IN THE HIGH COURT OF JUDICATURE AT BOMBAY
NAGPUR BENCH, NAGPUR.

CRIMINAL APPLICATION (APL) NO. 792 OF 2019

1. Pravin Shyamrao Samarth
Aged:- Major, Occ.: Service,
R/o Metro House, Anand Nagar,
Civil Lines, Nagpur — APPLICANT

//VERSUS//

1. The State of Maharashtra,
Through Police Station Officer,
Police Station, Sadar
2. Shri Ashish Kumar Tribhuvan Sanghi
Aged 44 years, Occ.: Additional
Chief Project Manager, Telecom,
R/o 28/02, Metro House, Anand,
Nagar, Civil Lines, Nagpur — NON-APPLICANTS

Mr. S.P. Bhandarkar, Advocate for the applicant.
Mr. Nikhil Joshi, APP for non-applicant No.1/State.
Mr. G.A. Kunte, Advocate for non-applicant No.2.

CORAM : URMILA JOSHI PHALKE, J.

JUDGMENT RESERVED ON:- 02.04.2026
JUDGEMENT PRONOUNCED ON:-08.04.2026

ORAL JUDGMENT :

1. Heard.

2. ADMIT. Taken up for final disposal with the consent of learned counsel for the parties.

3. The present application is preferred by the applicant for quashing of the First Information Report in connection with crime No.305/2019 registered with the non-applicant No.1-Police Station Sadar, District Nagpur City under Section 66 B of the Information Technology Act, 2000 and under Section 3(1)(c) of the Official Secrets Act, 1923 and consequent proceeding arising out of the same bearing Charge-sheet No.246/2020.

4. Crime is registered on the basis of the report lodged by non-applicant No.2- Ashish Kumar Tribhuvan Sanghi on an allegation that present applicant namely Pravin Shyamrao Samarth was working as Assistant Manager for the period of three years. The work assigned to him was to connect the conference calls between Managing Director and other Directors via intercom system which was in the control room. The calls were connected as stated earlier between Managing Director and other Directors. On 09.07.2019 the Director (Finance) received a audio recording clip in which conversation of one Mr. Brijesh Dixit and other Project Director Shri Mahesh Kumar was recorded. On hearing the said audio clip, the authorities called upon present applicant as well as one Lokesh Gahane and made enquiries with

them. At the relevant time, said application disclosed that on the request of Mr. Vishwaranjan Beora who is having some inter departmental disputes had asked the present applicant to record the said call and on his instruction, he has recorded the said calls. His mobile phone was verified and audio clips were found in his mobile phone between him and Mr. Beora. On the basis of the said FIR the crime came to be registered.

5. After registration of the crime Investigating Officer has recorded the relevant statements of the witnesses. Seized mobile phones which are sent for the analysis and after completion of the investigation submitted charge-sheet against the present applicant.

6. Heard Mr. S.P. Bhandarkar, learned counsel for the applicant who submitted that applicant is an employee of Maharashtra Metro Corporation Limited. As per the allegation he recorded the conference call and shared the same information with Vishwaranjan Beora who is working in different department. The call which was recorded was viral and during inquiry it reveals that said call was recorded by the present applicant. He submitted that even accepting the allegation the said conference

call was opened to all. Anybody can hear that call and therefore, there is nothing wrong committed by the present applicant. He submitted that offence under Section 66(B) itself is not made out which deals with punishment for dishonestly receiving stolen computer resource or communication device. He submitted that there is no allegation that present applicant retains any stolen computer resource or communication device and therefore, the offence under Section 66(B) of the Information Technology Act, 2000 is not made out. He further submitted that at the most, it would be misconduct on his part for which he has already punished by suspending his services. He invited my attention towards the entire investigation papers and submitted that from none of the statement it reveals that present applicant has shared the information with somebody else which would cause the loss to the company or it would affect the sovereignty and integrity of the country. Therefore, the offence under Section 3 of the Official Secrets Act is also not made out.

7. In support of his contentions he placed reliance on the decision of the Hon'ble Apex Court in the case of ***Vineet Kumar and ors. vs. State of Uttar Pradesh and another*** reported in

(2017) 13 SCC 369, Aditya Mehta vs. The State of Maharashtra and another in *Criminal Application No.224/2016* decided on *16.10.2020, Ramesh Rajagopal vs. Devi Polymers Private Limited* reported in *(2016) 6 SCC 310 and Zishan Mukhtar Hussain Siddiqui vs. The State of Maharashtra* in *Criminal Writ Petition No.3894/2022* decided on *28.11.2022.*

8. Per contra, learned APP and learned counsel for the non-applicant No.2 strongly opposed the said contention and submitted that from the recitals of the FIR itself apparently clear that work of the present applicant was connecting conference call. However, he has recorded conference call on his mobile and transferred it to some other person. The said clips are under the process of recovering and investigation is already completed. During investigation it reveals that Investigating Officer, Crime Branch has seized the mobile phone of the applicant/accused and sent it for analysis. The audio clip as mentioned in the complaint was transferred in compact disk and chemical analysis report has also been received by the prosecution. The said report discloses the involvement of the present applicant in the alleged offence. In view of that, the application deserves to be rejected.

9. On hearing both the sides and on perusal of the investigation paper it is not in dispute that present applicant was the employee of the Maharashtra Metro Corporation. He was assigned with the duty of connecting the conference call. Accordingly, on the day of incident, he has connected the call between Brijesh Dixit and other Project Director Shri Mahesh Kumar. The said conference call was recorded by the present applicant and said information was shared by him with one Vishwaranjan Beora who is working in another department. During investigation mobile phones of the present applicant and other co-accused Vishwaranjan Beora were seized. The analysis report which is filed on record shows that Analyst of Cyber Forensic Expert, Nagpur found call recording between Mr. Pravin Samarth and Mr. Vishwaranjan Beora. It was also found voice recording recorded by Mr. Pravin Samrath which had conference calls between the Metro Officials. The Analyst also found that call Logs between " Mr. Vishwaranjan Beora and Mr. Pravin Samarth," "Mr. Prashant Pawar and Mr. Praveen Samarth", "Mr. Swami and Mr. Praveen Samarth". Similarly, in mobile phone of Beora he found call logs between Mr. Prashant Pawar and Mr. Vishwaranjan

Beora and Mr. Swami and Mr. Vishwaranjan Beora. Some SMS also found sent by Mr. Swami to Mr. Vishwaranjan Beora.

10. The Cyber Forensic Expert Report further shows that he has collected the Laptop and Desktop Hard drive from Mr. Anil Taksande then he performed the imaging of the Hard Drives with Cyber Forensic Software FTK Image (the imaging process is accomplished according to the cyber forensic investigation procedure which says “that the investigation should be performed on the imaged copy of evidence”). After the imaging process he investigated by following the process of the Hard drives using Cyber Forensic Tool OS Forensics and noted his observations. His observations are as follows:-

A) In Desktop Hard drive.

During the analysis of the USB Logs, he found that number of External devices were connected to the official PC of Mr. Vishwaranjan Beora, which shows that he may have been using these external devices to transfer the official data for his personal use. (Refer Annexure-1- in Pendrive).

During the analysis of the Browsing History log, (Refer Annexure-2 in Pendrive) -he found that some documents

(Maha Metro Complaint/PMO, Election Commission) were sent through the Email of Mr. Vishwaranjan Beura. He found that Mr Vishwaranajn Beura used to open his Whatsapp in Desk top through web.whatsapp.com and had downloaded some documents (Prime Minister.docx) through WhatsApp.

11. During the Analysis he also found some Documents (Refer Annexure- 3 in Pendrive) which has- A letter written by Mr.Vishwaranjan Beura to the Honorable President of India having Subject "Violation of Model Code of Conduct by Maharashtra Metro Rail Corporation Ltd during Central Election 2019.

12. A Letter written by Mr.Vishwaranjan Beura to Shri Sunil Arora, Chief Election Commissioner having Subject "Violation of Model Code of Conduct by Maharashtra Metro Rail Corporation Ltd. During Central Election 2019" (These document were the same documents as released in the press conference).

13. The transaction between present applicant and said Beora also shows that present applicant has transferred the information as to some tender to the said Beora.

14. Though learned counsel for the applicant submitted that this information is opened to all and therefore, no offence is committed by the present applicant. He submitted that there is no such secret in it.

15. Learned counsel for the non-applicant No.2 was asked to furnish on record any Rules or Manual as far as working pattern of the employees of Maharashtra Metro Corporation is concerned, he could not produce the same on record. He has only produced on record the office order which shows that present applicant was assigned with the duty to (1) maintain telephonic in the NMRCL Premises in working order, (2) Liaison with the service providers BSNL, Idea for NMRCL works, (3) maintain all the files and correspondence related with Signal and Telecommunications, (4) Execution of telecom related contracts and works. (5) Maintenance of computers, printers and other IT related hardware, preventive maintenance and breakdown attention, (6) any other work related to Signaling and Telecommunications.

16. I have perused the Maharashtra Metro Rail Corporations Limited Rules.

Rule-2 defines Applicability:-

These rules apply to all employees those in casual employment or paid from contingencies; those who are inducted on re-employment, consultant, retainership basis.

Rule-4. GENERAL CONDUCT OF THE EMPLOYEE.

4.1 Every employee of the Corporation shall at all times;

(a) Maintain absolute integrity to the Corporation.

(b) Maintain devotion to duty; and

(c) Do nothing which is unbecoming of a public servant.

4.2 Every employee of the Corporation holding a Supervisory/ Executive post shall take all possible steps to ensure integrity and devotion to duty of all employees for the time being under his control and Authority.

Rule-5 deals with MISCONDUCT specially Rule 5.4 and 5.5 which are reproduced as under:-

5.4 Furnishing false information regarding name, age, father's name, qualification ability or previous service or any other matter germane to the employment at the time of employment or during the course of employment.

5.5 Acting in a manner prejudicial to the interest of the Corporation. At the same time Rule 5.17 is also material which states that "Commission of any act which amounts to a criminal offence involving moral turpitude."

17. As far as present matter is concerned, Rule 11 is of utmost importance which deals with Unauthorized communication of information:-

No employee shall, except in accordance with any general or special order, the Corporation or in the performance in good faith of the duties assigned to him communicate, directly or indirectly, any official document or any part thereof to any officer or other employee, or any other person to whom he is not authorized to communicate such document or information.

Similarly **Rule-28** deals with **ETHICAL CONDUCT.** Sub rule 28(1) states that every employee of Maharashtra Metro shall deal on behalf of the company with professionalism, honesty and integrity, while conforming to high moral and ethical standards. Such conduct shall be fair and transparent and be perceived to be so by third parties.

Similarly **Rule- 34** deals with **INTEGRITY OF DATA FURNISHED** which states that every employee of Maharashtra Metro shall ensure, at all times, the integrity of data on information furnished by him/her to the company. He/she shall be entirely responsible in ensuring that the confidentiality of all data is retained and in no circumstance transferred to any outside person/party in the course of normal operations without express guidelines from or, the approval of the management.

18. In the light of the above Rules, it has to be seen whether the applicant has committed an offence punishable under Section 66(B) of the Information Technology Act. Section 66 deals with computer related offences which specifically states that if any person, dishonestly or fraudulently, does any act referred to in Section 43, shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

19. Section 66(B) deals with punishment for dishonestly receiving stolen computer resource or communication device

which reads as under “whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reasons to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both”.

20. As Section 66 refers Section 43 of the Information Technology Act, therefore, both Sections required to be read conjointly. Section 43 under Chapter IX of the Information Technology Act deals with Penalties and compensation and adjudication.

Section 43 reproduced as under:-

“penalty and compensation for damage to computer, computer system, etc. If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network (a) accesses or secures access to such computer, computer system or computer network [or computer resource];

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer

network in contravention of the provisions of this Act, rules or regulations made thereunder;

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network;

(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

(j) steal, conceal, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;] [he shall be liable to pay damages by way of compensation to the person so affected.]

Explanation.--For the purposes of this section,--

(i) "computer contaminant" means any set of computer instructions that are designed--

(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(b) by any means to usurp the normal operation of the computer, computer system, or computer network;

(ii) "computer data-base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

(iv) "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

[(v) "computer source code" means the listing of programme, computer commands, design and layout and programme analysis of computer resource in any form.]

21. Here in the present case, specially Section 43(1)(b) is relevant which states that if any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium is said to have committed an offence under Section 66.

22. In simple words Section 66 of the Information Technology Act makes it crime to misuse computer or other electronic device if he do it with dishonest intention. If any person dishonestly or fraudulently performs any act listed in Section 43 of the Information Technology Act, such as gaining unauthorized access to a computer system, downloading data,

introducing a virus, causing damage or denies authorized access said to have committed a criminal offence.

23. The Hon'ble Apex Court in the case of ***Gagan Harsh Sharma vs. State of Maharashtra and others*** reported in ***(2019) Cri.L.J. 1398*** in paragraph No.17 observes as follows "applying the aforesaid principles to the facts involved in the case, perusal of the complaint would reveal that the allegations related to the use of the data code by the employees of the complainant company by accessing the Code and stealing the said data by using the computer source code. The Act of accessing or securing access to computer/computer system or computer network or computer resources by any person without permission of the owner or any person who is in charge of the computer, computer system, computer network or downloading of any such data or information from computer in a similar manner falls within the purview of Section 43 of the Information Technology Act, 2000. When such Act is done dishonestly and fraudulently it would attract the punishment under Section 66 of the Information Technology Act, such Act being held to be an offence. The ingredients of dishonestly and fraudulently are the

same which are present if the person is charged with Section 420 of the Indian Penal Code, 1860. The offence of Section 379 in terms of technology is also covered under Section 43. Further, as far as Section 408 is concerned which relates to criminal breach of trust, by a clerk or servant who is entrusted in such capacity with the property or with any dominion over property, would also fall within the purview of Section 43 would intends to cover any act of accessing a computer by a person without permission of the owner or a person in charge of computer and/ or stealing of any data, computer data base or any information from such computer or a computer system including information or data held or stored in any removable storage medium and if it is done with fraudulent and dishonest intention then it amounts to an offence. The ingredients of an offence which are attracted by invoking and applying Sections 420, 408, 379 of the Indian Penal Code are covered by Section 66 of the Information Technology Act, 2000 and prosecuting the petitioners under the both Indian Penal Code, 1860 and Information Technology Act would be a brazen violation of protection against double jeopardy.

24. It is further held that in paragraph No.28 as " in such circumstances if the special enactment in form of the Information Technology Act contains a special mechanism to deal with the offences falling within the purview of Information Technology Act, then the invocation and application of the provisions of the Penal Code, 1860 being applicable to the same set of facts is totally uncalled for.

25. Here in the present case, the allegation levelled against present applicant is that he was assigned with duty as Assistant Manager Telecom and work of the said applicant is to connect conference call between Managing Director and other Directors via intercom system which was in the control room. The calls were connected as stated earlier between Managing Director and other Directors but he has recorded the conversation between Brijesh Dixit and other Project Director Shri Mahesh Kumar. During investigation mobile phone of the present applicant was seized and the analysis report shows that the call recordings between present applicant and other co-accused Vishwaranjan Beora was also found. It was further found that the voice recording recorded by present applicant which had conference

calls between metro officials. Thus, it reveals that present applicant who was only assigned with the duty to connect the conference call has not only connected but he has recorded communication between two officials and shared the same with one Mr. Vishwaranjan Beora. It further reveals during the investigation that communication between the present applicant and said Beora further discloses that the present applicant has shared information with the said Beora. In view of the Rules which are already referred show that it was not only a misconduct on the part of the present applicant but it is an unauthorized communication regarding information of the department which was shared by the present applicant with an employee of another department. Rule 11 of the Maharashtra Metro Rules Corporations Limited itself shows that no employee shall, except in accordance with any general or special order of the Corporation or in the performance in good faith of the duties assigned to him communicate, directly or indirectly, any official document or any part thereof to any officer or other employee, or any other person to whom he is not authorized to communicate such document or information. Thus, it is not only an unethical conduct on his part but the dishonest intention can be inferred from the circumstances

that he has not only recorded said calls but also shared the said calls with other co-accused.

26. Thus, in view of Section 43 and Section 66 of the Information Technology Act the allegations relate to the use of communication by the employee of the complainant company by recording the conference call sharing without permission of the communicators or any other person who is in-charge of the said system and sharing it to other person falls within the purview of Section 43 of the Information Technology Act. When such act is done dishonestly or fraudulently it would attract the punishment under Section 66 of the Information Technology Act. The ingredients of dishonesty or fraudulent are the same which require to be considered in view of Section 420 of IPC. As far as dishonest intention is concerned, which prima-facie reveals from the fact that he has shared the said information with the person who is working in another department. Thus, prima-facie offence under Section 66 read with Section 43 is made out against the present applicant. Merely because Investigating Agency has applied wrong section by mentioning Section 66 (B) is not sufficient to quash FIR against the applicant.

27. After going through the entire recitals of the FIR and investigation papers the case of the present applicant would cover under Section 43(b) of the Information Technology Act which is punishable offence under Section 66 of the Information Technology Act.

28. The applicant is also charged for the offence punishable under Section 3(1) of the Official Secrets Act, 1923. Admittedly, considering Section 3 of the Official Secrets Act which deals with penalties for spying. In view of Section 3(1)(c) - if any person for any purpose prejudicial to the safety or interests of the State obtains, collects, records or publishes or communicates to any other person any secret official code or pass word, or any sketch, plan, model, article or note or other document or information which is calculated to be or might be or is intended to be, directly or indirectly, useful to an enemy [or which relates to a matter the disclosure of which is likely to affect the sovereignty and integrity of India, the security of the State or friendly relations with foreign States] he shall be punishable with imprisonment for a term which may extend, where the offence is committed in relation to any work of defence, arsenal, naval,

military or air force establishment or station, mine, minefield, factory, dockyard, camp, ship or aircraft or otherwise in relation to the naval, military or air force affairs of Government or in relation to any secret official code, to fourteen years and in other cases to three years. The contents of the FIR states that the aforesaid allegations against the present applicant, the statement of alleged witnesses recorded during the course of investigation and made part of charge-sheet.

29. On perusal of Section 3 of the Official Secrets Act which provides penalties for spying. In the context of the definition given under Section 2(8) of the Official Secrets Act of 'prohibited place'. Admittedly, the spot of incident is not prohibited place. The said definition does not specifically include the place i.e. office of the complainant company as a prohibited place. Therefore, the offence under Section 3 of the Official Secrets Act is not made out against the present applicant. The invocation of Section 3 of the Official Secrets Act prima-facie appears to have been invoked under the misconception. By no stretch of imagination it can be said that recording of the said calls as stated aforesaid be an act constituting an offence of spying.

The word spying has different meaning. Section 3 of the Official Secrets Act provides punishment for acts, prejudicial to the safety or interests of the State; acts done affecting the sovereignty and integrity of India and so on i.e. for the acts stipulated therein. Prima-facie it is apparent that the Official Secrets Act applied by the Investigating Agency is under wrong conception. Section 3 could have been invoked in the facts of the present case when there is any apprehension due to act of the present applicant to the sovereignty or integrity of India. In view of that, the offence under Section 3 of the Official Secrets Act is not made out.

30. The present application is preferred by the applicant for quashing of the FIR. The legal position is well settled that when prosecution at the initial stage is asked to be quashed, the test to be applied by the Court is as to whether the uncontroverted allegations as made prima-facie established the offence. It is also for the Court to take into consideration any special features which appear in the particular case to consider whether it is expedient and in the interests of justice to permit a prosecution to continue. This is so from the basis of that the Court cannot be utilized for any oblique purpose and when the opinion of the Court that

chances of an ultimate conviction are less and therefore, no useful purpose is likely to be served by allowing criminal prosecution to continue, the Court may while taking into consideration special facts of a case also quashed the proceeding even though it may be at a preliminary stage.

31. Therefore, the parameters laid down by the Hon'ble Apex Court in the case of **State of *Haryana and others vs. Bhajanlal and others*** reported in ***1992 Supp(1) Supreme Court Cases 335*** are relevant. It reads as under:-

> *" (a) where the allegations made in the First Information Report or the complaint, even if they are taken at their face value and accepted in their entirety do not prima facie constitute any offence or make out a case against the accused;*
>
> *(b) where the allegations in the First information Report and other materials, if any, accompanying the F.I.R. do not disclose a cognizable offence, justifying an investigation by police officers under Section 156(1) of the Code except under an order of a Magistrate within the purview of Section 155(2) of the Code;*
>
> *(c) where the uncontroverted allegations made in the FIR or 'complaint and the evidence collected in support of the same do not disclose the commission of any offence and make out a case against the accused;*
>
> *(d) where the allegations in the FIR do not constitute a cognizable offence but constitute only a non-cognizable offence, no investigation is permitted by a police officer without an order of a Magistrate as contemplated under Section 155(2) of the Code;*
>
> *(e) where the allegations made in the FIR or complaint are so absurd and inherently improbable on the*

basis of which no prudent person can ever reach a just conclusion that there is sufficient ground for proceeding against the accused;

(f) where there is an express legal bar engrafted in any of the provisions of the Code or the concerned Act (under which a criminal proceeding is instituted) to the institution and continuance of the proceedings and/or where there is a specific provision in the Code or the concerned Act, providing efficacious redress for the grievance of the aggrieved party;

(g) where a criminal proceeding is manifestly attended with mala fide and/or where the proceeding is maliciously instituted with an ulterior motive for wreaking vengeance on the accused and with a view to spite him due to private and personal grudge.

32. By applying the same to the facts of the present case the application deserves to be allowed partly. Accordingly, I proceed to pass the following order:-

ORDER

(i) The Criminal Application is allowed partly.

(ii) The First Information Report in connection with crime No.305/2019 registered with the non-applicant No.1-Police Station Sadar, District Nagpur City for the offence punishable under Section 3(1)(c) of the Official Secrets Act, 1923 and consequent proceeding arising out of the same bearing Charge-sheet No.246/2020 is quashed and set aside to the extent of

offence punishable under Section 3(1)(c) of the Official Secrets Act.

(iii) The prosecution would continue against the applicant as far as offence under Sections 66 and 66(B) of the Information Technology Act is concerned.

33. The criminal application stands disposed of in the above said terms.

Pending applications, if any, also stand disposed of.

(URMILA JOSHI PHALKE, J.)

manisha