$~11

* **IN THE HIGH COURT OF DELHI AT NEW DELHI**

\+ W.P.(CRL) 1006/2015

POOJA KHETAN ..... Petitioner

Through: Mr. Shashank Deo Sudhi, Dr. Shashi Bhushan and Mr. Bijender P. Kumar, Advocates.

Versus

GOVT OF NCT OF DELHI & ORS ..... Respondents

Through: Mr. Rahul Mehra, Standing Counsel (Crl.) with Ms. Nandita Rao, ASC alongwith Mr. Jamal Akhtar, Ms. Iti Pandey and Mr. Chaitanya Gosain, Advocates.

CORAM:
HON'BLE MR. JUSTICE NAJMI WAZIRI

O R D E R

% 18.09.2018

1. Mr. Rahul Mehra, the learned Standing Counsel for the Government of National Capital Territory of Delhi states that pursuant to various orders of this Court and keeping in mind the fact that nowadays in almost every criminal act, there is some element of electronic evidence or footprint, therefore, for collection of such technological evidence, and for a more scientific investigation into crimes, the State has constituted Cyber Crime Teams for each police district, for due assistance to each police station. He submits that each cyber team has the benefit of qualified personnel having due academic qualification and technical competence to deal with the matters relating to cyber crimes and for collection and analysis of electronic evidence.

2. According to the Standing Instructions, now issued, Call Detail Records of all relevant numbers are to be collected within one month from the date of registration of the FIR and CCTV records are to be collected within 48 hours of the registration of the FIR. The Delhi Police have prepared an action plan for strengthening cyber crime investigation infrastructure. It includes the following steps:-

> " *i) Setting up of cyber training division in the police Training College. For conducting short duration training in Cyber Crime investigation.*
> *ii) Satisfactory minimum performance in the Cyber Crime Investigation training to be a criteria for posting of officer in police station who supervises witnesses such as Crime Branch on the EOW.*
> *iii) Cyber Crime Investigation training to be a mandatory module in the basis foundation training of fresh recruits of all ranks (Constable, Sub-Inspectors, ACPs).*
> *iv) Officers of Delhi Police to be send regularly to specialize training of Cyber Crime Investigation for skill enhancement.*
> *v) District police and field units to regularly conduct refresher course in cyber crime investigation for their officers.*
> *vi) All districts to conduct cyber safety awareness campaign in schools, colleges, offices and markets, RWAs on regular basis."*

3. Under the Standing Order Nos. 451/2017 and 448/2017, the police is required to conduct investigation in the following manner:-

> *" **DELHI POLICE***
> ***STANDING ORDER 451/2017***
> ***USE OF CALL DETAIL RECORD (CDR) ANALYSIS IN INVESTIGATION OF CASES***
>
> ***1. Introduction:***
>
> *In India, mobile phones have become an integral part of every citizen's life today. With over a billion mobile phone*

users, India today has the second largest subscriber base in the world. Therefore, the call details record (CDR) has become an important data source for quantifying and analyzing user profile, movements, activities and behavior. A CDR contains various details pertaining to each call who called whom, when and where was it made, how long it lasted, etc. These details can provide valuable direct as well as circumstantial evidence in criminal investigation. Therefore, it is important that the Investigating Officers (IO) of Delhi Police collect. CDRs and other relevant information from telecom service providers (TSPs) in course of their investigation.

2. ***Points to be considered in cases where Analysis of CDR is required:***

i. *IOs should, as soon as possible, collect the CDRs from the concerned telecom service provider (TSP) as soon as they pinpoint a mobile number that is relevant to investigation.*

ii. *IO should, within one month of registration of FIR, collect CDRs of all persons relevant to the investigation as per the FIR and facts brought out in the initial investigation, from the concerned telecom service providers(TSPs)*

iii. *There should not be any undue gap/lag in the period between the knowledge of a mobile number being relevant to investigation and the dispatch of request for its CDR to the TSP.*

iv. *Procedure mentioned in Standing Order 420/2013 should be followed while obtaining CDRs.*

v. *IO should note that the CDR of any mobile number is available only for the period of one year. Hence, efforts should be made to identify all telephone numbers relevant to investigation within the initial stages of investigation.*

vi. *CAF (Customer Application Form), in original, should also be taken from the concerned telecom service provider if the CDR of the number is to be included in list of evidences.*

vii. *Certificate under Section 65-B of the Indian Evidence Act should be taken from the concerned telecom service provider.*

3. CDR Analysis can be divided into the following parts

i.Call Details

ii. Subscriber/ CAF Details

4. The main columns in the Call Details are as follows:

i.Calling Number: The Number that has originated the call.

ii. Called Number: This is the Number of the receiver.

iii. IMEI of the device used: International Mobile Equipment Number. This is the unique number given to each mobile device for its identification.

iv.IMSI Number of the SIM Card: International Mobile Subscriber Identity Number.

v. Date and time of call: Date and time of the call made over the telecom network.

vi.Duration: Duration of the call made (mainly in seconds)

vii. Type of Call: Type of Call like Incoming/ Outgoing/ SMS/ Data etc.

viii. Cell ID: Number given to the Cell Tower located at the place from where the caller made the call.

5. ***The analysis may cover the following points:***

i.Caller No./ called No. can identify the following details:

a. The column will provide the list of numbers on which the target number is making calls.

b. The column will provide the list of numbers on which the target number is receiving calls.

c. The column will provide the list of numbers on which the target number is sending SMSs.

d. The column will provide the list of numbers on which the target number is receiving SMSs.

e. The column will provide the total number of times from which the target number is in contact with other numbers.

ii. ***IMEI***

a. This column will provide details that how many phone sets has been changed by the target number during the period.

b. Type or model of phone can also be identified by the given column as there are several websites available on the internet from where one can find out the model by submitting the IMEI of the phone.

iii. ***IMSI***

a. This column will provide number of times the SIM Cards for the target number is being replaced.

b. Dates on which the target has stopped using the number and again the number has been activated.

c. Date on which the number has been ported to another service provider, as generally, if ported, then the new telecom service provider provides a new SIM card and the IMSI will get changed.

iv. ***Date & time***

a. This column will show the date and time when the calls/ SMS were made/ sent during the required period.

v. ***Duration***

a. This column will show the duration of the call (in seconds).

vi. ***Type of Call***

a. This column will show the category of the entry made in the CDR as one of the following:

1) Incoming call

2) Outgoing call

3) SMS

4) RCF (Roaming call forward)

5) Internet/Data

vii. ***Cell ID:***

a. This column will show an alpha-numeric number which represents a code given to all the towers of a particular telecom service provider through which they are providing connectivity to the mobile number concerned. By looking for the number in the Cell ID chart the IO can find out the location of the target number at the time of call given in the CDRs.

viii. ***CAF or Subscriber Data :***

This is a document provided by the service provider which contains the following information:

a. Name of the subscriber

b. Address of the subscriber

c. Alternative number of the subscriber

d. Permanent address of the subscriber

e. Local reference details, if the permanent address is from other state

f.Details of the shop from where the SIM has been purchased

g. Details of the agency that has verified the details provided by the subscriber

The form will also have, annexed with it, copies of document like address proof submitted by the subscriber while getting the SIM issued.

The Investigating Officers of all criminal cases should ensure that they collect the CDRs and the user details/CAF of all relevant numbers brought out during the investigation and they should extract the various pertinent information/ details from the CDRs/ CAFs as per this Standing Order.

This Standing Order supersedes all earlier Standing Orders regarding this issue, in so far as provisions of such Standing Orders are repugnant to the provisions detailed in this Standing Order".

"DELHI POLICE

STANDING ORDER 448/2017

PROCEDURE FOR SEARCH AND SEIZURE OF COMPUTER,COMMUNICATION, DIGITAL STORAGE DEVICES AND PREPARATION OF SEIZURE MEMO DURING INVESTIGATION

1. Introduction

1.1 With increased use of communication devices/ computers and digital storage devices in homes and offices, there has been increasing instances of crimes involving these devices, either as a tool, or target or simply as a piece of evidence. The investigation of such crimes is complex as the evidence is often in an intangible form. Its collection and preservation presents unique challenges to the investigator. The increased use of networks and the growth of the internet have added to this complexity.

1.2 During the seizure of digital evidence in course of investigation of a cyber crime or conventional crime with digital trails, the seizure procedure involves several precautions that are required to be taken in addition to the precautions and care taken during seizure of conventional articles.

1.3 The stages of digital crime scene search and seizure are:

A. Preparation/ Planning stage.

B. Collection stage.

C. Preservation/ Transportation stage.

2. Guidelines for search and seizure of digital evidence

2.1 Preparation/ Planning Stage:

Before proceeding to the place of the suspect or the scene of crime from where the seizure of electronic items/ digital evidence is to be done, the IO should try to get the following information.

1. *Whether the system is live or offline. In case of live systems, IO needs to obtain appropriate orders from the competent court to make the system offline. The IO will have to take Image copy of the data with the help of cyber expert and forensic devices. Thereafter, the image copy will be considered as the original (primary) evidence in such cases alongwith the certificate under Sec. 65-B of Indian Evidence Act.*
2. *Format of 65-B, Indian Evidence Act certificates as per the requirements.*
3. *Requirement should be analyzed in advance as to whether seizure of the complete system is required or a portion of the data needs to be seized. In case of seizure of part data, necessary 65-B certification will be required from the concerned authority (custodian of the data).*

2.2 <u>Collection / seizure Stage</u>

While conducting search and seizure, the IO should follow the following steps:

1. *The IO should separate all the employees from their working terminals.*
2. *IO should avoid taking help from the alleged company's employees or from the accused persons.*
3. *IO should identify the equipment of concern as soon as possible.*
4. *IO should document all the steps with proper date and time. A format for the same is attached for reference.*
5. *Date and time of seizure of electronic device is very*

important IO should made sure while preparing the seizure to mention the date and time (in 1ST format).

Note: *IO should ensure to mention the current time as obtained from any standard source (such as Indian Meteorological Department website).*

2.3 Preservation / Transportation Stage

1. *IO should make sure that a serial number is allotted for each device and the same should be duly noted, not only in the Panchnama, but also in the Chain of Custody and Seizure Memo.*
2. *IO should protect digital magnetic media from external electric and magnetic fields. IO should also ensure protection of digital media, particularly optical media from scratches.*
3. *As computer devices and parts are sensitive in nature, hence they should be handled carefully. IO should wrap the computer components using Styrofoam and other protective coverings.*
4. *IO should keep the components of each computer system together and should label each part after dismantling.*
5. *The computer system should be secured in a way that would reduce vibrations. The IO should store the computer in a secure, cool, dry place, away from any electric or electromagnetic signals.*

*3. **Dos and Don'ts***

3.1 For Laptop

1. *Check whether the Laptop is ON or OFF.*
2. *If **ON**, then*

a. *Take a Screen Shot of the screen.*
b. *Take the list of Programs running in RAM; running Operating System.*
c. *Remove the power chord of the laptop from the power outlet (Never Shutdown).*
d. *Remove the battery from the Laptop.*
e. *Note down the color, Make and Model of the Laptop.*
f. *Note down any Serial number available on the chassis of the Laptop.*
g. *If you can remove the back cover of the laptop, then note*

down the make, model, Serial no. and capacity of hard disk.

*3. If **OFF,** then*

a. Remove the power chord of the laptop from the power outlet (Never switch on the Laptop).

b. Remove the battery from the Laptop.

c. Note down the color, Make and Model of the Laptop.

d. Note down any Serial number available on the chassis of the Laptop.

e. If you can remove the back cover of the laptop, then note down the make, model, Serial no. and capacity of hard disk.

3.2 <u>For Desktop</u>

1. Check whether the desktop is ON or OFF.

*2. If **ON,** then*

a. Take a Screen Shot of the screen.

b. Take the list of Programs running in RAM; running Operating System.

c. Remove the power chord of the laptop from the power outlet (Never Shutdown).

d. Note down the color, Make and Model of the desktop.

e. Note down any Serial number available on the chassis of the desktop.

f.If you can remove the side panel of the desktop/ CPU, then note down the make, model, Serial no. and capacity of hard disk.

*3. If **Off,** then*

a. Remove the power chord of the desktop from the power outlet (Never switch On).

b. Note down the color, Make and Model.

c. Note down any Serial number available on the chassis.

d. If you can remove side panel of the desktop/ CPU, then note down the make, model, Serial no. and capacity of hard disk.

3.3 <u>For Mobile Phones/ Tablets</u>

1. Check whether the device is ON or OFF

*2. If **ON,** then*

a. Leave it ON.

b. Photograph the device.

c. Label and collect all cables of the device.

d. If possible keep the device charged.

e. Seize the phone in a Faraday bag.

f.Note down any Serial number if available on the chassis of the mobile phone.

g. Never remove the battery.

*3. If **OFF,** then*

a. Seize the device in a Faraday Bag along with all cables of the device

3.4 For Miscellaneous storage devices

1. Collect any storage media like USB Pen drives, External storage hard disks, Memory cards, SIM Cards, CDs, DVDs etc. which may be used to store data. For these types of devices:

a. Note down the make, color, capacity and any Serial No. available on the device.

b. Wrap the device in 'Antistatic Bag' and wrap it in a bubble wrapper along with the connecting cables, if any.

c. Seize the CDs and DVDs in a suitable protective hard case only.

2. Check if any printer, Photostat machine or any scanning device is available, If yes then:

a. Check whether the system is available with its internal storage capacity.

b. If yes then follow the procedure mentioned in point 3.2.

3.5 For CCTV Footage / Digital Video Recorder

1. Immediately after registration of FIR, the Investigating Officer should identify all CCTV cameras in and around the relevant spot without any avoidable delay.

2. The Investigating Officer should call the District Cyber Cell Team at the Scene of Crime for collection of CCTV System Hard Disks without any delay and not later than 48 hours as far as practicable, from the registration of FIR.

3. The District Cyber Cell Team should scan the Scene of Crime to identify any CCTV system that may have captured any visuals/audio.

4. Thereafter, the District Cyber Cell Team should extract the storage media (Hard Disk) containing the relevant CCTV footage and assist the Investigating Officer in its seizure.

5. The District Cyber Cell Team should simultaneously ensure

that the Hard Disk/storage media of the concerned CCTV System seized by the Investigating Officer is immediately replaced by a new Hard Disk/storage media of same/similar specification to enable uninterrupted operation of CCTV system.

6. *In case the DVR is also seized along with the Hard Disk, a corresponding replacement of the same should be provided to the custodian/owner of the CCTV system.*
7. *If the Investigating Officer is not able to collect all relevant CCTV footages in 48 hours, then he should notify all persons owning/operating relevant CCTV systems, to take necessary steps to ensure that the relevant footage as detailed in the Notice is not altered/destroyed/deleted.*
8. *In respect of CCTV systems, other than those at the Scene of Crime or in its immediate vicinity, the IO should get their Hard Disks seized with the help of the District Cyber Cell Team without any undue or avoidable delay in course of ongoing investigation.*
9. *Whenever possible, the proprietary recorded video files from the DVR should be retrieved to maintain the integrity and image quality of the evidence.*
10. *Steps involved :*

a) *A copy of the DVR's instruction Manual should be taken in possession by the IO.*
b) *IO should determine the earliest recorded date. This will determine approximately how much time the IO has to retrieve the data before the system begins to overwrite it.*
c) *IO should compare the time displayed by the DVR system with the current time. (such as the time displayed by Indian Meteorological Department website)*
d) *Remove the power cord from the DVR.*
e) *Remove all the cables connected with the DVR.*
f) *Seize the hard disk in an antistatic bag.*
g) *IO to collect, if available, a copy of the original CD of the DVR Player provided by the DVR manufacturer along with the DVR from the owner/custodian of the DVR.*

11. *If the IO needs footage from any banking premises like ATM or from Bank or any other agency, then he*

earliest and without any delay. Most of the ATM footages are overwritten in a time span ranging between 3 to 7 days.

12. *Whenever the District Cyber Cell Team assists the IO in seizure of hard disk from the custody of any person other than the accused, it should immediately provide a replacement hard disk with same/similar specifications to the custodian/ owner of the CCTV.*

13. *Whenever the District Cyber Cell Team assists the Investigating Officer in seizure of complete DVR from the custody of any person other than the accused, it should immediately provide a replacement DVR with same/similar specifications to the custodian/ owner of the CCTV.*

14. *The Heads of the Officers of the Units/ Districts should ensure that their respective District/Unit maintains a reserve stock of DVRs/Hard Disks of the most common specifications and the same is made available to the District Cyber Cell Team and replenished as per requirement. The Districts/Units should replenish their reserve hard disks stocks through regular procurement as per laid down procedures of procurement.*

15. *The Investigating Officers should follow the abovementioned guidelines at the time of search and seizure of CCTV Systems, computer and communication devices.*

16. *A suggested seizure memo for seizure of computer, storage and communication devices is provided at Annexure 'A'.*

This Standing Order supersedes previous SO No. 448/2016 issued vide No.6402-6530/ RB/ PHQ, dated 01.12.2016 and all other standing/ Circular orders are repugnant to the provisions detailed in this Standing Order".

4. The learned counsel for the State submits that Standing Order No. 442/2016 mandates: (i) the constitution of a well-equipped District Cyber Cell in each Police District; (ii) Cyber Teams in each police station; and (iii)

the conduct of awareness campaigns about cyber crimes, their prevention and investigation. He submits that the requisite personnel trained in cyber crime are yet to be appointed. It is expected that they would be appointed in the next two months, failing which the case would be listed for directions.

5. The DCP, EOW, Cyber Cell, shall file an affidavit of compliance on or before 30.11.2018.

6. The petitioner is stated to have been provided due protection in terms of this Court's order dated 01.08.2016 and has no complaint regarding the same. The other portions regarding framing of the guidelines and receiving of any anonymous obscene calls or e-mails have been taken care of in terms of the aforesaid guidelines.

7. It is expected that due compliance of the same shall be made in every case. The petition stands disposed-off in the above terms.

NAJMI WAZIRI, J

SEPTEMBER 18, 2018
RW