

Kamalakanta Tripathy @ Babuli... Vs State Of Odisha & Ors

Court: Orissa High Court

Date of Decision: July 21, 2020

Acts Referred: Code Of Criminal Procedure, 1973 " Section 41(A), 91, 105K, 160, 161, 166A, 465, 468, 469, 482
 Indian Penal Code, 1860 " Section 465, 469
 Information Technology Act, 2000 " Section 43, 66

Hon'ble Judges: S.K. Panigrahi, J

Bench: Single Bench

Advocate: Devashis Panda, Sk. Zafarulla

Final Decision: Dismissed

Judgement

1. The petitioner in this Criminal Misc. Case preferred under Section 482 of the Criminal Procedure Code, 1973 has challenged the Notice No.1373

dated 12.05.2020 issued by the Opp. Party No.2 in connection with Cyber Crime P.S. Case No. 0028 of 2017 corresponding to G.R. Case No.

1731/2017, wherein the petitioner was directed under Section 91 of the Cr.P.C to appear in person along with three seized Laptops on 12.06.2020 and

with a further direction to produce those seized laptops, as they were, without any tampering. Resultantly, it is prayed by petitioner that the said

impugned notice under Annexure-3 dated 12.5.2020 may be quashed and set aside.

2. The factual matrix of the case in hand is that one Madhusudan Padhy, IAS, Transport Commissioner, Odisha lodged a written report on 11.09.2017

before the I.G., Crime Branch, C.I.D. with a request to investigate into a possible "hacking" of his e-mail I.D mspadhi@gmail.com by an

unknown miscreant. Accordingly, on the basis of his report, Cyber Crime P.S. Case No.28 dated 13.09.2017 was registered under Sections 465, 469

of the IPC read with Section 66 of the Information Technology Act, 2000 against an unknown person. Thereafter, a corresponding G.R. Case

No.1731 of 2017 was registered in the Court of learned SDJM, Sadar, Cuttack.

3. The prosecution case, in short, is that the informant received information from one Ashok Nanda on 2.8.2017 which narrates that he received three

emails from an unknown person namely one Prasanta Rath having email ID prasanta.rath007@gmail.com. He further stated that the above e-mails

purportedly related to the account of the informant wherein the said Prasanta Rath had sent a threatening email i.e. "you stop nuisance or we

would go to Crime branch against you". On getting such email, the informant enquired into the matter and found that some unknown miscreant had

probably hacked into his email account and by creating forged electronic record and via a fictitious email ID i.e. prasanta.rath007@gmail.com for

sending those incriminating e-mails. Accordingly, the informant requested for investigation into the matter by the police through its cyber cell.

4. After registration of the case, the Opp. Party No.2 was entrusted with the investigation and immediately registered the case on 13.09.2017 and on

the very next day correspondence was made with Google Inc. USA vide letter No.3119/3120/3121/CID-CB seeking details and information regarding

cobweb of those three e-mail IDs in question i.e. ashoknanda6@gmail.com, prasanta.rath007@gmail.com and mspadhi@gmail.com. Thereafter on

23.09.2017, the I.O received a reply from the legal investigation support team of Google Inc. USA and commenced investigation of the case. It is

pertinent to mention here that in the reply of Google Inc., it was ascertained that the accused has prepared a forged electronic document by using a

pseudonym i.e. Prasanta Rath. By using the said pseudonym, the accused had sent the incriminating emails to Ashok Nanda (who is said to be a

school senior of the informant) to threaten the informant. Taking into account, the entirety of the facts and circumstances, prima facie, it was found

that an offence under different provisions of the I.T Act, 2002 was committed. The Investigating Officer started investigation into the case and she

came to know that the petitioner herein Kamalakanta Tripathy was, in fact, using the said email ID by masking his true identity while sending the

offending emails to the said Ashok Nanda.

5. Having figured out the identity of the accused who was hiding behind an alias, the Opp. Party No.2 further dug into the issue in order to establish

the culpability of the petitioner with the help of some trained agencies since the investigation of this nature involved a lot of technicalities. The

investigation was initially initiated with an anonymous criminal with a masking identity but finally, prima facie, discovered a ghost living behind a shell in

the form of the petitioner Kamalakanta Tripathy. A notice under Section 160 of Cr.P.C was issued on 24.02.2018 asking him to appear before the

I.O. for interrogation and to produce certain documents. Accordingly, the petitioner appeared before the I.O. on 5.3.2018 and his statement was

recorded on the next day and seizure was effected on 17.3.2018 in respect of three laptops wherefrom 3 emails were suspected to have been sent.

After having effected the seizure on the same day i.e. on 17.3.2018, all the three laptops were handed over to the custody/zimnama of the petitioner

with an instruction to produce the same as and when required for the purpose of investigation.

6. The Investigating Officer on 22.03.2018 issued a letter to the BSNL, i.e. internet service provider (ISP) seeking a detailed report regarding the

MAC ID No. of the seized "Router", which was seized from the house of the petitioner. It may be noted here that a media access control

address (MAC address) is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within

a network segment. MAC addresses are primarily assigned by the device manufacturers which are often referred to as the "burned-in" address

or physical address. These are indicative of the physical address/location of the device used. The records show that the investigation continued and

during such investigation on 13.06.2018 a report was received from BSNL i.e. the service provider. The said report intimated that as per available

Internet Protocol Detailed Report (IPDR) record of the router seized from the accused unskinned the MAC address and the seized "Router",

belonged to said Kamalakanta Tripathy i.e. the accused petitioner herein. When the complicity of the accused was prima facie established, the Opp.

Party No.2 herein issued a notice u/s. 41(A) of Cr.P.C to the petitioner on 14.08.2018 and was received by the petitioner on 16.08.2018.

7. It has been submitted that from the available materials and evidence collected thus far, prima facie involvement of accused has been established. In

so far as the motive regarding the crime is concerned, the I.O. during her investigation came to know that there was previous dispute of the accused

with the informant. While the informant helmed as Secretary to the Rural Development, Govt. of Odisha and held additional charge of OMFED

certain irregularities had arisen in connection with the supply of Poly Roll where the petitioner was allegedly involved and some payment was

punitively stopped by the informant. The said factum of long-standing dispute and online intimidation tactics adopted by the petitioner were unearthed

during the investigation. Upon receipt of such a piece of information, the involvement of the accused petitioner was further reinforced and finally the

Opp. Party no.2 issued a notice u/s 91 of the Cr.P.C on 12.5.2020 to produce those three laptops which were given in Zimanama so that investigation

could be completed and charge- sheet could be filed in time.

8. A bare perusal of the FIR demonstrates that Shri Ashok Nanda who was a senior to the informant during his school days informed him

telephonically on 2.8.2017 stating that he had received three emails from one unknown person Prasanta Rath having email ID

prasanta.rath007@gmail.com. He has further stated that the unknown miscreant has attached three emails by intruding into informant's account

and threatened him. The informant, thereafter, requested to Ashok Nanda to forward those three emails to him so that he could look into the matter.

The informant was shocked to see the contents of the three emails. The first email was received from his school seniors email ID i.e.

ashoknanda6@gmail.com which related to the nomination as a visitor to Jharpada jail by the collector which was the subject matter of the email. The

second email was received from email ID nanupany@gmail.com which related to a tender matter of the State. The third email related to supply of

poor quality of calf feed under RKVY scheme by a private supplier to milk farmers of the State. The informant in his complaint has stated that the

nature of all those documents which were forwarded/sent to the said Ashok Nanda said to be purely confidential government documents obtained

illegally by the unknown miscreant which could directly or indirectly offends the data secrecy of the Government. Having gone through the content of

the emails, the informant was sure of the fact that his email account had been hacked by some mischief mongers and apparently, they had access to

his emails and data therein for a dilated time period. The informant has stated that he suspects that the unknown miscreants were hiding behind a

veneer by creating a fake email ID i.e. prasanta.rath007@gmail.com to threaten the informant through his school senior Ashok Nanda.

9. Shri Devashis Panda, learned counsel for the Petitioner has submitted that petitioner has been falsely dragged into the present case despite the fact

that there is no nexus with any of the allegations and he has been made a scapegoat in the entire investigation process at the behest of a Senior IAS

officer of the state. The Criminal Justice system dictates that investigation cannot be perennial and should be completed as expeditiously as possible to

avoid harassment to the accused. He further submits that for verification of IP addresses neither the I.O. nor the police anywhere in India or

worldwide have the necessary facilities that are required to correspond with Google headquarters electronically and get the necessary information

with respect the address of origin of the email which is the subject matter of the current investigation. He also contended that when the laptop

originally seized by the I.O., she should have taken out the contents of the hardware by means of external hard disk drives for the purpose of

ascertaining the source of emails and for further investigation. This was not done but the production of laptops was being requisitioned belatedly only

to prolong the investigation process. The prosecution has the power to seize the incriminating device or any material therefrom and it could have

shortened the delayed investigation process but they chose not to do so.

10. Per Contra, Sk. Zafurulla, learned Additional Counsel for the State has submitted that investigation has been conducted diligently without any

laches which is reflected in the case diary. After due investigation the involvement of the accused was detected and thereafter, a notice u/s of 91 of

the Cr.P.C for production of the three laptops was issued to the Petitioner so that it could enable the I.O. to submit charge-sheet/final form at the

earliest. The Investigation is on the verge of completion and Investigating Officer is going to submit the charge-sheet shortly but the Petitioner is using

the instant petition as a trick to further prolong the submissions of charge sheet. The petitioner has filed this application challenging only a formal

notice issued u/s.91, Cr.P.C for production of three laptops which have been returned back to the accused. Due to non-submission of those laptops

which, in turn, emanates from a binding obligation to cooperate with the investigating agency, the accused is causing undue and probably an intentional

delay in causing the submission of the charge-sheet. The submission of the three laptops before the Investigating Officer shall not cause any prejudice

to him. The law is well settled that no Court shall take cognizance after the expiry of period of limitation provided under Section 468 of the Cr.P.C. In

the instant case, on 13.09.2017 an FIR was registered under Sections 465, 469 of the IPC read with Section 66 of the Information Technology Act,

2002 in which prescribed maximum punishment is up to three years. Therefore, the Court can take cognizance within 3 years from the date of offence

or when the accused was not known, the first day the identity of the offender was known i.e. 06.10.2017 on which date the report from BSNL was

received regarding the involvement of the petitioner herein. It is with this understanding, it is submitted, that there is no delay in completion of the

investigation. Since the investigation is still continuing and the charge-sheet is going to be filed within the stipulated period, therefore, the submission of

the petitioner seeking quashment of the entire criminal proceeding on the ground of delay is not tenable.

11. Heard Ld. Counsel for the parties. The case diary in the instant case was called for and the same has been produced. The case in hand coincides

with an exponential rise in cybercrime, a medium that this petitioner has, prima facie, exploited to hilt to the target with his own narratives. It is

revealed from a perusal of the case diary that the response has been received from Google Inc. which has pointed out that they require all

communication be sent from the end of official government email address backed by appropriate legal documentation seeking any kind of disclosure of

user data. Further, it is revealed from the report of Google that by using the IP address 117.242.188.70 the accused had prepared a fake email

ID in the name of the fictitious person i.e. Prasanta Rath and immediately used the same email ID to send the email in question to Ashok Nanda.

Thus, from the proximity of time span between both the acts, it can be inferred that the objective with which the email ID was created was only to

threaten the informant through his friend. It was further observed from the case diary that BSNL in its reply email dated 16.10.2017 provided the user

details (IPDR) of the IP address which are as under:

User ID :kt2440281_ecdrid@bsnl.in

Name: Tripathy Kamalakanta

Phone No: 0671-2440281

Address: New Malgoldown Road, Gandarpur, College Square, Cuttack, Orissa-753003

Start Time : Tue 01 Aug 2017 16:33:18

Stop Time : Wed 02 Aug 2017 12:43:11

MAC: 00:17:7c:48:dc:11

PORT: 9/4 vlan-id 3318;310 pppoe 9854

BNG: ctk-ras-bng-ctk-01

IP Address: 117.242.188.70

12. There is a further noting, as per the information report obtained from BSNL, that the particular IP address in question is in the name of the

accused herein from which the three emails have been sent to the said Ashok Nanda from the fictitious email ID prasanta.rath007@gmail.com on

2.08.2017. It also transpires from the case diary that correspondences with BSNL as well as Google Inc continued with an effort to obtaining requisite

data and information. Due to the transnational dimension of the issue, the communication as has been received from Google Inc. states that in cases

where a request is issued from non-US government, the said request should be made in accordance with the Mutual Legal Assistance Treaty

(MLAT) and that such request must be protected by way of a treaty i.e. treaty between the government of United States and the government of the

Republic of India. During the course of investigation, a router has been seized from the possession of the accused and its MAC ID has been noted.

Three laptops of Apple (silver colour), Lenovo (black colour) and HP (silver colour) have been seized and later return them back to the accused on

17.03.2018 with an instruction to produce them as and when required. A detailed reply with regard to the IPDR Report has been obtained on

13.06.2018 which indicates that the seized router was being used to hack the email ID of the informant and also to create a fake email ID to entrap

the informant. It is also revealed that the motive behind such an act is arguably more profound since the informant was officiating as the Secretary,

Rural Development Department, Government of Odisha, with an additional charge of OMFED, he had ordered to stop the payment of the accused

due to some irregularity. The said action of the informant has led to dissonance in the mind of the accused which motivated him to adopt illegal means

to wreak vengeance on the informant. It has further come to the fore from the statement recorded under Section 161 of the Cr. P.C dated 13.09.2017

of one Suresh Chandra Attia who was working a Dy. General Manager, Finance OMFED, that the accused used to run a firm called M/s Kamala

Agency and during the financial year 2015-2016 he had supplied Poly Roll to the said OMFED. However, it was observed by the management of

OMFED that the said goods were being supplied at a higher rate by the accused's firm. The informant who was then helmed as Managing

Director of the OMFED had stopped payments of approximately ₹ 6 crores which was due to the accused herein. The documents which have been

mischievously sent from the fictitious email ID are essentially internal documents for the use of senior functionaries of the State Government and deal

with policy issues which have a large-scale administrative, social and financial ramification on the decision-making process of government servants

involved.

13. The details of those documents are not being gone into here as they contain sensitive information with regard to certain tenders. It shocks the

conscience of the court and one shudders at the thought as to how calamitous technology can be in the hands of such reprobates who can sabotage

the e-mail accounts of government functionaries and use the information derived therefrom to arm twist and blackmail them. This court takes a very

serious view of the matter though accuracy, corroboration, and neutrality of the evidence collected are likely to be pipped through a detailed trial

process.

14. The digital age has transformed many aspects of our life experience, but the most obvious yet very much neglected feature of our electronic

governance, has led to a variety of unprecedented and ugly outcomes like the present one. In the Internet Crime Report for 2019, Internet Crime

Complaint Centre, Federal Bureau of Investigation (USA), India stood third among top 20 countries in the world (excluding USA) that are victims of

internet crimes. Alarming, the Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics & Information Technology

Government of India has handled about 2,08,456 incidents in the year 2018 Annual Report of 2018 alone. Further, as per the National Crime Records

Bureau, Ministry of Home Affairs Crimes in India 2018- Statistics Vol 1 the number of cases of cybercrimes increased from 12317 in 2016 to 27248

in 2018. During 2018, 55.2% of cyber-crime cases registered were for the motive of fraud (15,051 out of 27,248 cases) followed by sexual exploitation

with 7.5% (2,030 cases) and causing disrepute with 4.4% (1,212 cases) Crimes in India 2018- Statistics Vol 2 . Out of the total number of cases in

2018, 843 cases were registered in Odisha.

Appositely, the Interpol elucidate the issue of cyber crime as under:

Words and phrases that scarcely existed a decade ago are now part of our everyday language, as criminals use new technologies to

commit cyberattacks against governments, businesses and individuals. These crimes know no borders, either physical or virtual, cause

serious harm and pose very real threats to victims worldwide.

Cybercrime is progressing at an incredibly fast pace, with new trends constantly emerging. Cybercriminals are becoming more agile,

exploiting new technologies with lightning speed, tailoring their attacks using new methods, and cooperating with each other in ways we

have not seen before.

Complex criminal networks operate across the world, coordinating intricate attacks in a matter of minutes.

Police must therefore keep pace with new technologies, to understand the possibilities they create for criminals and how they can be used as

tools for fighting cybercrime.

One cannot be oblivious of the challenges thrown by this new age menace, which are seen to be increasing day by day. Needless to say, the new

methods and techniques adopted by such criminals pose a grave challenge to the investigating agencies as they are intricate both technically and

legally. The inherent differences between the technical and legal systems of different nations, would make investigation into such crimes, having cross

border implications, more complex. However, the challenges thrown in this regard cannot be used to the advantage of a criminal to escape the long

arm of the law. Keeping the above in mind, I may now proceed to examine the present case.

15. On the whole, after having extensively gone through the case records it is trite to prima facie believe that the Investigating Officer has conducted

the investigation thus far diligently and to the best of her ability. However, at this stage a major impediment that has cropped up featuring heavily on

the role of Google Inc. which is protected under the laws of United States. In its response to the query sent to it by the investigating officer, it has

stated that the information requested relates to services offered by Google Inc., a company incorporated in the US and governed by the US laws.

Absent a statutory exemption, Google Inc., is precluded under the US laws from providing the contents of a subscriber's communication by the

Electronic Communication Privacy Act, 18 U.S.C. g 2702(a) as construed and enunciated by the US Circuit Court of Appeals for the Sixth Circuit in

the cases of United States V. Warshak 631 F. 3d 266,282-288 (6th Cir.2010), and by the US Circuit Court of Appeals for the Ninth Circuit in Theofel

v. Farey- Jones 359 F. 3d 1066 (9th Cir 2004). It is thus clear, that the only option available to the investigating officer to secure the evidence available

with Google Inc. is to seek refuge in the remedies available under Indian law especially through "Letters Rogatory".

16. The term "Letters Rogatory" is derived from the Latin term rogatorius (requesting for evidence). Letters Rogatory are the letters of request

sent by the court of one country to the court of another country for obtaining assistance in investigation or prosecution in a criminal matter. The

assistance sought under Letters Rogatories is for service of documents and taking of evidence. Letters Rogatory may be made to any country on the

basis of Bilateral Treaty/Agreement, Multilateral Treaty/Agreement or International Convention or on the basis of assurance of reciprocity and comity

of courts. India has thus far entered in Mutual Legal Assistance Treaty with about 42 countries till date. Google Inc. (as incorporated under the laws

of the United States) as evident from its responses seems to be suggesting that it can only supply the requisite data only through the mechanism

provided under the Treaty. India has signed such a treaty with the United States of America since October 17, 2001 Treaty on Mutual Legal

Assistance in Criminal Matters signed at New Delhi October 17, 2001; transmitted by the President of the United States of America to the Senate

April 8, 2002 (Treaty Doc. 107-3, 107th Congress, 2d Session); reported favorably by the Senate Committee on Foreign Relations October 8, 2002

(Senate Executive Report No. 107-15, 107th Congress, 2d Session); Advice and consent to ratification by the Senate November 15, 2002; Ratified by

the President January 29, 2003; Ratified by India July 1, 2005; Ratifications exchanged at New Delhi October 3, 2005; entered into force October 3,

2005. The treaty inter alia provides assistance will be provided by either of the contracting nations in securing evidence upon the prescribed procedure

being followed.

17. Section 166-A of the Cr P.C provides for issuance of a Letter of request by a competent authority from outside the country. If during the course

of an investigation into an offence a competent investigating officer believes that evidence may be available in a foreign country, the competent

Criminal Court may issue a letter of request to a Court or an authority in that country competent to deal with such request. Such request may also be

for the purpose of examining orally any person supposed to be acquainted with the facts and circumstances of the case and also may require such

person to produce any piece of evidence which may be in his possession pertaining to the case. It is further provided that every such statement

recorded or document or thing received thereunder shall be deemed to be the evidence collected during the course of investigation. Section 105-K of

the Cr.P.C. provides that such a request may be made in the manner as provided for by the Central Govt. Pursuant to the aforesaid enabling provision,

the Central Govt. has framed comprehensive guidelines called the Guidelines on Mutual Legal Assistance in Criminal Matters dated 4.12.2019 which

outlines detailed procedure to be followed after invoking the aforesaid provisions.

18. The Supreme Court of India has from time to time dealt with the issuance of such "Letter Rogatories" as was done in the case of Union of

India v. W.N. Chadha 1993 Supp (4) SCC 260 wherein it was held that "Letter Rogatory" is a formal communication in writing sent by a Court in

which action is pending to a foreign Court or Judge requesting the testimony of a witness residing within the jurisdiction of that foreign Court may be

formally taken thereon under its direction and transmitted to the issuing Court making such request for use in a pending legal contest or action. It has

also been held, that at the investigative stage, the accused had no right to contest the issuance of the letter rogatory and need not be heard before

issuance of the same. The same view was upheld in Dinubhai Boghabhai Solanki v. State of Gujarat (2014) 4 SCC 626. Further in the case of Janata

Dal v. H.S. Chowdhary (1992) 4 SCC 305 the question arose as to whether the Investigating Agency (CBI in that case) needed to convince the Court

that the allegations against the accused were satisfactorily established before requesting a letter rogatory. The Supreme Court did not find merit in the

argument and ordered that the issuance of the letter rogatory was to remain unaffected and was to be proceeded with in accordance to law. In the

case of CBI v. Ashok Kumar Aggarwal (2013) 15 SCC 222 the Hon'ble Apex Court held that the documents sent in reply to a letter rogatory

issued under Section 166 A of the Cr.P.C are "evidence collected during course of investigation".

19. Indian courts have from time to time, depending on the facts of the case, supported the move to issue such requests both for the purposes of

collecting evidence as well as for conducting investigation which have been aptly reiterated in cases like Paramjit Singh Gulati vs. Directorate of

Revenue Intelligence MANU/DE/0735/2020 Ravina Associates Pvt. Ltd. vs. Additional Commissioner of Income Tax 2018 (64) ITR (Trib) 149

(Delhi) Ashok Kumar Aggarwal vs. CBI and Ors. 2016 Cri LJ 2410 Harsh W. Chadha vs. DDIT [2011] 43 SOT 544 (Delhi) Oommen vs. Union of

India (ILR 2017 (4) Kerala 607)

20. The FIR in the instant has been lodged under Section 465 of the IPC which provides for the punishment of forgery, Section 469 of the IPC

provides that whoever commits forgery with an intention or knowledge that such a forged document or electronic record is likely harm the reputation

of a person shall be punishable with a maximum term of 3 years and fine. Section 66 of Information Technology Act, 2002 states that when a person

dishonestly or fraudulently does any of the acts referred to in Section 43 of the Act shall be punishable with a term of 3 years and fine. Section 43 of

the said Act provides for a host of offences which have been made punishable including when any person without permission of the owner of a

computer or computer network accesses such computer or computer network and downloads, copies or extracts any data or information from such

computer or computer network shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Such an offence in common parlance is referred to as "hacking".

21. "Hacking" in a layman's understanding simply means gaining unauthorized access to a computer or a computer network. When a person

destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means with

intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person, he is said to have committed an offence of

hacking under Section 66 of the Act. The person, who commits an offence of hacking is called "hacker". However, over time, such knowledge of

electronic intrusion has been weaponized by wanton elements to wreak vengeance or blackmail hapless victims. Plainly put, within the legal confines,

hacking, means willful and malicious computer trespassing and make a critical impact on the network security. The culpability of hacking depends on

the presence of mens rea or the object with which the act was carried out for it to be punishable under Section 66 of the IT Act.

22. The investigation thus far has been able to establish that the IPDR report obtained from the internet service provider (ISP) i.e. has indicated that

the IP Address: used was "117.242.188.70". The said IP address is a static address which remains constant and never in a state of flux. The

MAC ID of the router has also been obtained. It is thus clear that the router seized from the accused has been used from the aforesaid IP address

which in turn matches with report of Google that the said IP address i.e. "117.242.188.70". The said IP address has been fraudulently used to

create the fake email ID which has been used to send the confidential documents as well as to mail the informant's friend. Thus, from a conjoint

reading of the above facts, prima facie, imply that the accused herein has hacked into the email account of the informant. In this context, a thorough

trial is very much required to testify the prima facie view of the case in hand.

23. In the facts and circumstances of the case, considering that the email account of a Senior IAS Officer of the State has been hacked so as to

illegally obtain sensitive and confidential documents, the Investigating Officer may do well to follow the procedure referred to hereinabove so as to

obtain further evidence as may be required by seeking issuance of a letter rogatory from the competent court to aid in its investigation.

24. In so far as the question of using the inherent powers of this court to quash vexatious proceedings or proceedings which are used to abuse the

process of court are concerned. The Hon'ble Apex Court over the years has more or less crystallized as to when such powers may or may not be

used. In the case of Parbatbhai Aahir and Ors. vs. State of Gujarat and Ors (2017 (9) SCC 641, it has been held that in forming an opinion whether a

criminal proceeding or complaint should be quashed in exercise of its jurisdiction under Section 482 of the Cr.P.C., High Court must evaluate whether

the ends of justice would justify the exercise of the inherent power. In the case of State of Haryana vs. Bhajan Lal 1992 Supp (1) SCC 335 the

Hon'ble Supreme Court has extensively dealt with the scope of the powers under Section 482 of the Cr.P.C. to quash a proceeding holding that it

should not be used mechanically or routinely, but with care and caution, only when a compelling case for quashing is made out. The said judgment has

also laid down an indicative guidelines for this purpose. The Hon'ble Supreme Court recently in the case of Google India Private Limited vs.

Visakha Industries and Ors 2019 SCC Online SC 1587 reiterated the guidelines laid down in Bhajan Lal's Case (supra). The position that the

inherent power of the High Court can be exercised under Section 482 Cr.P.C only in respect of a proceeding pending before an inferior criminal court

is well settled as held in the cases of Kurukshetra University v. State of Haryana (1977) 4 SCC 451 State of W.B. v. Sujit Kumar Rana²⁰ and State of

Punjab v. Davinder Pal Singh Bhullar (2004) 4 SCC 129 . But merely because a FIR is sent to the Magistrate it cannot be said that a case is pending

before the Magistrate. A case can be said to be pending before the Court only if the Court, after taking cognizance of the offence on a police report

issues process to the accused. Then only the accused can be said to have been proceeded against. Strictly speaking, at this stage only the accused

gets the right to challenge the proceedings before the court and possibly to ask for the relief of quashing the proceedings including, the charge-sheet,

under Section 482 of the Cr.P.C., any of the grounds available to him. This view of the matter is in tune with the law laid down by the Hon'ble

Supreme Court in Union of India v. W.N. Chadha, Narender 1993 Supp (4) 260 G. Goel v. State of Maharashtra (2009) 6 SCC 65 , Simon v. State of

Karnataka (2004) 2 SCC 694, Mohd. Kalam v. State of Rajasthan (2008) 11 SCC 352 etc. holding that the accused have no right to interfere with the

investigation by the police. In Sri Bhagwan Samardha Sreepada Vallabha Venkata Vishwanandha Maharaj v. State of A.P. (1999) 5 SCC 740 it has

also been held that the accused does not have any right to question "further investigation" conducted under Section 173(8) Cr.P.C. Thus, until the

matter reaches the Court and a stage has reached when it could be said that the case is pending before the Court, there cannot be any plea of abuse

of the process of Court or a right to challenge the FIR under Section 482 Cr.P.C. The main factor to be considered while exercising its inherent

powers under Section 482 Cr.P.C is to ascertain as to whether the complaint has been taken at its face value discloses the commission of an offence

or not, this view is strewn through a series of judgments as in the case of T. Vengama Naidu v. T. Dora Swamy Naidu & Ors (2007) 12 SCC 93,

Dhanalakshmi v. R. Prasanna Kumar & Ors 1990 (Supp) SCC 686, State of Madhya Pradesh v. Yogendra Singh Jodan and Anr 2020 SCC Online SC

111, Sushil Sethi and Another v. The State of Arunachal Pradesh & Ors. (2020) 3 SCC 240. In the instant case, the facts and evidence on record

clearly point towards the involvement of the Petitioner in the alleged offence. Hence, he is not entitled to any such indulgence as prayed for in the

instant case at this stage.

25. Further, in the instant case, the contention of the accused Petitioner is that delay in investigation has been caused due to the prosecution, cannot be

lent any credence due to the fact that Section 468 (2)(c) of the Cr.P.C. mandates that the period of limitation shall be three years, if the offence is

punishable with imprisonment for a term exceeding one year but not exceeding three years, the same also draws support from a conjoint reading of

Section 468 (3), Section 473 and Section 173 of the Code. Thus, from the facts and evidence borne out from the records of the case, it is crystal clear

that the investigation has been carried out diligently and it is well within time. In fact, no undue delay has been caused by the prosecution, rather the

delay has been caused by the accused petitioner who has evaded the process of law by causing non-production of the laptops before the I.O. for

further investigation.

26. Considering the aforesaid discussion, submissions made and taking into account a holistic view of the facts and circumstances of the case at hand,

this Court is not inclined to entertain the instant petition. Accordingly, the present petition u/s 482 of the Cr.P.C. filed on behalf of the

accused/petitioner stands rejected. The petitioner has also preferred I.A. No. 655 of 2020 wherein a prayer has been made to stay the operation of

the Notice No.1586 dated 10.6.2020 and an I.A. No.636 of 2020 with the prayer to ascertain and produce the status report of the investigation in

relation to the present petition. Since the instant petition has been dismissed, therefore, these I.As. do not survive and accordingly stand dismissed.