state of a litigant or a defendant. The input received from such experts is provided due recognition and is always held in high esteem before the judgement is pronounced. The penal of judges are often liable to refer to input from third-party professionals in the course of a review since there could be various aspects in a murder case which would not be entirely and correctly perceived by the presiding judge on their own standing. This would be applicable in multiple scenarios, including when trying to explain situations involving the likes of poisoning or rigging systems. Counterfeiting bank notes require a degree of expertise which is not under the preview of the presiding judge alone, which would necessitate the hiring of industry professionals to determine their authenticity. [3]

The experts would contribute to enabling the judge to have a clearer perception of the issue at hand, so that justice could be served through the judicial system in its entire entirety.

There are certain crimes requiring a quantitative degree of expertise in resolving the challenges born in trying to successfully conclude them. In pronouncing judgement upon such issues, it is imperative that the judicial system have recourse to technical expertise and assistance, excluding which it may not be possible to clearly comprehend the issues therein and deliver honest judgement. In a particular case investigated by the Court of Cassation, the veracity of a licence was questionable. It was decided to have recourse to third party technical input towards having a clearer understanding in this regard so that any judgement delivered by the court would not be at risk of being upturned on a review by a Court of Appeal.[4]

Where a considerable degree of expertise is required to successfully resolve an issue, it is perfectly understandable for the court to have recourse to third-party technical input from industry professionals.[5] This would contribute towards providing a neutral forum for concluding the reasons contributing to the current state of affairs, enabling the court to deliver its judgement and set penalties commensurate to the magnitude of the crime being investigated. Hence, in the event of the detection of a forgery, this could be easily verified and commented upon by a neutral third-party professional entity which could draw upon its technical expertise regarding the subject matter under review so that the authenticity of the signatures on the document is verified. Indeed, the personal perception of the judge alone may not necessarily have enough legal clout to be able to successfully rule on the issue to the satisfaction of all stakeholders party to the litigation under process. It is also in the interest of both the prosecution and the defence to have recourse to third-part professional bodies who could adjudicate upon the issue at hand so that the issue is unequivocally and unambiguously decided upon. Hindrances bought forth in this regard would be to the detriment of all litigants involved and would be a violation of the rights of the accused. This would in turn prejudice the case and it could be later needlessly alleged that one party was perhaps unduly favoured upon the court at the expense of the other.

[1] See Cassation Court Decision, Act Number 296/1999 on 5/1999.
[2] See Cassation Court Decision, Act Number 159/1983 on 5 /1983.
[3] See Cassation Court Decision, Act Number 815/1999 on 5/1999.
[4] Jondi Abdul Malik, Criminal encyclopedia, note 49 above.
[5] See Cassation Court Decision, Act Number 746/2004,30/5/2004.

Where the court reviews the case papers and concludes that there is probably no need for specific input from a neutral third-party adjudicator, the court itself decides on the specifics of the litigation brought forth. The objective in such instances is not necessarily assumed to be controlled by the Court of Cassation, considering how it would suffice for the available evidence to be reviewed by the judge overseeing the proceedings within the trail court. A Jordanian Court of Cassation was of the perspective that there could be the possibility of a certain minimal degree of discrimination, although such instances are duly addressed within the provisions stated within the specifics contained within Article 147.[1]

Considering the multiple parameters bought forth for discussion, the investigation of e-crimes and associated electronic issues, delivering commensurate penalties equal to the magnitude of the crime detected is a technical aspect which has been adequately discussed in the course of the initial part. Therefore, it is important to have technical advice and input from professionals in trying to investigate upon such issues. Correspondingly, it is important that cyber crime issues be investigated by technical professionals since doing so otherwise would risk compromising the integrity of the investigation concluded and perhaps even dilute the validity of the judgement ultimately pronounced in the context of the case under review.[2] Hence, in the event of a flawed judgement delivered by a court which had decided not to have recourse to qualified technical input, there is a serious possibility of the proceedings being subsequently censured and the earlier judgement delivered being overturned once technically qualified third parties are brought into to arbitrate on the issue under consideration at some later point in time, like perhaps during a review of the case by a higher court of law. Further, the accused is allowed to request for technical input on the issue being considered, and could even request such evidence in presenting their defence to the court during the proceedings of the case. Failing to allow the defence to present such evidence would constitute a denial of adequate rights to the accused, and would therefore constitute a violation of the prevailing law in this regard.[3]

5- **Estimate Expertise and Presumption of Innocence**

The evidence presented and the corresponding specific methodology adopted in reviewing the same is often the prerogative of the presiding judge, irrespective of the extent of the technicality of the case being considered. Further, the court is nevertheless constrained upon evaluating the evidence and judgements pronounced; ensuring that judgements finally pronounced in this regard should be consistent with the faith and the conscience of the judge presiding within the court. The Court of Cassation is of the perspective that considering the provisions stated within Article (2/6), as stated within the Evidence Act, it is important that the evidence presented should be realistic to the extent possible.[4] The Court of Cassation has allowed a significant degree of freedom to the lower court in this regard, as long as the proceedings are conducted in an open and fair manner. The Court of Cassation is of the opinion that the technical input provided is not full and final in determining the conclusion of the case, and instead at times the court may ultimately be observed to have ruled diametrically opposite to what had been originally ruled.[5] This could be attributed to the fact that irrespective of the validity of the technical input and advice received, oftentimes the artistic ideals have a greater sway on the proceedings under consideration, so long as the legal provisions are being observed.

The legislative branch of the government has provided trial courts the freedom to pass judgements irrespective of the weight of the evidence presented publicly. The court is seemingly and supposedly empowered to provide judgements at its discretion, so long as the legitimacy of the court is maintained and the innocent is not needlessly persecuted. Therefore, depending upon the court situational parameters, it may be possible to ignore the conclusions derived by the technical input sourced. This is attributable to the fact that the court is at liberty to consider what it ultimately thinks is relevant to the issue under-consideration.[6]

In consequence thereof, the court would probably strike a middle ground by taking in part of the report submitted by the expert. This would contribute to fulfilling the fact that the court is not necessarily compelled to incorporate all the recommendations made by an externally hired resource towards bringing closure to the proceedings related to the lawsuit brought forth by the parties concerned. It is ultimately the discretion of the

[1] See Cassation Court Decision, Act Number 120/1992, 6/1992.
[2] See Cassation Court Decision, Act Number 2295/2014, 2/2015.
[3] See Cassation Court Decision, Act Number 307/2014, 3/2014
[4] Mohammed al-Halabi, note 22 above, P. 315.
[5] See Cassation Court Decision, Act Number 681/2013, 3/2014.
[6] See Cassation Court Decision, Act Number 663/2000, 8/2000.

court to decide on precisely what aspects they would like to be incorporated within the report released, and the sections they would prefer to be excluded. In seeking advice and input from a neutral third-party technical resource, it does not in any way whatsoever dilute the authority and ownership of the court over the proceedings taking place, since the court remains at full and complete liberty to decide on precisely what aspects of the evidences they would like to remain part of the proceedings and what would be excluded. Thus, the recommendations and opinions put forth by technical experts hired by the court are a necessity, since it enables the court to have a more comprehensive perception and understanding of the issue being discussed, and enables more fair-play within the judgement ultimately released.[1]

The technical expertise and input provided to the panel undertaking decisions vis-à-vis issues under debate is of great significance towards agreeing upon the penalties to be imposed upon an accused. This is especially true where it is perceived that the litigants are making confusing claims and the actual magnitude and seriousness of the issue under consideration is not being fully and comprehensively perceived in its actual sense. The Court of Cassation has been observed to state that it is not advisable for the courts to simply rely on the input and testimony provided by the litigants in the course of the proceedings of the court, especially where it is perceived and observed that the confession is in contravention to the conclusions presented by the team of hired third-party technical experts and consultants. Thus, the input provided to the court by the hired technical team has its own legal standing within the parameters of the law. [2]

This is to be considered in the context of how mere testimony provided by both the defendant and the litigants may not be completely accurate since each party to the dispute would like to see the judgement being delivered to be to their utmost benefit. Therefore, in the case of deciding upon electronic communication, it is often advisable not to wholly depend upon the input provided, especially if the same contradicts the technical advice received in this regard. It is therefore very relevant and important that the court processing the case be completely at ease and well conversant with the technical input received, even if such input could at times be perceived to be diametrically opposite and divergent to the testimony provided by the parties to the dispute which is being tried to be judged and arbitrated upon. The technical input provided and made available would contribute towards enabling a more comprehensive perception of the issue being debated, irrespective of the sometimes misleading statements made by the various witnesses made part of the proceedings by the litigants. Oftentimes, the statements of such witnesses would be contradictory and it would be difficult to correctly separate exactly what is correct and what else is inconsistent with the facts. The technical input provided by professional third party consultants therefore provides a significant degree of truth and honesty for the court in deciphering or perceiving the actual state of affairs. [3]

It is to be noted that input provided by both the litigants can often be overturned on the basis of third party recommendations, which would otherwise be expected to have minimal direct benefit from any of the parties to the dispute. Such input provided should be considered solely in consideration of the technical expertise of the teams involved. Expert advice received should be ideally corroborated by other input gathered from surrounding sources, or if the same is required from a different technical team in order to ensure that the same is unequivocally recognized and acknowledged by a court of law. The Court of Cassation is of the learned input that the purpose of hiring the services of such technical specialists is to enable the courts to conclude the actual state-of-affairs so that any misleading statement and input provided does not cloud the concluding judgement provided. Such input would be anecdotal to the testimony provided by experts, and would be a full and fair description of the medical reports presented in support thereof.[4]

The Jordanian Court of Cassation is of the conclusion that the rulings made should be based upon what is unequivocally decided to be a true reflection of the affairs, and which are not in dispute by both the litigants. The facts should have been technically and scientifically reviewed and their authenticity confirmed in consideration of the modern day progresses made within the context of the arts and the sciences. Such a scenario would incorporate the factual occurrences recorded in relation to the crime committed. The accuracy of whatever being finally concluded would be increased in consideration of technical input received from the domains of the sciences and the arts.[5]

[1] See Cassation Court Decision, Act Number 214/2004, 4/2004.
[2] See Cassation Court Decision, Act Number 86/1986, 2/1987.
[3] See Cassation Court Decision, Act Number 293/1995, 7/1995.
[4]See Cassation Court Decision, Act Number 209/1996, 4/1996.
[5]See Cassation Court Decision, Act Number 293/1995, 7/1995.

To this end, technical expertise is considered relevant when taken as proof of what has occurred. This is stated within Article 147 of the Criminal Procedure Code which empowers the judge to evaluate all available evidences and related input and decipher what they mean at the personal discretion of the judge.[1] This provides a clear mechanism on how various certificates and clues or related aspects could be evaluated. While the lower courts are often compelled to seek the assistance of outside technical resources in arriving at a judgement, the same would often hold true for the higher courts too since they too could have access to a different team of experts in order to ensure the validity of the claims made by the litigants, and also to ensure the validity of the judgement provided by the lower court. The courts should therefore ensure that the technical team referred to are specialists in their individual and respective professions. This would ensure that should the judgement of a lower court be found to be subsequently flawed on review by a different team of experts; the original ruling could be over-turned in favour of a new judgement. The expertise of the professionals hired for this purpose should be such so that the testimony provided should have significant weightage over and above what is stated by the complainants to the case. [2]

6- **Debate Expert and Presumption of Innocence**

The panel of judges overlooking and reviewing the proceedings of a case encourages a structured discussion of the report provided by especially hired professionals to ensure that any loopholes are identified and debated upon. Within the domain of electronic crimes, there is a significant and specific need to discuss the various aspects under consideration which is necessitated due to the nature of the evidences provided. Such input is often liable to be tampered with, which makes them susceptible to be doubted upon with regard to their authenticity. The nature of electronic data gathered is such that at times they may not by themselves provide the required information, but when taken in support and conjunction with other available evidence, it could provide a clearer image of the overall situation under review.[3]

The Court of Cassation is of the viewpoint that it is detrimental to singularly rely on the testimony of experts alone while ignoring the input to be provided by the litigants and parties to the dispute being resolved. If it is subsequently proved that the complainant of the case involving forged signatures actually agreed to actually allow the defendants the benefit they had intended to derive from the action to start off, the case bought forth could be withdrawn. Further, the integrity of the locales storing such documents was also to be reviewed. [4]

It is therefore important that the courts agree to hear out the testimony stated within the regulator's report in consideration of the learned input provided by the experts. Failure to do so could constitute a denial of the rights of the defendant, and could invalidate the judgement pronounced by the lower court. Considering the digitization of the data under consideration, there is normally a certain degree of uncertainty and doubt associated with the integrity of the information being evaluated, which is also true when reviewing cases involving electronic crimes. There is a real possibility of the defendant in the court proceeding clashing with the testimony provided by the panel of neutral third-party experts. This could contribute to sway opinion within the court on the legality of the pitch put forth by the litigants regarding the extent of the guilt of the defendant. The Court of Cassation is of the perspective that the testimony of the coroner would be considered crucial herein, who would provide input and corroborate the fact whether the death of the deceased could be actually attributed to a disruption in the blood flow to the brain due to the two bullets fired at and subsequently striking the individual. It is therefore important for experts to testify whether an accused in a stabbing case should be held liable for the grievous bodily harm bought forth upon the victim since if it can be proved that the victim's lung was already suffering from a serious ailment beforehand, the guilt of the perpetrator could be pleaded to be reduced.[5]

The conclusion derived wherein the individual is considered innocent unless proven guilty in a court of law is tilted to be in favour of the accused in a crime. The assumption holds true within the duration of the proceedings conducted, and hinders prosecutions and imprisonment on mere conjecture or suspicion. For a judge sentencing an individual in a penal reform, it is important that the guilt be proven beyond all reasonable doubt and it is the responsibility of the judge to reject and do away with the lingering suspicions in this regard. The

[1] See Cassation Court Decision, Act Number 86/1986, 2/1987.
[2] See Cassation Court Decision, Act Number 86/1986, 2/1987.
[3] Da-Yu Kao and Shiuh-Jeng Wang, note 17 above.
[4] See Cassation Court Decision, Act Number 209/1996, 4/1996.
[5] See Cassation Court Decision, Act Number 293/1995, 7/1995.

penal code emphasizes the need for the guilt of the accused to be proven beyond all measures of reasonable doubt before the convict can be awarded any sentence as penalty for whatever grievous action has been perpetrated by the individual upon others. The same principle also holds true for electronic crimes too and this is where technical experts are liable to provide their valuable input on how they could prove that a crime has been actually committed. Alternatively, if the experts are hindered in proving the guilt of the accused, the charges initiated would all need to be waived off and dropped.

Conclusion

A review of the parameters associated with cyber crimes would go on to demonstrate that the issues raised therein may not be resolved solely by considering the technical capabilities of the investigating staff. It is important that investigators not be mediocre personnel but should instead be experts in their individual fields to enable a thorough investigation of the case.

Unfortunately, the majority of judges may not be expected to be technical experts regarding this specific field, necessitating them to refer to third party contractors aware of the finer specifics associated in how the case should proceed. In the event that the input received by the court is in any way flawed, there is the risk of an incorrect judgement being pronounced, which necessitates that a careful screening be undertaken of the technical professionals hired by the court for conducting the review of the case under consideration and to successfully conclude the same. It is important that cyber crime issues be resolved by technical input from experts in their respective fields, considering how easy it is for the common man to lose track of the minute specifics involved in modern day specialities and related fields. Indeed, it is often times a difficult and challenging proposition to factually ensure that a defendant is truly responsible for a crime committed in the electronic sphere, and criminals are often known to take advantage of this aspect for their benefit. This makes it a challenge for the judge to ensure that the perpetrators of such crimes are brought to justice, considering how the judges needs to overcome their own shortcomings regarding this topic, and instead depend upon the input from certain other third party contractors. The dynamics are seemingly more complicated by the fact that the crime needs to be unambiguously proved for a conviction to proceed. Indeed, the judgement pronounced and the penalty imposed should not be in consideration of mere speculation and conjecture. There are indeed multiple legalities involved in condemning an individual to a penal sentence solely on the basis of certain electronic blips and signals, since it could often be subsequently concluded that the same on the basis of which the initial judgement was pronounced, was in fact fake. The very nature of digital medium makes them susceptible to tampering and this makes it all the more difficult and challenging to successfully conclude a judicial decision. It is therefore important to thoroughly investigate the available range of electronic evidences to ensure that the case proceeds to a successful conclusion, and is in turn hampered by minimal bottlenecks due to data tampering fears.

In evaluating the issue from a procedural viewpoint, it could be observed that should the public prosecutor decide not to refer to expert testimony from qualified personnel, there is a very serious risk of the trial falling through when evaluating an electronic crime. Therefore, it is important that if there is a perceived need for technical input, the same should be obtained at the earliest instead of being needlessly delayed or skipped. The legal procedures in place certainly sanction the hiring of technical input considering that this would be of assistance in either substantiating or disproving the official stance adopted by both the defence and the prosecution. The court in itself has to remain neutral on the issue till a final judgement is delivered against either of the parties to the dispute. It is important not to consider this stance in conjunction with Article 226 within the Code of Criminal Procedure which states that litigants can request the presence of multiple witnesses to supplant their perspective during the court proceedings towards reflecting the validity of the original claim made by either party. Nevertheless, this specific act of the law seemingly does not recommend the hiring of technical experts at court expense to prove or disprove the stance maintained by the parties to the dispute. The Court of Cassation is of the perspective that it is not the responsibility of the court to create evidences for either party to the dispute, considering that the court is a neutral forum in itself where both parties would have their grievances redressed. This is aptly demonstrated in how the Amman criminal court gave a not-guilty verdict considering that enough evidence was not provided to prosecute an individual brought before the court related to a case of forgery. It is indeed not the responsibility of the court to create or destroy evidence, and therefore in the event that there are questions on the validity of signatures presented, or in verifying the handwriting of an accused, the court by itself would not create the evidence required to have a guilty verdict. Doing so would reflect negatively upon the court since it would no longer make the entity as being impartial to the dispute. The Court of Cassation is of the opinion that the prosecution is liable to provide the evidences on the basis of which a court could thereafter declare a guilty verdict. It is therefore concluded that it is but the responsibility of the prosecution to investigate the issue under consideration towards generating the required evidences, as per Article 226 within the Criminal Procedure Code.

Researcher's Recommendations

It can be reasonably concluded from this treatise that the complexity of modern day cyber crimes cannot just be resolved from the input provided by skilled professionals drawn from the highly specialized fields of communication and technology. Further, we cannot just depend upon testimony from our witnesses in this regard too. In their resolution number 26956/2014, the Amman Court of Appeal disputed the validity of the witnesses in a case regarding the misuse of a Facebook account and concluded that their testimony alone was insufficient to prove that there had been a misuse of the social media account. The court explained that the law was explicit in that an individual could only be penalized if it could be unequivocally proved beyond all reasonable doubt that a crime had indeed been committed. Therefore, no one could be penalized on mere conjecture and suspicion. The court further explained that it was not their responsibility to arrange for evidences, since the prosecutor was working on this aspect. Since there was insufficient evidence presented to link the accused to the crime, the court ultimately had to release the suspect. It is also concluded from a review of the text of this document that expertise could certainly contribute towards building a sound basis upon which a court of appeal would be satisfied by the electronic data presented for the eventual prosecution of the accused.

Correspondingly, it is crucial that sound evidences are presented in prosecuting electronic crimes since the process cannot be successfully concluded on mere conjecture alone. The Amman Court of Appeal is of the perspective that patent announcements associated with offensive mails should be beyond doubt directed to the complainant since it would be compulsory for this aspect to be proved beyond doubt to prove that the mail was indeed sent over to the respondent. The Court of First Instance was in support of this stance and concluded that this was indeed valid in consideration of the associated circumstances. Therefore, the IP address owner or other individuals may not necessarily be held liable for the misuse of their addresses if it can be proved that the same was forcefully used by someone else after hacking into the system of the original owner. On a similar note, the Irbid court of appeal also decided to come out in support of the decision made by the court of first instance regarding the failure of a conviction in consequence of incomplete evidences presented while reviewing a cyber crime within its jurisdiction. Thus, the Orange internet provider was not held liable for the actions performed through its databases and technology since the firm denied that it knowingly contributed to the unfortunate actions observed. The criminal case bought forth provided a legal basis in deciding multiple civil cases related to the same in how it was considered that it was not necessarily a crime in consideration that there was no actual physical or mental harm borne of the action. Finally, the profile of the individual was not accepted. Hence, it is crucial that appropriate and adequate evidences be made available to successfully prosecute an individual.

To conclude, in consideration of the multiple legal and technical challenges associated and borne of the increasing incidences of cyber crimes in society, the researchers are of the recommendation for laws making the owner of the Internet account used in an account to be responsible for the crime committed using the same. Such laws should be worded to unequivocally make it clear that irrespective of the actual operator of the system for the duration of the crime being in process, the account holder would be held responsible in the courts.

References

- **Books**

Ahmed Nashaat, A Message of Proof, Part I, 7th ed. , Alhalbi publication.

Jondi Abdul Malik, Criminal Encyclopedia, Dar Alelem Leljamea Beirut Lebanon, Part I.

Mohammed al-Halabi, The Mediator in Explaining Criminal Procedure Code, Part II.

Todd G. Shipley, Art Bowker, Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace (Syngress, USA, 1st ed, 2014) .

- **Articles**

A. Joint and E. Baker, 'Knowing the past to understand the present' (2011) 27(4) Comput. Law Secur. Rev. 407.

August Bequai, 'A guide to cyber-crime investigations' 1998 17(7) Computers & Security 579.

Christopher Hooper, Ben Martini, Kim-Kwang and Raymond Choo, 'Cloud computing and its implications for cybercrime investigations in Australia' (2013) 29(2) Computer Law & Security Review 152.

Christos Kalloniatis, Haralambos Mouratidis and Shareeful Islam, 'Evaluating cloud deploymentscenarios based on security and privacy requirements' (2013) 18(4) Requirements Engineering 299.

Da-Yu Kao and Shiuh-Jeng Wang, The IP address and time in cyber-crime investigation 2009 32(2) Policing: An International Journal of Police Strategies & Management 194.

David W. Chadwick and Kaniz Fatema, ' A privacy preserving authorization system for the cloud' (2012) 78(5) Journal of Computer and System Sciences 1359.

Dawei Sun, Guiran Chang, Lina Sun and Xingwei Wang, 'Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments' (2011) 5 Procedia Engineering 2852.

Denis Reilly, Chris Wren & Tom Berry. 'Cloud Computing: Pros and cons for computer forensic Investigation' (2011) 1(1) International Journal Multimedia and Image Processing 26.

Donghee Shin, 'Beyond user experience of cloud service: Implication for value sensitive approach' (2015) 32(1) Telematics and Informatics 33.

F Etro, 'The economic impact of cloud computing on business creation, employment and output in the E.U.' (20 09) 54(1) Rev. Bus. Econ 179.

José A. GonzálezMartínez and et al., 'Cloud computing and education: A stateofthe-art survey' (2015) 80 Computers & Education 131.

Kalloniatis, Mouratidis and Islam, above n 4, 299. See, José A. GonzálezMartínez and et al., 'Cloud computing and education: A stateoftheart survey' (2015) 80 Computers & Education 131.

Mark Vincent & Nick Hart, 'Law in the Cloud' (2011) 49(5) Law Society Journal 50.

Nancy J. King and V.T. Raja, 'Protecting the privacy and security of sensitive customer data in the cloud' (2012) 28(3) Computer Law and Security Review: The International Journal of Technology and Practice 308.

R Buyya and et al., 'Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility' (2009) 25(6) Future Generation Computer Systems 599.

T Behrend, E. Wiebe, J London and E Johnson, 'Cloud computing adoption and usage in community colleges' (2 011) 30(2) Behav. Info. Technol 231.

Sathiyapriya K. and et al., 'A Study on Security Challenges and Issues in Cloud Computing' (2013) 2(7) Internati onal Journal of Engineering and Innovative Technology 256.

S.W. Brenner, B. Carrier, J. Henninger,'The Trojan Horse Defense in Cybercrinme Cases' (2005) 42 Purdue University, West Lafayette, Purdue University, West Lafayette, IN.

- **Cases**

Dow Jones and Company Inc v Gutnick [2002] High Court of Australia 56; 210 CLR 575.

- **Conventions**

Convention on Cybercrime, opened for signature 23 November 2011 (entered into force 1 July 2004).

- **Internet Sources**

Dynamic IP vs Static IP, whatlsIPAddress <http://whatismyipaddress.com/dynami c-static>.

Jordan July 2014 -December 2014, gvernment requests report <https://govtrequests .facebook.com/country/Jordan/ 2014-H2/#>

IP Addresses in Online Investigations, AVVO <http://www.avvo.com/legal-guides/ugc/ip-addresses-in-online-inv estigations>
Margaret Rouse, Cloud Computing Definition, TechTarget <http://searchcloudcom puting.techtarget.com/definitio n/cloud-computing>

How you connect to the world, whatls myIPAddress <http://whatismyipaddress.co m/ip-basics>.
How to Find the MAC Address of Your Computer, wikihow <http://www.wikihow .com/Find-the-MAC-Address-of-Your-Computer>

What is DHCP?, whatls myIPAddress <http://whatismyipaddress.com/dhcp>

What is a MAC Address?, IP location <https://www.iplocation.net/mac-address>

What's the difference between a Mac Address and an IP Address?, Ask Leo <https ://askleo.com/whats_the_differ ence_between_a_mac_address_and_an_ip_a ddress/>

Why Does Your IP Address Change Now and Then?, whatls myIPAddress <http:// whatismyipaddress.com/keeps-changing>.

Why IP Addresses Alone Don't Identify Criminals, Electronic frontier foundation <https://www.eff.org/deeplinks/ 2011/08/why-ip-addresses-alone-dont-identify-criminals>