

**IN THE HIGH COURT OF JUDICATURE AT BOMBAY
CRIMINAL APPELLATE JURISDICTION**

CRIMINAL APPLICATION NO.1217 OF 2018

Mr.Ajay Murlidhar Batheja

Residing At #2 Rajab Mahal

Oval Maidan, Mumbai – 400 020.

...Applicant

V/s.

1. State of Maharashtra

(At the instance of Cyber Police Station)

2. Manoj Prabhakar Joshi

Senior Manager of Mahanagar Telephone

Nigam Ltd., CBCRM-O & M,

Telephone Exchange, Cuffe Parade,

Mumbai.

...Respondents

Mr.Pranv Badheka a/w Mr.R.S. Niranjana, P.V. Babar i/b Mr.A.P. Ghag for the Applicant in APL No.1217 of 2018.

Mr.K.V. Saste, APP for the Respondent-State in APL No.1217 of 2018.

CORAM : RANJIT MORE &

SMT.BHARATI H. DANGRE, JJ.

RESERVED ON : 19th OCTOBER 2018

PRONOUNCED ON : 26th OCTOBER 2018

JUDGMENT : (Per Smt.Bharati H. Dangre,J)

1. The applicant, Chief Executive Officer cum Director of one Xalted Information System Pvt. Ltd. incorporated under the

provisions of the Companies Act, 1956 have approached the Court praying for exercise of its inherent jurisdiction for setting aside CR No.01 of 2018 registered with Cyber Police Station, Mumbai for under Section 43, 65 and 66 of the Information Technology Act r/w Section 420, 34 of the Indian Penal Code. The applicant has also prayed for interim relief to the effect that the investigation in connection with the impugned FIR be stayed and the respondent No.1 be directed not to file charge-sheet in connection with the subject C.R.

2. It would be appropriate for us to refer to the factual background in which the aforesaid relief is sought. One Mr. Manoj Prabhakar Joshi working as Senior Manager (CBCRM-O & M) at Mahanagar Telephone Nigam Ltd., Cuffe Parade, Mumbai lodged a complaint with the Cyber Police Station on 01.02.2018. In the said complaint it is stated that he is assigned the duty of maintenance and management in respect of CBCRM (Conversant Billing Customer Relation Management). It is alleged in the said complaint that on 13.10.2017 the Deputy General Manager (IT), New Delhi vide his letter dated 29.09.2017 informed regarding mis-billing about the Service Provisioning in the CBCRM System. Accordingly, on 05.12.2017, complaint was given to the senior Inspector of Police,

Cuffe Parade Police Station, Mumbai which was subsequently forwarded to Cyber Crime for further action. The annual maintenance contract of keeping support and maintenance of the CDR Best Billing and CRM System Software in the said Conversant Billing Customer Relation Management (CBCRM) was given to M/s.Tech Mahindra Ltd from 01.07.2017 to 30.06.2017 and thereafter, to M/s.Silver Touch Technologies Limited from 01.07.2017 to 30.06.2019 for the purpose of upgrading it for implementation of GST. The annual maintenance contract for keeping support and maintenance of the CDR billing and CRM System Software was given to M/s.Silver Touch Technologies Limited, who was given access to the server concerned with Service Provisioning of the said CBCRM System with effect from 24.06.2017. It is alleged by first informant that, after taking contract by M/s.Tech Mahindra Ltd., on 30.06.2017 their access to the software was closed and the same was given to the M/s.Silver Touch Technologies Limited and they have started work from 01.07.2017. On 17.07.2017, it was noticed by Sahajad Akhtar, Assistant Manager, CBCRM-O & M, MTNL that on 15.07.2017 after 23.59 p.m. in the night, the work of Server 'Provisioning Application (SP) of CBCRM System was stopped. Therefore, it was informed to the M/s.Silver Touch Technologies Ltd., and on the basis of backup

they have restored the said application on 19.07.2017 and the Server Provisioning Application (SP) of the and CBCRM System has started functioning. As both the servers remained closed between 15.07.2017 to 19.07.2017, all work concerned with the same was affected and there was a feeling of disappointment in the minds of the customers about the MTNL and it affected the reputation of the company. Similarly, as the Server Provisioning (SP) was not working during the aforesaid period, thus, financial loss is alleged to have been suffered by MTNL.

It is further alleged that on inspection, in respect of stopping of the Server Provisioning of CBCRM System, it is revealed someone had made changes in the instructions of source code of server Provisioning Application (SP) in such a way that, the Servers Provisioning Application of the CBCRM system would stop working from 16.07.2017. In connection with the same, when inspection of the logs on firewall of the said server was made and it is found that the said Internet activity of 27.06.2017 had occurred from I.P. Address, of M/s.Tech Mahindra Ltd., who were previously giving service of the keeping support and maintenance of CBCRM System. Thereafter, more information in respect of the same was obtained, the said IP addresses were of Prasanna Salimath and Rajesh Sharma of M/s.Tech Mahindra Ltd., who were doing the work of

maintenance through a distant method (VPN). The Incharge of the Cyber Police Station Crime No.01 of 2018 invoked and applied provisions of Sections 43, 65, 66 of the Information Technology Act r/w Section 420, 34 of the Indian Penal Code.

3. As far as the present applicant is concerned it is his specific case that the Annual maintenance Contract of keeping support and maintenance of CBCRM was given by MTNL to M/s.Tech Mahindra Ltd for the period commencing from 01.07.2014 to 30.06.2017. The M/s.Tech Mahindra Ltd., had giving sub-contract to M/s.Elite IT Services (I) Pvt. Ltd., from 01.07.2016 to 30.06.2017 and it was awarded to M/s.Xalted Information Systems Pvt. Ltd., by M/s.Elite IT Services (I) Pvt. Ltd., by executing a Service Contract Agreement on 15.12.2016. It is a specific case of the applicant, that in terms of the said Service Contract Agreement Xalted was assigned the responsibility for delivery of service for MTNL CBCRM including, provisioning, inter-connect billing as per M/s.Tech Mahindra Contract on back to back basis. This contract was valid from 15.12.2016 to 30.06.2017. It is specific case of the applicant that by virtue of the said agreement Xalted was maintaining CBCRM System until 30.06.2017. It is case of the applicant that while they were maintaining and providing the

services on 20.06.2017, the Senior Manager (Billing-GSM) made a request Prasanna Shalimat for providing National Roaming while converting prepaid and postpaid conversion and further requested to arrange modification in service provisioning command at the earliest. The said request was considered and the necessary changes to the Software were made and the same was communicated. The reply was also received confirming the changes. According to the applicant the service contract came to an end on 30.06.2017 and post period, Silver Touch Technologies Ltd., was awarded Annual Maintenance Contract by MTNL. It is the specific contention of the applicant that they have not logged into the system with effect from 01.07.2017, since the AMC was already awarded to another company. The specific case of the applicant is that at the time of the upgrading of the software on 27.06.2017 they had put their key to the software to ensure that the software is not being misused and it is usual practice to introduce key to all their software to ensure confidentiality. The case of the applicant is that the key to software which was introduced by the company's employee was not introduced with any malice or to cause any loss to MTNL. Further, the applicant was not initially arraigned as an accused and infact it is specific case of the applicant that the company had maintained healthy relationship with the MTNL and even subsequent contracts

are awarded to the company.

4. We have heard, Shri. Badheka, learned counsel appearing for the applicant. His specific submission is that the applicant is not at all responsible for stopping of server provisioning application of CBCRM System and in case of upgrading of the software the license key was to introduced to ensure that the same was not misused however it did not impact functioning of the network and calls. His specific submission is that the offences under Section 43, 65 and 66 of the Information Technology Act were not made out as the ingredients of the said Section to show a fraudulent intention at the inception of transaction has not been demonstrated. Further, according to the learned counsel for the applicant the essential ingredient of Section 420 viz to gain something for the applicant or their company is also conspicuously absent.

He would also rely upon the judgment of the Hon'ble Apex Court in case of Sharat Babu Digumarti V/s. Government (NCT of Delhi)¹ and his precise submission is that the Information Technology Act, 2000 being a special statute and complete Code to cover the alleged activity and since it been accorded and overriding effect by virtue of Section 81, provision of 420 is not attracted and

¹ (2017) 2 SCC 18.

the investigation cannot proceed under of the Indian Penal Code. His specific submission is that the FIR has been registered with *malafide* intention of the complainant and it is based on the assumptions and thus it amount the abuse of process of law and hence he has approached this Court seeking quashment of the said FIR in exercise of inherent power of this Court.

5. In the backdrop of these facts the applicant approached this Court through the present petition praying for the relief sought in the petition.

The learned counsel appearing for the applicant would rely on the judgment of the Hon'ble Apex Court in case of ***Sharat Babu Digumarti V/s. Government (NCT of Delhi) (Supra)*** and it is his submission that the criminal proceedings against the applicants are misconceived. His alternate submission is that even if the offences under the Information Technology Act are to be prosecuted, the applicant cannot be made to face the charges under the Indian Penal Code, since the offences under the Information Technology Act are sufficient to take care of the allegations levelled against him. He submits that the offences under the Indian Penal Code are intentionally invoked and applied so that the applicant is deprive of the benefit of the bail and compounding of the offences

which is ofcourse available under the provisions of the Information Technology Act, 2000. According to the learned counsel in light of the binding precedent laid down by the Hon'ble Apex Court, in the aforesaid judgment *Sharat Babu Digumarti V/s. Government (NCT of Delhi) (Supra) (Supra)* the provisions of the Information Technology Act have been given an overriding effect to cover criminal acts contained in the Indian Penal Code and this law being a special law must prevail over the general law. In the facts of the case the applicant would pray for quashing of the FIR at least to the extent of offences punishable under the Indian Penal Code.

6. In light of the facts referred to above we have heard the respective Senior Counsels and perused the material placed before us.

The Information Technology Act, 2000 is a legislation to provide legal recognition for transactions carried out by means of electronic data inter change and other means of electronic communication, commonly referred to as “electronic commerce” which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government Agencies and further to amend the Indian Penal Code, the Indian Finance Act, 1872 etc.

The said Act has been brought into force from 17th October 2000. The introduction of new communication system and digital technology has necessitated the said enactment with a view to facilitate Electronic Governance. With proliferation of information technology enabled services such as e-governance, e-commerce and e-transactions, protection of personal data and information and implementations of security practices and procedures relating to these applications of electronic communications have assumed great importance and the Enactment was necessitated in the backdrop of the security of the nation, economy, public health and safety.

7. Perusal of the said provisions of the I.T. Act, 2000 would reveal that it provides complete mechanism for protection of data in a computer system or a computer network. The computer system is intended to cover a device or collection of devices, including input and output support devices capable of being used in conjunction with external files, containing computer programs, electronic instructions, input and output data, data storage and retrieval. The said enactment is a complete code which deals with electronic governance and confers a legal recognition on electronic records and the manner in which such records can be secured. The said Act of 2000 makes certain acts punishable in Chapter-IX and

Chapter-XI of the said act which enumerates the offences related to the computer including the source documents. Thus, the said enactment is a complete Code in itself and deals with various aspects of electronic data and computer system.

Section 43 of Information Technology Act, 2000 prescribes penalty and compensation for damage to computer and computer system needs a reproduction:-

43 [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, conceals, 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 database" 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 resource 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 programmes, computer commands, design and layout and programme analysis of computer resource in any form.]

It is apposite to refer Section 65 and 66 which reads

thus :-

*"65. Tampering with computer source documents:-
Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used*

for a computer, computer programme, computer system or computer network when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both.

Explanation-For the purposes of this section, computer source code” means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.”

66. Computer related offences:- *If any person, dishonestly or fraudulently, does any act referred to in Section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakhs rupees or with both.*

Explanation-For the purposes of this section-

(a) the word “dishonestly” shall have the meaning assigned to it in Section 24 of the Indian Penal Code (45 of 1860).

(b) the word “fraudulently” shall have the meaning assigned to it in Section 25 of the Indian Penal Code (45 of 1860)”.

8. The distinction between Section 43 and 66 is very succinct. All the acts which are covered within the purview of Section 43 if committed dishonestly and fraudulently are made

punishable under Section 66 with an imprisonment for a term which may extend to three years or with fine. It is relevant to note that the word “dishonestly” and “fraudulently” is assigned the same meaning as in Section 24 and 25 of the Indian Penal Code respectively. The offences under the Information Technology Act, 2000 are compoundable and the offences which are punishable with imprisonment of three years and above are bailable and cognizable. Another important provision contained in the said enactment is Section 81 which reads thus :-

“81. Act to have overriding effect :-The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force:

Provided that nothing contained in this Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957 (14 of 1957) or the Patents Act, 1970 (39 of 1970).”

9. In the backdrop of the scheme of the enactment the claim of the rival parties will have to be examined.

10. The Hon'ble Apex Court in case of ***Sharat Babu Digumarti (Supra)*** had in great detail dealt with the offences

punishable under the Information Technology Act and at the same time punishable under the relevant provisions of the Indian Penal Code. In the said case, an FIR was filed against the appellant and on investigation, chargesheet came to be filed before the Magistrate who took cognizance of the offences punishable under Section 292 and 294 of the Indian Penal Code and also Section 67 of the Information Technology Act. In a petition before the High Court seeking quashment, he was discharged of the offences under Section 292 and 294 but the prosecution under Section 67 of the Information Technology Act continued. The appellant approached the Apex Court and on the ground that the company was not arraigned as a party and the Director could not have been liable of the offences punishable under Section 85 of the Information Technology Act and the proceeding came to be quashed. Subsequently an application came to be filed before the Trial Court to drop the proceedings and the Trial Court refused to drop the proceedings under Section 292 of Indian Penal Code and framed the charge. With this issue he approached the Apex Court and the question for consideration before the Hon'ble Apex Court was whether the appellant who has been discharged under Section 67 of the Information Technology Act could be proceeded under Section 292 of the Indian Penal Code. The Hon'ble Apex Court also

examined whether an activity emanating from electronic form which may be obscene would be punishable under Section 292 of the Indian Penal Code or 67 of the Information Technology Act or both or any other provision of the Information Technology Act. In the backdrop of the said facts the Hon'ble Apex Court observed thus :-

30. *In this regard, we may reproduce [Section 81](#) of the IT Act, which is as follows:-*

“81. Act to have overriding effect.- The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

Provided that nothing contained in this Act shall restrict any person from exercising any right conferred under the [Copyright Act](#) 1957 or the [Patents Act](#) 1970.”

The proviso has been inserted by Act 10 of 2009 w.e.f. 27.10.2009.

31. *Having noted the provisions, it has to be recapitulated that Section 67 clearly stipulates punishment for publishing, transmitting obscene materials in electronic form. The said provision read with Section 67-A and 67-B is a complete code relating to the offences that are covered under the IT Act. Section 79, as has been interpreted, is an exemption provision conferring protection to the individuals. However, the said protection has been expanded in the dictum of Sherya Singhal and we concur with the same.*

32. *Section 81 of the IT Act also specifically provides that the provisions of the Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force. All provisions will have their play and significance, if the alleged offence pertains to offence of electronic record. It has to be borne in mind that IT Act is a special enactment. It has special provisions. Section 292 of the IPC makes offence sale of obscene books, etc. but once the offence has a nexus or connection with the electronic record the protection and effect of Section 79 cannot be ignored and negated. We are inclined to think so as it is a special provision for a specific purpose and the Act has to be given effect to so as to make the protection effective and true to the legislative intent. This is the mandate behind Section 81 of the IT Act. The additional protection granted by the IT Act would apply.*

37. *The aforesaid passage clearly shows that if legislative intendment is discernible that a latter enactment shall prevail, the same is to be interpreted in accord with the said intention. We have already referred to the scheme of the IT Act and how obscenity pertaining to electronic record falls under the scheme of the Act. We have also referred to Sections 79 and 81 of the IT Act. Once the special provisions having the overriding effect do cover a criminal act and the offender, he gets out of the net of the IPC and in this case, Section 292. It is apt to note here that electronic forms of transmission is covered*

by the IT Act, which is a special law. It is settled position in law that a special law shall prevail over the general and prior laws. When the Act in various provisions deals with obscenity in electronic form, it covers the offence under Section 292 IPC.

39. *In view of the aforesaid analysis and the authorities referred to hereinabove, we are of the considered opinion that the High Court has fallen into error that though charge has not been made out under Section 67 of the IT Act, yet the appellant could be proceeded under Section 292 IPC.*

11. Reading of the said judgment, makes is clear that the Hon'ble Apex Court had considered the effect of the overriding provisions contained in the Information Technology Act and has observed that all the provisions in the enactment are of significance particularly if the alleged offences pertains to electronic record. By observing that the Information Technology Act is a special enactment and it contain special provision, the Hon'ble Apex Court has also considered the effect of Section 79 contained in the Information Technology Act which is enacted for a specific purpose and has observed that the mandate behind Section 81 of the Information Technology Act needs to be understood in its proper perspective. It referred to the earlier precedents on the point where

a special statute is pitted against a General enactment and thereafter has concluded by making reference Section 79 and 81 that once the special provisions are accorded overriding effect to cover a criminal Act, the offender gets out of the net of the Indian Penal Code and in the case in hand of Section 292.

12. It is well known principle of law that a prior general Act may be effected by a subsequent particular or a special Act. In the principles of statutory interpretation by justice G.P. Singh 13th Edition 2012 the aforesaid principle is culled out in the following manner:-

“A prior general Act may be effected by a subsequent particular or a Special Act, if the special matter of particular Act prior to its enforcement was being governed by the general provision of the earlier Act. In such a case the operation of the particular Act may have the effected of parallel rebelling the general Act or curtailing its operation or added conditions to its operation for the particular cases.

A general Act operation may be curtailed by a latter special Act even if the general Act contained a non-obstante clause. The curtailment of the general Act will be more readily inferred with the latter special Act also containing an overriding non-obstante provision.

13. In light of the aforesaid authoritative pronouncements it can very well be seen that the statute and its provisions must be construed by keeping in mind the object behind the enactment of such a statute. The Hon'ble Apex Court in case of ***RBI V/s. Peerless General Insurance Finance and Investment Company Ltd.***² has made observations to the following effect :-

“33. If a statute is looked at, in the context of the enactment, with the glasses of the statute makes and provided by such context, its scene, the sections, clauses, phrases and words may take colour and appear different that when the statute is looked at without the glasses provided by the context. With these glasses we must look at the set as a whole and discover what each section, each clause, each phrase, each word is meant and designed to say as to fit into the scheme of the entire Act.”

14. Perusal of the FIR would reveal that the allegations are to the effect that the M/s.Tech Mahindra Ltd fraudulently and dishonestly made changes in the Server Provisioning application (SP) to the Conversant Billing Customer Relation Management System resultantly stopping its functioning and this resulted into financial loss to MTNL and also tarnished its image. The FIR is registered under Section 420, 34 of the Indian Penal Code r/w

2 2014-8-SCC-319

Section 43, 65, 66 of the Information Technology Act. Perusal of Section 43 of the Information Technology Act would reveal that it prescribes penalty and compensation for damage to the computer or computer system if any person without permission of the owner or in charge of a computer, computer system accesses or secure access to the computer or caused any damage to any computer, computer system or computer database or any other programs residing in such computers. It is also attracted if there is disruption of any computer or a computer system or a computer network and further stealing, concealing or any alteration of any computer source code used for computer source with an intention to caused damage.

If the aforesaid acts are done fraudulently and dishonestly, then it attracts the provisions of Section 66 of the Information Technology Act, 2000 and such acts are made punishable with imprisonment for a term which may extend to three years or fine or with both. The word 'dishonestly' and 'fraudulently' have been assigned the same meaning as in the Indian Penal Code and as such any such act which falls within the purview of Section 43 if committed with a dishonest and fraudulent intention, it would fall within the scope of Section 66 and amounts to an offence. Perusal of the facts of the present case could reveal that the ingredients of the Act which has been alleged to be an offence under

Section 420 read with 34 of Indian Penal Code are also covered by Section 66 of the Information Technology Act, 2000. If the ingredients of both the offence are same, in such circumstances a person cannot be prosecuted for the same act by invoking the provisions contained in two different statute, specifically when the Information Technology Act has been held by the Hon'ble Apex Court to be code in itself and cater to the entire arena relating to Information Technology and its use.

In such circumstances though we are not inclined to quash the FIR filed against the petitioner in its entirety, we are of the opinion that the allegations levelled against the applicant would also attract Section 65 and 66 of the Information Technology Act, since all the acts alleged and attributed to the applicant would squarely fall within the purview of Section 43 and since it is alleged that the said Act has been committed fraudulently and dishonestly and it would amount to an offence under Section 66 of the Information Technology Act. We are therefore not inclined to quash the said FIR as far as the offences under the Information Technology Act are concerned, however we hold that the invocation and application of the provisions of the Indian Penal Code and specifically Section 420, is not sustainable in light of the judgment *Sharat Babu Digumarti v/s. Government (NCT of Delhi) (Supra)*.

Since, the ingredients of the offence under the Information Technology Act which have been invoked and applied are the same.

In such circumstances, we allow the Writ Petition and set aside the FIR bearing CR No.01 of 2018 registered with Cyber Police Station, Mumbai only to the limited extent where it invokes and applies Section 420 read with 34 of Indian Penal Code, As far as the offences under the Information Technology Act are concerned, the prosecution against the applicant is directed to be continued.

(SMT.BHARATI H. DANGRE, J.)

(RANJIT MORE, J.)