

# INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

---

Volume 6 | Issue 6

---

2023

© 2023 *International Journal of Law Management & Humanities*

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

---

This article is brought to you for “free” and “open access” by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact [Gyan@vidhiaagaz.com](mailto:Gyan@vidhiaagaz.com).

---

**To submit your Manuscript** for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to [submission@ijlmh.com](mailto:submission@ijlmh.com).

---

# Analysis of Impact of Social Media and Information Technology on Evidence Law

---

SUDHIR KUMAR DWIVEDI<sup>1</sup> AND KUSH KAKKAR<sup>2</sup>

## ABSTRACT

*It is undeniable that this era is era of information technology. Focus of every country is on digital advancement. India is not an exception to this and focus of the country is on Digital India. Legal field is drastically changing by the advancement of science and technology as technology has become an integral part of judicial system. Drastic change have taken field in legal field with digitalization of legal works, online hearing, submission of file after scanning all the documents are now days a common trend, E-courts are need of the hour. Government is also taking steps for improvement if digital infrastructure, as it has dual advantage firstly it is cost effective and secondly bulk of information can be stored without fear of physical loss of document as within a minute same document can be easily stored in multiple number of digital file in different mode if digital arability. With digitalisation of legal work one common question is arising that how much weight age shall be given to digital evidence in court, because digital evidence are very delicate in nature and can easily be tempered. By the passing of IT Act, 2000, relevancy and admissibility of digital evidence has been fixed though amendment in Indian Evidence Act, 1872. But basic condition of admissibility is still governed by the Act. Electronic evidence are so called Digital evidence have been admitted as documentary evidence under S/3 of the Indian Evidence Act, which provides “all documents including electronic records produced for the inspection of the court are called documentary evidence”. The main difference is that the verbal statement produced as evidence is called oral evidence while verbal statement contained in electronic record is treated as documentary evidence are records.*

*Use of science and technology by criminals, in commission of crime, is increasing day by day and to deal with such crime and criminals, it is very important that the investigating agencies must be aware and trained about such technologies. Collection of scientific evidence is important aspect of crime investigation, police officers involved in collection of direct evidence, are hardly trained in collection of scientific evidence. Another issue is that there is neither specific guideline of court nor any specific law to deal with scientific investigation. The Information technology Act, 2000 brought certain important changes in Indian Evidence Act, 1872, specially in regard to admissibility of electronic evidence, but*

---

<sup>1</sup> Author is an Assistant Professor at Department of law, JIMS Greater Noida Affiliated to GGSIPU, New Delhi, India.

<sup>2</sup> Author is a student at Department of law, JIMS Greater Noida Affiliated to GGSIPU, New Delhi, India.

*this admissibility is subject to certain condition laid down the Act itself. Investigating agencies while conducting investigation especially scientific investigation, collects a number of scientific evidence like tape recorded conversation, Facebook, WhatsApp chat messages, Mobile text messages, mobile communication records and so on. However how much weightage shall be given to such evidence is subject to controversy. Social media has changed the way of interaction with each other.*

*The main thrust of this paper is to analyse different type of Social media evidence and to find out how much evidentiary value is given by courts. Whether such scientific evidence may be concluded as a conclusive proof or not, needs to be analysed. Indian evidence Act doesn't contain any provision how the accuracy or validity of such evidence is to be decided or it is totally on the capability of the court. Author will suggest some factors to be taken into consideration while appreciating such evidence.*

**Keywords:** *Scientific Evidence, Evidentiary value, Scientific Investigation, Collection of Evidence.*

## I. INTRODUCTION

Interpretation of Section 2(1) (t) and (i) of IT Act makes it clear that mobile phones are included in the definition of computer and that's why SMS, WHATSAPP, FACEBOOK and E-MAIL Messages are treated as electronic record. So, such electronic Messages would be admissible as documents under the Section 65 R/W 65A and 65B of Indian Evidence Act, 1872 Provided that conditions of Section are fulfilled.

Under the provisions of Section 88A, there is a presumption that an electronic message forwarded by the sender through an electronic mail server to the addressee to whom the message fed into his computer for transmission.<sup>3</sup> However, there is no presumption as to the person by whom such message was sent. This provision only presumes the authenticity of the electronic message, and not the sender of the message.<sup>4</sup>

Before Information Technology (IT) amendment Act 2000, evidence of 'Electronic Documents' were generally produced by taking print of digital records and authenticity of such printed document was been certified by competent authority. Such authority is called in the court to identify his/her signature and is subjected to cross examination. This procedure met the requirements of Section 63 and Section 65 of the Act. But by passing of IT amendment Act,

---

<sup>3</sup> M. Monir , text book on The Law of Evidence 312-313 (universal law publishing Co. New Delhi- India 9<sup>th</sup> edn., 2013).

<sup>4</sup> Tejas D. Karia , "Digital Evidence: An Indian Perspective" 5 digital evidence and electronic signature law review 216 (2008)

2000 two new sections 65A and 65B were added in the Indian evidence Act to deal with electronic records. Section 65A is equivalent to section 61 in reference to documentary evidence means it can be said the 65A plays the same role for electronic records what section 61 do for documentary evidence. It provides a simple and different procedure for oral evidence contained in electronic records to deal with rule of hearsay evidence. It also secures other interests, such as the authenticity of the technology and the sanctity of the information retrieval procedure.<sup>5</sup> But it does not mean that there is repetition of provision in the Act as section 65A is different because it is a special law to electronic records produced in the documentary form. Section 65B of the Evidence Act details this special procedure for adducing electronic records in evidence. Sub-Section (2) lists the technological conditions upon which a duplicate copy (including a print-out) of an original electronic record may be used. Sub-Section (4) of Section 65B requires the production of a certificate by a senior person who was responsible for the computer on which the electronic record was created, or was stored. The certificate must uniquely identify the original electronic record, describe the manner of its creation, describe the device that created it, and certify compliance with the technological conditions of sub-Section (2) of Section 65B.<sup>6</sup>

Fundamental principle of evidence laws is that oral evidence is allowed to prove all facts but facts contained in documents cannot be proved by oral evidence, for this document itself is to be produced in the court. One other requirement is that oral evidence must be direct otherwise it will be affected by rule of hearsay evidence and if it is not falling in one of exception of rule of hearsay it will not be admissible.

Non acceptance of hearsay evidence is based on the principle that truth or accuracy of hearsay evidence cannot be established as the real person will not be available for cross examination. Since the person who makes such statement and the person to whom it is made cannot be cross examined, as third person's account of it, is excluded.<sup>7</sup>

Hearsay rule is basically associated with oral evidence but somehow it also affects rules related to documentary evidence. Hearsay rule has faced new challenges due to digitalization of documents. Rule of best evidence focuses that primary evidence (the original document itself) shall be presented before the court and secondary evidence shall be accepted only when it satisfies the requirement of law on secondary evidence, but digitalization has increased the

---

<sup>5</sup>M. Monir, text book on The Law of Evidence 276-178 (universal law publishing Co. New Delhi- India 9<sup>th</sup> edn., 2013).

<sup>6</sup>*Ibid*

<sup>7</sup> Arvind Kumar Dubey (ed.), "The Law of Evidence", by Batuk Lal 257(Central Law Agency, Allahabad 16<sup>th</sup> edn., 2003).

volume of digitalized documents and they are stored as secondary evidence. The result of this is that courts have now started depending on secondary evidence and basic rule of best evidence that primary evidence shall be presented is running behind the advance digitalized system of justice administration. In the **Anvar P.V. v. P.K. Basheer & Ors**<sup>8</sup> the Supreme Court noted that “...*there is a revolution in the way that evidence is produced before the court*”.

Acceptance of digital evidence in court depends on the fact whether the evidence is relevant, whether it is authentic, whether it is hearsay, if yes, whether a copy is acceptable or the original is required. Relevancy and admissibility of a digital evidence has to be seen in the light of Sections 3, 5, 65A, 65B and 136 of The Indian Evidence Act, 1872 (Hereafter referred as Evidence Act) as well as on general principle of evidence that all admissible fact are relevant but all relevant facts are not admissible. Relevancy of a fact depends upon the connection of fact with either the fact in issue or some other relevant fact in such a manner as is provided in either of the provisions of relevancy in the Indian evidence act but relevancy Section of the Act has nowhere dealt with relevancy of digital evidence except in admission clause. Thus, it shows that digital records are form of admission provided that such digital records are fulfilling the basic criteria of admissibility in other words it suggests an inference as to facts in issue or relevant facts (Section 5 R/WS136). Accordingly, admissibility has to be seen in two perspectives-

1. Admissibility of fact in order to decide the case
2. Admissibility of evidence in order to prove the fact

Regarding the admissibility of facts, the first proviso of Section 165 expressly provides that judgment shall be based only upon relevant facts. On the other hand, Section 136 (1) R/W Section 5 provides that evidence shall be admitted only upon relevant facts or directly upon issue. The duty has been cast on the court U/S 5 itself that it shall allow evidence only upon relevant facts or fact in issue. A manifestation of this duty in the form of direction is to be found in Section 136 (I) which reads as-

*“When either party purposes to give evidence, the judge may ask in what manner the alleged fact, if proved, would be relevant and the judge shall admit the evidence if he thinks that the fact if proved would be relevant, and not otherwise.”*<sup>9</sup>

Under this situation the relevancy and admissibility of digital evidence may be analyzed as follows-

---

<sup>8</sup>Anvar P.V. v. P.K. Basheer & Ors [MANU/SC/0834/2014]

<sup>9</sup> Section 136(i) The Indian Evidence Act, 1872. (Act No. 1 of 1872).

Digital evidence as documentary evidence has been made relevant U/S 17 of the Evidence Act in the form of admission. As per Section 17 a statement, oral or documentary, or contained in electronic form, which suggests any inference as to any fact in issue or relevant fact, is relevant. Again, as per Section 22A which deals with relevancy of oral evidence as to contents of electronic records makes it clear that oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic records produced is in question. Section 39 which deals with statements that forms part of a longer statement or of a conversation or part of an isolated document, or is contained in a document that forms part of a book or series of letters or papers specify it that When any statement of which evidence is contained is part of electronic record (Section 39 Evidence Act), evidence must be given of so much and no more of the electronic record as the court considers necessary in that particular case to the full understanding of the nature and effect of the statement and of the circumstances under which it was made.<sup>10</sup>

It is clear from above discussion that electronic records are relevant however the admissibility of digital evidence depends upon fulfilling of the condition laid down in Section 5 R/W Section 136 of the Evidence Act. The controversy/difficulty in regard to admissibility of digital evidence is that digital evidence is treated as documentary evidence in the Act, though are oral statements. So, it is against the basic principle of evidence that “Oral statements should be made available before the opposition for cross examination failing which they will be mere statements”<sup>11</sup>

It should be noted that even if electronic records have been disclosed, the evidence still needs to meet the threshold for relevancy and reliability to be admissible. Disclosure or production of a document should not be taken as an admission of relevance or admissibility. For an electronic record to be deemed relevant at trial, the ordinary analysis of its probative value outweighing its prejudicial effect must take place. The record must also be deemed reliable.

It is also important that a party producing the electronic evidence in court the onus of showing its authenticity is on the person. It is to be established that electronic records are the same as it has been claimed and for this admission of opposite party or by cross examination it can be done. In the same line integrity of the electronic record is to be established and this depends upon how accurately information was recorded and maintained. Though in the absence of contrary evidence, there is presumption of integrity of such electronic evidence subject to

---

<sup>10</sup> Arvind Kumar Dubey (ed.), “The Law of Evidence”, by Batuk Lal 98-221(Central Law Agency, Allahabad 16<sup>th</sup> edn., 2003).

<sup>11</sup> Syed Md. Husain Aftiqar v. Mirza F Beg (1932) 8 Luck 135.

procedure provide by law has been followed.

## **II. SEARCH AND SEIZURE OF ELECTRONIC DEVICE**

In litigation social media evidence comes into play in two respects, first the discovery process and second admission at trial. It is also important that every document relevant to any fact in issue must be shown in whose possession, control or power the document is or has been.

Hon'ble Karnataka High Court has issued guidelines to be complied by the Investigating officers in regards to the manner of carrying out a search and/or for preservations of the evidence gathered during the particular search in respect of smart phones, electronic equipment or email accounts etc. Single Judge bench of Hon'ble Mr. Justice Suraj Govindaraj said "It would be in the interest of all the stakeholders that detailed guidelines are prepared by the police department in relation to the same. Pending such formulation, it would be required that the following minimum guidelines are implemented."

The court issued the guidelines to be followed.

### **“In the case of a personal computer or a laptop”.**

When carrying out a search during investigation of the premises, as regards any such electronic equipment, Smartphone or e-mail account, the search team is to be accompanied by a qualified Forensic Examiner.

When carrying out a search of the premises, the investigating officer should not use the computer or attempt to search a computer for evidence. The usage of the computer and/or search should be conducted by a properly authorized and qualified person, like a properly qualified forensic examiner.

At the time of search, the place where the computer is stored or kept is to be photographed in such a manner that all the connections of wires including power, network, etc., are captured in such photographs.

The front and back of the computer and/or the laptop while connected to all the peripherals to be taken. A diagram should be prepared showing the manner in which the computer and/or the laptop is connected.

**Seizure of networked devices: Apart from the above steps taken as regards seizure of the computer, laptop, etc., if the said equipment is connected to a network:**

### **WhatsApp Messages:**

In regard to WhatsApp message problem is this that WhatsApp messages are not stored on

server so once message has been send the receiver may very easily edit the messages and if any controversy arise in future in regard to content of message and if it is not saved in the senders mobile then it will be very difficult to prove what message had been sent and receiver may present edited message very easily because once WhatsApp message is delivered it is no more saved on sever like general mobile messages.

In *Rakesh Kumar Singla vs Union of India*<sup>12</sup> relying on WhatsApp chats court granted the bail in an NDPS Act. Gujarat High Court in *Chirag Deepak Bhai Sulekha vs State of Gujarat*<sup>13</sup> granted bail on the basis of WhatsApp chats. In regard to forwarded message on WhatsApp Delhi High Court in *National lawyers campaign for judicial reforms and reforms vs union of India*<sup>14</sup> held that forwarded message cannot be treated as evidence it cannot be treated as 'document' under Indian Evidence Act without having original of forwarded message. In *Sri P. padmanabh vs Syndicate Bank limited Karnataka*<sup>15</sup> High Court held that if computer itself was not in proper condition means it was malfunctioning then output or any information received from such computer cannot be treated as an evidence and should not be relied upon. On the basis of WhatsApp chat Delhi High Court in *Ritu vs state*<sup>16</sup> released the accused of rape. In the same line students of Jindal global University were punished for gang raping and blackmailing their juniors. The conviction was based on WhatsApp chats admitted as evidence.<sup>17</sup>

In case of *Girwar Singh vs CBI*<sup>18</sup> Court appointed committee to check the authenticity of electronic evidence and the committee found that evidence was not the original one but the copy of original one and the evidence was copied a number of time in different devices ultimately Delhi High Court did not accepted such messages as evidence in the case. Bombay High Court in *SBI cards installment and station private limited versus Rohit Jadhav*<sup>19</sup> held that if blue tick is appeared then it will be considered that receiver has opened (and read) the message. If message was notice then it will be presumed that notice was served. It is important to note that court did not consider the other situation in this scenario it is quite possible that in the member of the family may have opened the message or it is also quite was well that in general notice is not served through WhatsApp because if Court is admitting such mode of notice, then there

---

<sup>12</sup> CRM-M no. 23220 of 2020 , Available at : <https://caselaw.in>

<sup>13</sup> Criminal Misc. Application No. 18834 of 2020 Available at : <https://www.livelaw.in>

<sup>14</sup> 2019 SCC OnLine SC 411

<sup>15</sup> 2008 AIR (Kar) 42

<sup>16</sup> 2018 SCC online Delhi 12914

<sup>17</sup> Misc. No. 23 962 of 2017

<sup>18</sup> **(2016) 5 RCR (Cri) 757**

<sup>19</sup> 2018 SCC OnLine Bom 1262



must be a provision in law for such mode of notice.

In recent months a number of media highlighted case has been charge-sheeted on the basis of WhatsApp messages, whether it is TRP conspiracy between republic editor in chief Arnab Goswami and (BARC) CEO partho Das Gupta or whether it is case of North East Delhi by JNU students Sarjil imam and *Pinjra Tod* activist or it is Sushant Singh Rajput case.

So, it can be concluded that for a admissibility of such messages the device must be in good condition and must be in regular use again the sender of such message must have an intention to send those messages then only such messages can be treated as evidence.

**Instagram** conversations can be used as evidence under Section 65B of the Indian Evidence Act. In the preceding precedent, material exchanged on Instagram's parent firm Facebook was provided, thus Instagram conversations can be submitted as evidence. However, the veracity of the screenshots of Instagram discussions may be called into question in court.

**Facebook-** It follows that a court could order the disclosure or production for inspection of content on a social media user's profile even if that content was posted to a private account. It is incumbent on counsel to explain the disclosure requirement to their clients, including informing them that information posted on their Facebook page is fair game.<sup>20</sup>

### III. VIDEO CONFERENCING (VIDEO CALLING) RECORD AS (DIGITAL)

#### EVIDENCE

As per definition of evidence given U/S 3 of Evidence Act evidence includes electronic records produced for the inspection of the Court. This means that evidence, even in criminal matters, can also be by way of electronic records. This would include video- conferencing. The issue in regard to taking of evidence by video conferencing is this that Section 273 of criminal procedure code (Cr.P.C.) does not provide for the taking of evidence by video conferencing. It is also submitted that unless there is an express provision to the contrary, the procedure laid down in Section 273 has to be followed as it is mandatory. Other issue is in regard to Section 280 of Criminal Procedure Code which is related recording of remark on the basis of demeanour of witness by the magistrate. Video conferencing evidence is challenged also on the basis of Section 299 (record of evidence in the absence of the accused) and 317(provision for inquiries and trial being held in the absence of accused in certain cases).<sup>21</sup>

Supreme court in **The State Of Maharashtra v. Dr. Praful B. Desai**<sup>22</sup> dealt with all issue .In

---

<sup>20</sup> 2009] OJ No 681 (QL), at para 28

<sup>21</sup> Dr. K.N. Chandrasekharan Pill (ed), "R.V. Kelkar's Criminal Procedure (Eastern Book Co; 5th edn., 2008)

<sup>22</sup> (2003 (4) SCC 601

regard to first issue (i.e. interpretation of Section 273 Cr.P.C.) supreme court held that Section 273 provides for dispensation from personal attendance. In such cases evidence can be recorded in the presence of the pleader. The presence of the pleader is thus deemed to be presence of the Accused. Thus Section 273 contemplates constructive presence. This shows that actual physical presence is not a must. This indicates that the term "presence", as used in this Section, is not used in the sense of actual physical presence. Recording of evidence by video conferencing also satisfies the object of providing, in Section 273 that evidence be recorded in the presence of the Accused.

In regard to other issues (i.e., requirement of Section 280, 299 and Section 317) court held that there is a need to draw a balance between the right of accused and victim and therefore if the witness for the victim or accused cannot personally appear before court the court has to take device method for effective taking of evidence and deciding the case. Since evidence can be produced by oral or documentary records and electronic record is one such documentary records evidence may be produced through video conferencing. The Accused and his pleader can see the witness as clearly as if the witness was actually sitting before them. During video conferencing accused or his pleader are able to cross examine so it not affects the process of examination laid in CrPC. and Evidence Act. Court is also able to record the demeanour of the witness. The witness can be confronted with documents or other material or statement in the same manner as if he/she was in Court. All these objects would be fully met when evidence is recorded by video conferencing.<sup>23</sup> Thus no prejudice, of whatsoever nature, is caused to the Accused and that's why evidence by way of videoconferencing is admissible as well as reliable.

#### **(A) Analysis of foreign cases on Social media evidence:**

In *Leduc v. Roman*, Justice Brown reasoned that a private social media profile setting would not shield the social media account user from relevant disclosure.<sup>24</sup>

a functioning computer would, that will suffice to show that a computer has been operating properly.<sup>25</sup>

In *R v. Andalib-Goortani* the Court tackled whether to admit a photo found on the internet showing a police officer hitting a woman with his baton. The Crown sought to admit the photograph as evidence of assault; however, experts testifying could not be sure of the integrity of the photograph. The photo was widely circulated on the internet and, as a result, its metadata

---

<sup>23</sup> The State Of Maharashtra V. Dr. Praful B. Desai, 2003 (4) SCC 601

<sup>24</sup> 2009] OJ No 681 (QL), at para 32

<sup>25</sup> David M. Paciocco, (2015), "Proof and Progress: Coping with the Law of Evidence in a Technological Age", 11 C.J.L.T., at p. 193

which shows the “type of camera, focal length, lens type” was missing.<sup>26</sup> An expert concluded that the removal of the metadata resulted “in many uncertainties about the provenance of this photograph and makes it difficult to draw conclusions.”<sup>27</sup> Ultimately, the Crown was unable to convince the Court that the image had not been tampered with. When trying to admit information circulated on the internet, the moving party has to show that the copied information has not been altered during the process. This exercise will likely require the assistance of an expert witness.

In the cases where a printout has been taken from the web page it has to be established that printout has been properly authenticated, it is important to note that a proper legislation is required on this where a printout of web page has been provided it should be separately established that content of the web page was created by the concerned person. This was established in a U.S. case<sup>28</sup> where a printout of Facebook page was presented in court to establish the identity of person. The court further noted that “the mere fact that a page with [the defendant’s] name and photograph happened to exist on the Internet at the time of [the investigator’s] testimony does not permit a reasonable conclusion that this page was created by the defendant or on his behalf.” However, it is important to note that mere raising doubt on web printout will not shift the burden of proof rather the party has to some basis of such doubt otherwise the court will follow the rule of admissibility of electronic record.

In case where a social media user has joined a group and a post or photograph has been posted showing that it has been posted by a member of the group and that other evidence are available to show that concerned is member of a particular group/gang then defense like that the photos lacked proper predicate, that no evidence is available to show that photos were not altered, that there is no evidence that post or photos was created/uploaded by the concerned member etc. however in cases the social media evidence are not supported by other independent evidence then reliability on social media evidence will always be in doubt and defense question raised will always have a great weigh to decide the case. Same was held *Rene v. State of Texas*.<sup>29</sup>

In the cases where it has been established that social media account has been hacked then courts are free to not to take into consideration the evidence obtained from social media like Facebook comment, because in such case it will not be possible who posted the comment and that cannot be associated with social media account holder. In U.S. case where the accused was trying to

---

<sup>26</sup> *R v. Andilib-Goortani*, 2016 ONSC 575 at para 11.

<sup>27</sup> *Ibid* at Para 16

<sup>28</sup> *United States v. Vayner*, 2014 WL 4942227 (2014 2d Cir.

<sup>29</sup> 49 So.3d 248 (2010)

establish the defense by showing the comment on Face book court held that defendant has already established that account has been hacked so court cant not rely on such Facebook comments<sup>30</sup>.

Courts are accepting social media content as evidence around the world now. In ‘Largent v. Reed,<sup>31</sup> The complainant stated that a recent injury had made her life extremely difficult. However, the defendant presented to the court post-accident photographs of the plaintiff that she had put on her Facebook account, which indicated that she had gone to the gym and was feeling good enough to go about her regular activities. The plaintiff was ordered by the court to provide her Facebook login details for further inquiry.

#### **IV. CONCLUSION**

Social media has become an integral part of our lives and has changed the ways in which we communicate and share our personal experiences. As social media platforms take advantage of new technologies, it will be interesting to see how the courts interpret the use of this evidence. While the jurisprudence on electronic evidence is advancing day by day still it is at nascent stage and even of twenty-two years after the passing of Information Technology Act, 2000, we still waiting to see major developments in the subject matter in comparison to other countries judicial system.

\*\*\*\*\*

---

<sup>30</sup> State of Connecticut vs. Eleck, 23 A.3d 818 (2011), 130 Conn.App. 632

<sup>31</sup> PICS Case No. 11-4463 (C.P. Franklin Nov. 8, 2011) Walsh, J. (16 pages). Available at: <https://www.law.com/thelegalintelligencer/almID/1202532928380/>, Visited on: 26-2-23.