IN THE HIGH COURT OF KARNATAKA AT BENGALURU

DATED THIS THE 12TH DAY OF MARCH, 2021

BEFORE

THE HON'BLE MR. JUSTICE SURAJ GOVINDARAJ

WRIT PETITION NO. 11759 OF 2020 (GM-RES)

BETWEEN:

MR. VIRENDRA KHANNA
S/O SRI RAM KHANNA
AGED ABOUT 35 YEARS
RESIDING AT NO.301, PIYARSON WEST
LANGFORD ROAD, 1ST CROSS
RICHMOND, BANGALORE – 08 … PETITIONER

(BY SRI. HASHMAT PASHA, SR. COUNSEL FOR
SRI. NASIR ALI, ADVOCATE-PH)

AND:

1. STATE OF KARNATAKA BY:
BANASAWADI POLICE, BANGALORE-560043

2. POLICE INSPECTOR, CCB POLICE,
BANGALORE, NT PET
BANGALORE-560002 … RESPONDENTS

(BY SRI. VEERANNA G. TIGADI, SPP)

THIS WRIT PETITION IS FILED UNDER ARTICLES 226 & 227 OF THE CONSITUTION OF INDIA AND UNDER SECTION 482 OF THE CR.P.C., PRAYINT TO QUASH THE ORDER DATED 23.09.2020 VIDE ANNEXURE-E WHICH IS RE-AFFIRMED BY ORDER DATED

15.10.2020 VIDE ANNEXURE-H PASSED IN SPCL.C.C. NO.529/2019 ON THE FILE HON'BLE XXXIII ADDL. CITY CIVIL AND SESSIONS JUDGE AND SPECIAL COURT FOR NDPS CAES, BANGALORE CITY, WHICH IS ARISING OUT OF CRIME NO.588/2018 ON THE FILE OF R-1 BANASWADI POLICE, BANGALORE, AS AN ABUSE OF PROCESS OF LAW AND ETC.

THIS WRIT PETITION COMING ON FOR FURTHER ARGUMENTS AND HAVING BEEN RESERVED FOR ORDERS ON 14.12.2020, THIS DAY, THE COURT PRONOUNCED THE FOLLOWING:

ORDER

1. The petitioner/Accused No. 5 is before this Court seeking for:

   1.1. Issuance of a writ of certiorari or a writ or order or direction of appropriate nature in quashing the order dated 23-9-2020 as per Annexure - E, which is re-affirmed by order dated 15-10-2020 as per Annexure H Passed in Spl C.C. No. 529 of 2019 on the file of the XXXIII Additional City Civil and Sessions

Judge and Special Court for NDPS Cases, Bangalore City, which is arising out of Crime No.588/2018 on the file of first Respondent Banaswadi Police, Bangalore, as an abuse of process of Law.

1.2. Issuance of a writ of certiorari or writ or order or direction of appropriate nature in quashing the order dated 14-09-2020 as a part of Annexure-E in directing the Petitioner to co-operate for unlocking the mobile phone, passed in Spl. C.C. No. 529/2019 on the file of XXXIII Additional City Civil and Sessions Judge and Special Court for NDPS cases Bangalore City, which is arising out of Crime No.588/2018 on the file of the first respondent police as illegal and abuse of process of Law.

FACTS

2. In the Petition, it is contended that:

2.1. The Petitioner is an IT Engineer, having studied in M/s RV College of Engineering, Bangalore. He was selected as Software Engineer, during the process of on-campus recruitment by Accenture, IT company, Bangalore, where he worked for one year and thereafter resigned to do his self avocation of organising events and parties in 5-star hotels and other events by obtaining licence and permission from the police department.

2.2. It is claimed that the nature of work carried out by the Petitioner is only to book the participants for the event and the other arrangements of food and drinks are made by the hotel management, and he had no control

of it and even he was not allowed to carry anything.

2.3. The last event organised by the Petitioner was in the second week of March 2020 before COVID- 19 Pandemic lockdown, thereafter, he has not organised any event or party.

2.4. It is stated that on 3-09-2020, when the Petitioner was with his parents in Delhi at about 5:00 P.M, some policemen said to be from CCB police of Bangalore had visited his Delhi residence and insisted on his presence in Bangalore for interrogation by CCB police and accordingly, he was brought to Bangalore on 4-09-2020 by flight.

2.5. It is claimed that the Petitioner has been fixed in an old case in Crime No. 588/ 2018 of Banasawadi police station, in which

investigation was completed and the charge sheet was filed on 30-04-2019.

2.6. Petitioner was arrested and produced before the XXXIII Addl. City Civil and Sessions Judge and Special Judge for NDPS cases Bangalore City, on a remand application being filed, he was remanded to police custody. On the expiry of the said remand, he was once again remanded to judicial custody without hearing him or his counsel, which is contrary to Section 167 of Cr.P.C., and violative of Article 21 and 22 of the Constitution.

2.7. It is alleged that when he was brought from Delhi to Bangalore by the second respondent police, he had a mobile phone bearing SIM No.8105100009 and the same was seized under mahazar on 4-09-2020. The Petitioner

has claimed that he had unlocked his phone and shown it to the CCB police that it contains some contact numbers of his friends and family members. The police had seen the mobile phone details and thereafter retained the said mobile in police custody itself.

2.8. It is contended that the prosecution falsely alleged before the Special Judge on 14-09-2020 that the Petitioner is not giving his mobile phone password for unlocking his mobile when the Court directed the Petitioner to co-operate for unlocking the mobile phone. It is further stated that the Petitioner co-cperated with the police in opening his E-mail accounts.

2.9. On 16-09-2020, the Petitioner was produced before Court and got remanded to Judicial

custody because his presence was no more required for the police investigation.

2.10. On 23-09-2020, the second Respondent, CCB police, filed an application before the Special Court for an order of permission to subject the Petitioner for Polygraph test because he has not given mobile phone password for unlocking his mobile phone and also for getting opened two more E-mail accounts belonging to him. This application copy was not served either on the counsel for Petitioner or on Petitioner, and as soon as it was filed, an order dated 23-09-2020 was passed to send the Petitioner for Polygraph test as prayed in the Application, and it was ordered to the Investigation officer of CCB Police Bangalore to take the Petitioner for Polygraph test with proper escorts by 28-09-2020.

2.11. It is contended that before passing the order dated 23-09-2020 directing a Polygraph test, no opportunity was given to Petitioner or his counsel to defend the Application filed by CCB police for Polygraph test and thereby, the order for Polygraph test was not known to Petitioner or his counsel.

2.12. It is only on 03-09-2020, the Petitioner's father was told by his friends that in Media it is being reported that the Court has permitted a Polygraph test of the Petitioner. Petitioner's father immediately informed the counsel for Petitioner, and thereafter on verification, it was found to be true and the order dated 23-09-2020 had been passed without the Petitioner's knowledge.

2.13. On 3-10-2020, the Petitioner's counsel filed

an application to recall the order of Polygraph test dated 23-09-2020 as not tenable in Law as it amounts to testimonial compulsion hit by Article 20 clause (3) of the Constitution. He is not consenting to the Polygraph test; the order was passed behind the back of the Petitioner. Hence it was required to recall the order and to give an opportunity of hearing regarding the Polygraph test more so when the Petitioner was not willing to subject himself to such a test.

2.14. This recall application copy was served upon Spl.PP on 03-10-2020 and was put up on 05-10-2020 before the Special Court, which granted time to file objections, which was filed on 07-10-2020.

2.15. It is stated that during the course of

arguments, the Petitioner's counsel specifically brought to the notice of the Special Court that the Petitioner is not consenting for Polygraph test and the order for Polygraph test dated 23-09-2020 was passed without hearing him, it amounts to testimonial compulsion as held by the Hon'b1e Supreme court in the case of ***Selvi V/ s State of Karnataka reported in 2010 (7) SCC 263***, it interferes in his right to privacy which is guaranteed as Fundamental right under Article 21 of the Constitution as held in the case of ***Mr. Justice K.S. Puttaswamy V/ s Union of India reported in 2017(10) SCC Page.1***.

2.16. The Special Court, however, by its order dated 15-10-2020, rejected the recall application holding that the Court can order

for Polygraph test and the order dated 23-09-2020 cannot be recalled by the same Court.

2.17. It is aggrieved by the said order dated 23-09-2020, which is re-affirmed by order dated 15-10-2020, the Petitioner is before this Court seeking for the aforesaid reliefs.

3. On service of notice Shri. VeeranaTigadi learned special prosecutor has entered an appearance for the State and filed his objections; in the said objections, it is contended as under:

3.1. On 02.11.2018, a case was registered in Banaswadi Police Station Crime No. 588/2018 against Faith Phuks and two others for the offences punishable under Section 21(c) of Narcotic Drugs and Psychotropic Substances Act, 1985 and Section 14 of Foreigners' Act. After investigation, keeping open further

investigation interim final report was submitted to the Court. In continuation of the investigation and obtaining permission of the Court for further investigation, the Petitioner was apprehended and taken into custody. From the possession of the Petitioner incriminating evidence in the form of Mobile Phone, Laptop and other material objects seized and the property form prepared.

3.2. For the purpose of the investigation, it is necessary to open the Mobile Phones, other electronic gadgets seized from the Petitioner and the e-mails. The same is protected by passwords. Investigation Officer called upon the Petitioner to furnish the Passwords. The Petitioner refused to disclose the password of his Mobile Phone and e-Mail addresses. The Hon'ble Trial Court, by an order dated

04.09.2020, directed the Petitioner to co-operate and furnish the password to the investigating officer.

3.3. The order of the Trial Court was communicated to the Petitioner requesting him to furnish the password. In spite of the direction by the Trial Court the Petitioner did not furnish the password. On the contrary, he tried to contend that he has already provided the password, without having so provided.

3.4. It is on that basis that, Respondent No.2 filed an Application seeking permission of the Trial Court to subject the Petitioner to Polygraph test and the impugned orders passed.

3.5. On the facts and circumstances of the present case, the dicta laid down in the case of ***Selvi Vs. State of Karnataka reported in 2010***

(7) SCC Page 263 is not applicable to the case on hand as subjecting the Accused to Polygraph test for the limited purpose of unlocking the mobile by using the password and to furnish the password to open e-Mail does not amount to 'right against self-incrimination.'

3.6. It is contended that the direction of the Trial Court to the Petitioner to co-operate with the Investigating Officer and to unlock the mobile password is legal. Unlocking the mobile password does not amount to self-incrimination, nor does it violate Article 21 and 22 of the Constitution of India; unlocking mobile phone and/e-mails by furnishing a password does not amount to self-incrimination.

3.7. The contention of the Petitioner that the mobile phone contains his personal information which is protected under Right to Privacy cannot be accepted, the order of the Trial Court directing the Petitioner to co-operate in unlocking the mobile phone does not violate the Right to Privacy and does not amount to testimonial compulsion.

3.8. The Petitioner has not given the password of his mobile phone, or e-mail account, did not co-operate in the investigation; hence, the direction given by the Trial Court to unlock the mobile password of e-Mail addresses is justified and has not violated any rule of Law. The direction issued by the Trial Court to reveal the password to unlock his mobile phone and to open his e-Mail accounts does not amount to compelling him to be a witness

against himself, nor does it violate Section 161 (2) of the Code of Criminal Procedure.

3.9. Insisting upon the Petitioner for access to the data contained in his mobile phone does not amount to force him to reveal his personal information nor does it amount to self-incrimination.

3.10. On these grounds it is contended that the Petition is misconceived and is liable to be dismissed.

4. Shri Hasmath Pasha, Learned Senior counsel appearing for the Petitioner, submitted as under:

4.1. The order dated 23-9-2020 permitting second respondent police to subject Petitioner for polygraph test as requested by them is opposed to Law, and it is in violation of Article 21 and 22 of the Constitution.

Polygraph Test

4.2. The said order is in violation of the judgement of the Hon'ble Supreme Court in the case of ***Selvi V/s State of Karnataka reported in 2010(7) SCC page 263***, wherein the apex court has clearly laid down that subjecting the accused to a Polygraph Test is violative of *'right against self-incrimination'* which is a fundamental right guaranteed under article 20 clause (3) of the Constitution, he relies on the following paragraphs of the said judgement:

> ***184.*** *Even though the actual process of undergoing a polygraph examination or a BEAP test is not the same as that of making an oral or written statement, the consequences are similar. By making inferences from the results of these tests, the examiner is able to derive knowledge from the subject's mind which otherwise would not have become available to the investigators. These two tests are different from medical examination and the analysis of bodily substances such as blood, semen and hair samples, since the test subject's physiological*

responses are directly correlated to mental faculties. Through lie detection or gauging a subject's familiarity with the stimuli, personal knowledge is conveyed in respect of a relevant fact. It is also significant that unlike the case of documents, the investigators cannot possibly have any prior knowledge of the test subject's thoughts and memories, either in the actual or constructive sense. Therefore, even if a highly strained analogy were to be made between the results obtained from the impugned tests and the production of documents, the weight of precedents leans towards restrictions on the extraction of "personal knowledge" through such means.

185. *During the administration of a polygraph test or a BEAP test, the subject makes a mental effort which is accompanied by certain physiological responses. The measurement of these responses then becomes the basis of the transmission of knowledge to the investigators. This knowledge may aid an ongoing investigation or lead to the discovery of fresh evidence which could then be used to prosecute the test subject. In any case, the compulsory administration of the impugned tests impedes the subject's right to choose between remaining silent and offering substantive information. The requirement of a "positive volitional act" becomes irrelevant since the subject is compelled to convey personal knowledge irrespective of his/her own volition.*

186. *Some academics have also argued that the results obtained from tests such as polygraph examination are "testimonial" acts that should come within the prohibition of the right against self-incrimination. For instance, Michael S. Pardo (2008) has observed [cited from Michael S. Pardo, "Self-Incrimination and the Epistemology of Testimony" [30 Cardozo Law Review 1023-46 (December 2008)] ,Cardozo Law Review at p. 1046]:*

"The results of polygraphs and other lie detection tests, whether they call for a voluntary response or not, are testimonial because the tests are just inductive evidence of the defendant's epistemic state. They are evidence that purports to tell us either: (1) that we can or cannot rely on the assertions made by the defendant and for which he has represented himself to be an authority, or (2) what propositions the defendant would assume authority for and would invite reliance upon, were he to testify truthfully."

187. *Ronald J. Allen and M. Kristin Mace (2004) have offered a theory that the right against self-incrimination is meant to protect an individual in a situation where the State places reliance on the "substantive results of cognition". The following definition of "cognition" has been articulated to explain this position [cited from Ronald J. Allen and M. Kristin Mace, "The Self-Incrimination Clause Explained and its Future Predicted" [94 Journal of Criminal Law and Criminology 243-293 (2004)], Journal of Criminal Law and Criminology, Fn. 16 at p. 247]:*

"…'cognition' is used herein to refer to these intellectual processes that allow one to gain and make use of substantive knowledge and to compare one's 'inner world' (previous knowledge) with the 'outside world' (stimuli such as questions from an interrogator). Excluded are simple psychological responses to stimuli such as fear, warmness, and hunger: the mental processes that produce muscular movements; and one's will or faculty for choice. …"

(internal citations omitted)

The abovementioned authors have taken a hypothetical example where the inferences drawn from an involuntary polygraph test that did not require verbal answers, led to the discovery of incriminating evidence. They have

argued that if the scope of the Fifth Amendment extends to protecting the subject in respect of "substantive results of cognition", then reliance on polygraph test results would violate the said right.

188. *A similar conclusion has also been made by the National Human Rights Commission, as is evident from the following extract in the Guidelines Relating to Administration of Polygraph Test (Lie Detector Test) on an Accused (2000):*

"The extent and nature of the 'self-incrimination' is wide enough to cover the kinds of statements that were sought to be induced. In M.P. Sharma [AIR 1954 SC 300 : 1954 Cri LJ 865 : 1954 SCR 1077] the Supreme Court included within the protection of the self-incrimination rule all positive volitional acts which furnish evidence. This by itself would have made all or any interrogation impossible. The test—as stated in Kathi Kalu Oghad [AIR 1961 SC 1808 : (1961) 2 Cri LJ 856 . (1962) 3 SCR 10] —retains the requirement of personal volition and states that 'self-incrimination' must mean conveying information based upon the personal knowledge of the person giving information. By either test, the information sought to be elicited in a lie detector test is information in the personal knowledge of the accused."

189. *In light of the preceding discussion, we are of the view that the results obtained from tests such as polygraph examination and the BEAP test should also be treated as "personal testimony", since they are a means for "imparting personal knowledge about relevant facts". Hence, our conclusion is that the results obtained through the involuntary administration of either of the impugned tests (i.e. the narcoanalysis technique, polygraph examination and the BEAP test) come within the scope of*

"testimonial compulsion", thereby attracting the protective shield of Article 20(3).

II. Whether the involuntary administration of the impugned techniques is a reasonable restriction on "personal liberty" as understood in the context of Article 21 of the Constitution?

190. *The preceding discussion does not conclusively address the contentions before us. Article 20(3) protects a person who is "formally accused" of having committed an offence or even a suspect or a witness who is questioned during an investigation in a criminal case. However, Article 20(3) is not applicable when a person gives his/her informed consent to undergo any of the impugned tests. It has also been described earlier that the "right against self-incrimination" does not protect persons who may be compelled to undergo the tests in the course of administrative proceedings or any other proceedings which may result in civil liability. It is also conceivable that a person who is forced to undergo these tests may not subsequently face criminal charges. In this context, Article 20(3) will not apply in situations where the test results could become the basis of non-penal consequences for the subject such as custodial abuse, police surveillance and harassment among others.*

191. *In order to account for these possibilities, we must examine whether the involuntary administration of any of these tests is compatible with the constitutional guarantee of "substantive due process". The standard of "substantive due process" is of course the threshold for examining the validity of all categories of governmental action that tend to infringe upon the idea of "personal liberty". We will proceed with this inquiry with regard to the various dimensions of "personal liberty" as understood in the context of*

Article 21 of the Constitution, which lays down that:

"21. Protection of life and personal liberty.—No person shall be deprived of his life or personal liberty except according to procedure established by Law."

192. *Since administering the impugned tests entails the physical confinement of the subject, it is important to consider whether they can be read into an existing statutory provision. This is so because any form of restraint on personal liberty, howsoever slight it may be, must have a basis in Law. However, we have already explained how it would not be prudent to read the Explanation to Section 53 CrPC in an expansive manner so as to include the impugned techniques. The second line of inquiry is whether the involuntary administration of these tests offends certain rights that have been read into Article 21 by way of judicial precedents. The contentions before us have touched on aspects such as the "right to privacy" and the "right against cruel, inhuman and degrading treatment". The third line of inquiry is structured around the right to fair trial which is an essential component of "personal liberty".*

193. *There are several ways in which the involuntary administration of either of the impugned tests could be viewed as a restraint on "personal liberty". The most obvious indicator of restraint is the use of physical force to ensure that an unwilling person is confined to the premises where the tests are to be conducted. Furthermore, the drug-induced revelations or the substantive inferences drawn from the measurement of the subject's physiological responses can be described as an intrusion into the subject's mental privacy. It is also quite conceivable that a person could make an incriminating statement on being threatened*

with the prospective administration of any of these techniques. Conversely, a person who has been forcibly subjected to these techniques could be confronted with the results in a subsequent interrogation, thereby eliciting incriminating statements.

203. *This line of precedents shows that the compelled extraction of blood samples in the course of a medical examination does not amount to "conduct that shocks the conscience". There is also an endorsement of the view that the use of "force as may be reasonably necessary" is mandated by Law and hence it meets the threshold of "procedure established by law". In this light, we must restate two crucial considerations that are relevant for the case before us. Firstly, the restrictions placed on "personal liberty" in the course of administering the impugned techniques are not limited to physical confinement and the extraction of bodily substances. All the three techniques in question also involve testimonial responses. Secondly, most of the abovementioned cases were decided in accordance with the threshold of "procedure established by law" for restraining "personal liberty". However, in this case we must use a broader standard of reasonableness to evaluate the validity of the techniques in question. This wider inquiry calls for deciding whether they are compatible with the various judicially recognised dimensions of "personal liberty" such as the right to privacy, the right against cruel, inhuman or degrading treatment and the right to fair trial.*

226. *Therefore, it is our considered opinion that subjecting a person to the impugned techniques in an involuntary manner violates the prescribed boundaries of privacy. Forcible interference with a person's mental processes is not provided for under any statute and it most certainly comes into conflict with the "right against self-incrimination". However, this determination does*

not account for circumstances where a person could be subjected to any of the impugned tests but not exposed to criminal charges and the possibility of conviction. In such cases, he/she could still face adverse consequences such as custodial abuse, surveillance, undue harassment and social stigma among others. In order to address such circumstances, it is important to examine some other dimensions of Article 2.

Conclusion

262. *In our considered opinion, the compulsory administration of the impugned techniques violates the "right against self-incrimination". This is because the underlying rationale of the said right is to ensure the reliability as well as voluntariness of statements that are admitted as evidence. This Court has recognised that the protective scope of Article 20(3) extends to the investigative stage in criminal cases and when read with Section 161(2) of the Code of Criminal Procedure, 1973 it protects accused persons, suspects as well as witnesses who are examined during an investigation. The test results cannot be admitted in evidence if they have been obtained through the use of compulsion. Article 20(3) protects an individual's choice between speaking and remaining silent, irrespective of whether the subsequent testimony proves to be inculpatory or exculpatory. Article 20(3) aims to prevent the forcible "conveyance of personal knowledge that is relevant to the facts in issue". The results obtained from each of the impugned tests bear a "testimonial" character and they cannot be categorised as material evidence."*

4.3. The Petitioner is not willing or consenting for Polygraph Test, had there been an

opportunity provided to the Petitioner before passing the impugned order dated 23-9-2020, he would have mentioned the stand of *'no consent for Polygraph Test'*. Such opportunity not having been provided is a violation of his right against self-incrimination and right to privacy which are guaranteed under Articles 20 clause (3) and 21 of the Constitution

4.4. Therefore, involuntary Polygraph Test is prohibited under Law as laid down by the Hon'ble Supreme Court in the case of ***Selvi V/s State of Karnataka - reported in 2010 (7) SCC Page - 263***.

4.5. The decision of ***Selvi V/s State of Karnataka***, has been approved by Hon'ble Supreme Court in a recent decision of

Toofan Singh V/s State of Tamilnadu reported in 2020 SCC online SC 82.

4.6. The principle of ***Selvi's case*** has been reiterated in a case of ***Mr.JusticeK.S.Puttaswamy V/s Union of India reported in 2017 (10) SCC page 1***.

Violation of Principles of natural Justice:

4.7. Sections 53 and 311-A of the Code of Criminal Procedure also do not empower any Court or Magistrate to give direction to the accused during the investigation to give the password to unlock the mobile and thereafter to use the data available in mobile by the Investigation Officer in the investigation or trial of the accused.

4.8. Such an order could never have been passed,

much less without hearing the Petitioner or his counsel; the said order is violative of the principles of natural justice, more so the most fundamental Principle of *'Audi Alterm Partem'*.

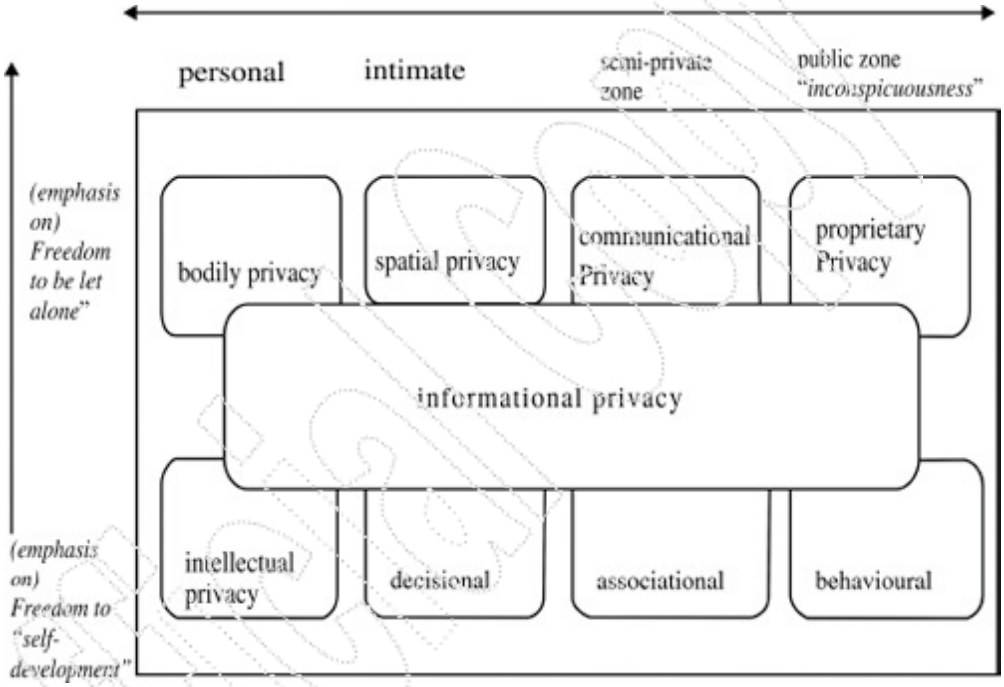
4.9. The said order is no order in the eye of Law as such an application was filed for recall of the order, the Court ought to have rectified its mistake taking into consideration the Judgment of the Apex Court. However, the Court did not.

Right to Privacy

4.10. Insisting the Petitioner to unlock his mobile phone which contains his personal information is violative of '*Right to Privacy'* as held by the Hon'ble Supreme Court in the case of ***Mr.JusticeK.S.Puttaswamy'scase***.

4.11. The order of Trial Court dated 14-9-2020 directing the Petitioner to co-operate by unlocking the mobile phone is contrary to the principle of the right to privacy and amounts to testimonial compulsion, which is guaranteed as fundamental rights; in this regard, he relies on the following paragraphs in ***Mr.JusticeK.S.Puttaswamy's case***.

> ***249.*** *Integrated together, the fundamental notions of privacy have been depicted in a seminal article published in 2017 titled "A Typology of Privacy" [Bert-Jaap Koops et al., "A Typology of Privacy", University of Pennsylvania Journal of International Law (2017), Vol. 38 Issue 2, at p. 566.] in the University of Pennsylvania Journal of International Law. The article contains an excellent visual depiction of privacy, which is presented in the following format:*



250. *The above diagrammatical representation presents two primary axes: a horizontal axis consisting of four zones of privacy and a vertical axis which emphasises two aspects of freedom: the freedom to be let alone and the freedom for self-development. The nine primary types of privacy are, according to the above depiction:*

(i) bodily privacy which reflects the privacy of the physical body. Implicit in this is the negative freedom of being able to prevent others from violating one's body or from restraining the freedom of bodily movement;

(ii) spatial privacy which is reflected in the privacy of a private space through which access of others can be restricted to the space; intimate relations and family life are an apt illustration of spatial privacy;

(iii) communicational privacy which is reflected

in enabling an individual to restrict access to communications or control the use of information which is communicated to third parties;

(iv) proprietary privacy which is reflected by the interest of a person in utilising property as a means to shield facts, things or information from others;

(v) intellectual privacy which is reflected as an individual interest in the privacy of thought and mind and the development of opinions and beliefs;

(vi) decisional privacy reflected by an ability to make intimate decisions primarily consisting one's sexual or procreative nature and decisions in respect of intimate relations;

(vii) associational privacy which is reflected in the ability of the individual to choose who she wishes to interact with;

(viii) behavioural privacy which recognises the privacy interests of a person even while conducting publicly visible activities. Behavioural privacy postulates that even when access is granted to others, the individual is entitled to control the extent of access and preserve to herself a measure of freedom from unwanted intrusion; and

(ix) informational privacy which reflects an interest in preventing information about the self from being disseminated and controlling the extent of access to information.

4.12. There is no specific law, enabling the taking away his right to privacy, or for a direction to be given by any court, either to give password of his mobile or to unlock the same and further to use the data contained in his mobile for the purpose of investigation.

4.13. Since the right to privacy is recognised as a fundamental right under Article 21 of the Constitution, to take away this fundamental right, even of an accused, there must be a law enacted by Parliament and the Law must meet the test of Article 21 as laid down in ***Maneka Gandhi's case*** i.e., it must be just, fair and reasonable not illusory.

4.14. Till today, no law is enacted by Parliament empowering any Court to give direction to accused to give password and information

contained in mobile phones. In the absence of this, the order of the Special Court dated 14-9-2020 is not sustainable in Law.

Self Incrimination

4.15. Even during police interrogation, the accused is entitled to remain silent, therefore insisting on revealing passcode or to unlock his mobile phone and to open his E-mail accounts amounts to compelling him to be a witness against himself, which is in violation of Section 161 (2) of the Code of Criminal Procedure and also under articles 20 clause (3) and 21 of the Constitution. In this regard, he relied on the decision of the Hon'ble Supreme Court of United States in ***Miranda vs. Arizona*** [**384 U.S. 436 (1966) DD 13.06.1966].**

In order fully to apprise a person interrogated of the extent of his rights under this system then, it is necessary to warn him not only that he has the right to consult with an attorney, but also that if he is indigent a lawyer wili be appointed to represent him. Without this additional warning, the admonition of the right to consult with counsel would often be understood as meaning only that he can consult with a lawyer if he has one or has the funds to obtain one. The warning of a right to counsel would be hollow if not couched in terms that would convey to the indigent—the person most often subjected to interrogation—the knowledge that he too has a right to have counsel present. As with the warnings of the right to remain silent and of the general right to counsel, only by effective and express explanation to the indigent of this right can there be assurance that he was truly in a position to exercise it.

Once warnings have been given, the subsequent procedure is clear. If the individual indicates in any manner, at any time prior to or during questioning, that he wishes to remain silent, the interrogation must cease. At this point he has shown that he intends to exercise his Fifth Amendment privilege; any statement taken after the person invokes his privilege cannot be other than the product of compulsion, subtle or otherwise. Without the right to cut off questioning, the setting of in-custody interrogation operates on the individual to overcome free choice in producing a statement after the privilege has been once invoked. If the individual states that he wants an attorney, the interrogation must cease until an attorney is present. At that time, the individual must have an opportunity to confer with the attorney and to have him present during any subsequent questioning. If the individual cannot obtain an attorney and he indicates that he wants one before speaking to police, they must respect his decision to remain silent.

> *This does not mean, as some have suggested, that each police station must have a 'station house lawyer' present at all times to advise prisoners. It does mean, however, that if police propose to interrogate a person they must make known to him that he is entitled to a lawyer and that if he cannot afford one, a lawyer will be provided for him prior to any interrogation. If authorities conclude that they will not provide counsel during a reasonable period of time in which investigation in the field is carried out, they may refrain from doing so without violating the person's Fifth Amendment privilege so long as they do not question him during that time."*

4.16. Insisting the accused for decryption of data contained in his mobile phone amounts to forcing him to reveal his personal information and even if any information regarding the commission of this offence or any other offence is contained therein, he can refuse to do so as contemplated U/s 161 (2) of Cr.P.C.

4.17. In this Writ Petition also the Petitioner has asserted that he has right to remain silent during police interrogation also and insisting him to give the password of his mobile

phone, is contrary to his right to remain silent as held by the Apex Court in ***Nandini Sathpathy v/s P.L.Danis 1978 (2) SCC 424***, and it amounts to testimonial compulsion hit by Article 20(3) of the Constitution.

4.18. Even in the famous decision of ***State of Bombay V/s Kathi Kalu Oghad reported in AIR 1961 SC Page 1808***, in para 11 which reads thus:

> *"To be a witness" means imparting of knowledge in respect of relevant facts by means of oral statements or statements in writing, by a person who has personal knowledge of the facts to be communicated to a court or to' a person holding an enquiry or investigation"*

4.19. Therefore, insisting the Petitioner - accused to give password of his mobile phone is imparting his knowledge by oral testimony or

in writing which is a Special knowledge in the mind of accused, cannot be forced to give, particularly when there is no specific law to that effect, even if the Law is enacted, how for it meets the Test of Article 20(3) and 21 of the Constitution?

4.20. The Application filed by the second respondent police lacks sanction of Law, and the Court erred in not following the Law and therefore the impugned orders dated 14-9-2020, 23-9-2020 and 15-10-2020 are all illegal and abuse of process of Law.

4.21. The Petitioner, in his Application dated 3-10-2020 has stated that he has fully co-operated for investigation and he has denied the allegation of not giving the password to unlock the mobile phone and further denied

the allegation of non-co-operation in opening E-mail accounts.

4.22. The principle of a right to remain silent of the accused during the investigation is well recognised in the decision of U.S.A Supreme court in ***Miranda V/s Arizona,*** which is applied worldwide and also by the Hon'ble Supreme Court in the decision Of ***Nandini Sathpaty V/s P.L.Danis and another reported in 1978(2) SCC Page 424***.

4.23. Mobile of Petitioner is seized in this case. Any mobile phone can be decrypted by experts. If the expert decrypt the mobile phone. Then the data available in the said mobile phone or any other electronic documents, if it is of nature protected under right to privacy, the same cannot be used without the consent of

owner, and if no consent is given, it cannot be taken, without the authority of Law.

4.24. Section 45-A of the Evidence Act, only describes the relevancy of the opinion of the examiner of Electronic Evidence as contemplated under Section 79-A of the Information Technology Act 2000.

4.25. But these provisions do not specifically provide for taking away the fundamental rights guaranteed under Article 20 (3) and 21, particularly the Right to privacy, is protected under Article 21 of the Constitution.

4.26. Therefore, the impugned orders dated 14-09-2020 and 23-09-2020, re-affirmed by order dated 15-10-2020, passed by the Hon'ble Special Court, take away the Constitutional Rights of Petitioner; hence those orders are

liable to be quashed.

5. Per Contra Shri VeeranaTigadi learned Special Public Prosecutor submitted as under:

5.1. Mobile phones, laptops and other materials were seized from the Petitioner. All the electronic gadgets obtained from the Petitioner are password protected.

5.2. On 14.09.2020, the investigating officer filed an application before the Trial Court seeking a direction to the Petitioner to co-operate with the investigation and divulge the password of Petitioner's mobile phone. The Trial Court allowed the Application filed by the investigation officer and directed the Petitioner herein to co-operate with the investigation officer to unlock the mobile password.

5.3. The application came to be filed only because the Petitioner did not divulge the passwords. If the Petitioner had divulged the password, there would have been no requirement to file the Application.

5.4. The order dated 14.09.2020 directing the Petitioner to furnish the password does not violate any of his rights under

5.4.1. Article 20(3) of the Constitution of India and Section 161(2) of the Code of Criminal Procedure, 1973;

5.4.2. Article 21 of the Constitution of India.

5.5. Article 20(3) of the Constitution of India provides that no person accused of an offence shall be compelled to be a witness against himself. In order to avail the benefit of this provision, the Petitioner must demonstrate

that:

5.5.1. the disclosure of the password is in the nature of personal testimony; and

5.5.2. the disclosure of the password would lead to self-incrimination.

5.6. Neither of the conditions being satisfied the order dated 14.09.2020 does not violate the rights of the Petitioner under Article 20(3) of the Constitution of India.

5.7. The disclosure of the password is not in the nature of personal testimony.

5.8. In ***Kathi Kalu Oghad***(paragraph 10, 11, 12, 13 and 16) a 11 judge bench of the Supreme Court of India held as under:

> ***10.*** *"To be a witness" may be equivalent to "furnishing evidence" in the sense of making oral or written statements, but not in the larger sense of the expression so as to include*

giving of thumb impression or impression of palm or foot or fingers or specimen writing or exposing a part of the body by an accused person for purpose of identification. "Furnishing evidence" in the latter sense could not have been within the contemplation of the Constitution makers for the simple reason that — though they may have intended to protect an accused person from the hazards of self-incrimination, in the light of the English Law on the subject — they could not have intended to put obstacles in the way of efficient and effective investigation into crime and of bringing criminals to justice. The taking of impressions of parts of the body of an accused person very often becomes necessary to help the investigation of a crime. It is as much necessary to protect an accused person against being compelled to incriminate himself, as to arm the agents of Law and the law courts with legitimate powers to bring offenders to justice. Furthermore it must be assumed that the Constitution-makers were aware of the existing Law, for example, Section 73 of the Evidence Act or Sections 5 and 6 of the Identification of Prisoners Act (33 of 1920). Section 5 authorises a Magistrate to direct any person to allow his measurements or photographs to be taken, if he is satisfied that it is expedient for the purposes of any investigation or proceeding under the Code of Criminal Procedure to do so: "Measurements" include finger impressions and foot-print impressions. If any such person who is directed by a Magistrate, under Section 5 of the Act, to allow his measurements or photographs to be taken resists or refuses to allow the taking of the measurements or photographs, it has been declared lawful by Section 6 to use all necessary means to secure the taking of the required measurements or photographs. Similarly, Section 73 of the Evidence Act authorises the Court to permit the taking of

finger impression or a specimen handwriting or signature of a person present in Court, if necessary for the purpose of comparison.

11. *The matter may be looked at from another point of view. The giving of finger impression or of specimen signature or of handwriting, strictly speaking, is not "to be a witness". "To be a witness" means imparting knowledge in respect of relevant facts, by means of oral statements or statements in writing, by a person who has personal knowledge of the facts to be communicated to a court or to a person holding an enquiry or investigation. A person is said "to be a witness" to a certain state of facts which has to be determined by a court or authority authorised to come to a decision, by testifying to what he has seen, or something he has heard which is capable of being heard and is not hit by the rule excluding hearsay, or giving his opinion, as an expert, in respect of matters in controversy. Evidence has been classified by text writers into three categories, namely, (1) oral testimony; (2) evidence furnished by documents; and (3) material evidence. We have already indicated that we are in agreement with the Full Court decision in Sharma case [(1954) SCR 1077] that the prohibition in clause (3) of Article 20 covers not only oral testimony given by a person accused of an offence but also his written statements which may have a bearing on the controversy with reference to the charge against him. The accused may have documentary evidence in his possession which may throw some light on the controversy. If it is a document which is not his statement conveying his personal knowledge relating to the charge against him, he may be called upon by the Court to produce that document in accordance with the provisions of Section 139 of the Evidence Act, which, in terms, provides that a person may be summoned to produce a*

document in his possession or power and that he does not become a witness by the mere fact that he has produced it; and therefore, he cannot be cross-examined. Of course, he can be cross-examined if he is called as a witness who has made statements conveying his personal knowledge by reference to the contents of the document or if he has given his statements in Court otherwise than by reference to the contents of the documents. In our opinion, therefore, the observations of this Court in Sharma case [(1954) SCR 1077] that Section 139 of the Evidence Act has no bearing on the connotation of the word "witness" is not entirely well-founded in Law. It is well established that clause (3) of Article 20 is directed against self-incrimination by an accused person. Self-incrimination must mean conveying information based upon the personal knowledge of the person giving the information and cannot include merely the mechanical process of producing documents in Court which may throw a light on any of the points in controversy, but which do not contain any statement of the accused based on his personal knowledge. For example, the accused person may be in possession of a document which is in his writing or which contains his signature or his thumb impression. The production of such a document, with a view to comparison of the writing or the signature or the impression, is not the statement of an accused person, which can be said to be of the nature of a personal testimony. When an accused person is called upon by the Court or any other authority holding an investigation to give his finger impression or signature or a specimen of his handwriting, he is not giving any testimony of the nature of a "personal testimony". The giving of a "personal testimony" must depend upon his volition. He can make any kind of statement or may refuse to make any statement. But his finger

impressions or his handwriting, in spite of efforts at concealing the true nature of it by dissimulation cannot change their intrinsic character. Thus, the giving of finger impressions or of specimen writing or of signatures by an accused person, though it may amount to furnishing evidence in the larger sense, is not included within the expression "to be a witness".

12. *In order that a testimony by an accused person may be said to have been self-incriminatory, the compulsion of which comes within the prohibition of the constitutional provision, it must be of such a character that by itself it should have the tendency of incriminating the accused, if not also of actually doing so. In other words, it should be a statement which makes the case against the accused person at least probable, considered by itself. A specimen handwriting or signature or finger impressions by themselves are no testimony at all, being wholly innocuous because they are unchangeable except in rare cases where the ridges of the fingers or the style of writing have been tampered with. They are only materials for comparison in order to lend assurance to the Court that its inference based an other pieces of evidence is reliable. They are neither oral nor documentary evidence but belong to the third category of material evidence which is outside the limit of "testimony".*

13. *Similarly, during the investigation of a crime by the police, if an accused person were to point out the place where the corpus delicti was lying concealed and in pursuance of such an information being given by an accused person, discovery is made within the meaning of Section 27 of the Evidence Act, such information and the discovery made as a result of the information may be proved in evidence*

even though it may tend to incriminate the person giving the information, while in police custody. Unless it is held that the provisions of Section 27 of the Evidence Act, insofar as they make it admissible evidence which has the tendency to incriminate the giver of the information, are unconstitutional as coming within the prohibition of clause (3) of Article 20, such information would amount to furnishing evidence. This Court in Sharma case was not concerned with pronouncing upon the constitutionality of the provisions of Section 27 of the Evidence Act. It could not, therefore, be said to have laid it down that such evidence could not be adduced by the prosecution at the trial of the giver of the information for an alleged crime. The question whether Section 27 of the Evidence Act was unconstitutional because it offended Article 14 of the Constitution was considered by this Court in the case of State of Uttar Pradesh v. Deomen Upadhyaya. It was held by this Court that Section 27 of the Evidence Act did not offend Article 14 of the Constitution and was, therefore, intra vires. But the question whether it was unconstitutional because it contravened the provisions of clause (3) of Article 20 was not considered in that case. That question may, therefore, be treated as an open one. The question has been raised in one of the cases before us and has, therefore, to be decided. The information given by an accused person to a police officer leading to the discovery of a fact which may or may not prove incriminatory has been made admissible in evidence by that section. If it is not incriminatory of the person giving the information, the question does not arise. It can arise only when it is of an incriminatory character so far as the giver of the information is concerned. If the self-incriminatory information has been given by an accused person without any threat, that will be

admissible in evidence and that will not be hit by the provisions of clause (3) of Article 20 of the Constitution for the reason that there has been no compulsion. It must, therefore, be held that the provisions of Section 27 of the Evidence Act are not within the prohibition aforesaid, unless compulsion had been used in obtaining the information.

16. *In view of these considerations, we have come to the following conclusions:*

(1) An accused person cannot be said to have been compelled to be a witness against himself simply because he made a statement while in police custody, without anything more. In other words, the mere fact of being in police custody at the time when the statement in question was made would not, by itself, as a proposition of Law, lend itself to the inference that the accused was compelled to make the statement, though that fact, in conjunction with other circumstances disclosed in evidence in a particular case, would be a relevant consideration in an enquiry whether or not the accused person had been compelled to make the impugned statement.

(2) The mere questioning of an accused person by a police officer, resulting in a voluntary statement, which may ultimately turn out to be incriminatory, is not "compulsion".

(3) "To be a witness" is not equivalent to "furnishing evidence" in its widest significance; that is to say, as including not merely making of oral or written statements but also production of documents or giving materials which may be relevant at a trial to determine the guilt or innocence of the accused.

(4) Giving thumb impressions or impressions of foot or palm or fingers or specimen writings

or showing parts of the body by way of identification are not included in the expression "to be a witness".

(5) "To be a witness" means imparting knowledge in respect of relevant facts by an oral statement or a statement in writing, made or given in Court or otherwise.

(6) "To be a witness" in its ordinary grammatical sense means giving oral testimony in Court. Case law has gone beyond this strict literal interpretation of the expression which may now bear a wider meaning, namely, bearing testimony in Court or out of Court by a person accused of an offence, orally or in writing.

(7) To bring the statement in question within the prohibition of Article 20(3), the person accused must have stood in the character of an accused person at the time he made the statement. It is not enough that he should become an accused, any time after the statement has been made.

5.9. The disclosure of the password by the Petitioner in terms of the order dated 14.09.2020 by itself does not incriminate the accused. Therefore, the disclosure of password can be viewed as anything but self-incrimination within the meaning of Article 20(3) of the Constitution of India.

5.10. The content of Section 161(2) of the Code of Criminal Procedure, 1973 is similar to Article 20(3) of the Constitution of India. In fact, Section 161(2) of the Code of Criminal Procedure, 1973 merely extends right against "*self-incrimination*" to suspects and witnesses in addition to '*persons formally accused of commission of an offence*'.

RIGHT TO PRIVACY:

5.11. In ***Justice K. Puttaswamy' case (supra)***, the Supreme Court of India held that '*right to privacy*' is 'an intrinsic element of the right to life and personal liberty under Article 21' embedded in Part III of the Constitution of India. However, the 9 judge bench has unanimously held that the right to privacy is not absolute and can be curtailed if the

following requirements are fulfilled:

5.11.1. legality, i.e. existence of a law;

5.11.2. legitimate state interest/ compelling state interest;

5.11.3. the action must be proportionate, i.e. there is a rational nexus between the object and means adopted to achieve them.

5.12. The order dated 14.09.2020 cumulatively satisfies all the aforesaid requirements and therefore does not abridge the rights of the Petitioner under Article 21 of the Constitution of India.

DISCLOSURE OF PASSWORD:

5.13. There are several provisions in the Code of Criminal Procedure, 1973 as well as the Indian Evidence Act, 1872 that empowered the Trial Court to direct the Petitioner to

disclose the password.

5.14. Section 139 of the Indian Evidence Act itself provides that a person may be summoned to produce a "*document*". The term "*evidence*" has been defined in Section 3 of the Indian Evidence Act *inter alia* to mean *"all documents including electronic records"*. Therefore, the term "*document*" used in Section 139 of the Indian Evidence Act includes any electronic record in possession of the Petitioner. Thus, Section 139 of the Indian Evidence Act authorises the disclosure of the password by the Petitioner and hence the order dated 14.09.2020 does not abridge Petitioner's right to privacy under Article 21 of the Constitution of India.

5.15. That apart, Section 54-A of the Code of

Criminal Procedure, 1973 *inter alia* stipulates that,

5.15.1. where a person is charged with committing an offence; and

5.15.2. his identification is necessary for the purpose of investigation of an offence, the Court may direct the person so arrested to subject himself to identification by any person as the Court deems fit.

5.16. In the present case, the password is nothing but an '*identification mark*' of the Accused/ Petitioner by the service providers hosting his data. Therefore, the disclosure of the password is sanctioned by Law under Section 54-A of the Code.

5.17. The disclosure of password is in the nature of giving specimen signatures or handwriting. Therefore, the disclosure of password can also be ordered under Section 311-A of the

Code of Criminal Procedure, 1973.

5.18. In ***Ritesh Sinha v. State of Uttar Pradesh (2019) 8 SCC 1***, the Supreme Court of India held that the Magistrate could order the collection of voice sample under Section 311-A of the Code of Criminal Procedure, despite there being no express provision to that effect, having regard to existing realities and imminent necessity of present situation. Therefore, given the fact that the disclosure of password is akin to giving specimen signature, disclosure can be ordered under the aforesaid provision. Hence, the order dated 14.09.2020 passed by the Trial Court is sanctioned by Law. In this regard, he relied upon paragraphs 5, 20 and 23 thereof, which are hereunder reproduced for easy reference:

5. *Two principal questions arose for determination of the appeal which have been set out in the order of Ranjana Prakash Desai, J. dated 7-12-2012 [Ritesh Sinha v. State of U.P., (2013) 2 SCC 357 : (2013) 2 SCC (Cri) 748] in the following terms: (Ritesh Sinha case [Ritesh Sinha v. State of U.P., (2013) 2 SCC 357 : (2013) 2 SCC (Cri) 748] , SCC p. 364, para 3)*

"3.1. Whether Article 20(3) of the Constitution of India, which protects a person accused of an offence from being compelled to be a witness against himself, extends to protecting such an accused from being compelled to give his voice sample during the course of investigation into an offence?

3.2. Assuming that there is no violation of Article 20(3) of the Constitution of India, whether in the absence of any provision in the Code, can a Magistrate authorise the investigating agency to record the voice sample of the person accused of an offence?"

20*. In the present case, the view that the Law on the point should emanate from the legislature and not from the Court, as expressed in the Judgment [Ritesh Sinha v. State of U.P., (2013) 2 SCC 357 : (2013) 2 SCC (Cri) 748] of this Court from which the reference has emanated is founded on two main reasons viz.:*

20.1. *The compulsion to give voice sample does in some way involve an invasion of the rights of the individual and to bring it within the ambit of the existing Law would require more than reasonable bending and stretching of the principles of interpretation.*

20.2. *If the legislature, even while making amendments in the Criminal Procedure Code (Act 25 of 2005), is oblivious and despite express reminders chooses not to include voice*

sample either in the newly introduced Explanation to Section 53 or in Sections 53-A and 311-A CrPC, then it may even be contended that in the larger scheme of things the legislature is able to see something which perhaps the Court is missing.

23. *The exercise of jurisdiction by constitutional courts must be guided by contemporaneous realities/existing realities on the ground. Judicial power should not be allowed to be entrapped within inflexible parameters or guided by rigid principles. True, the judicial function is not to legislate but in a situation where the call of justice and that too of a large number who are not parties to the lis before the Court, demands expression of an opinion on a silent aspect of the statute, such void must be filled up not only on the principle of ejusdem generis but on the principle of imminent necessity with a call to the legislature to act promptly in the matter.*

5.19. He relied on the decision of the Apex court in ***Sudhir Chaudhary v. State (NCT of Delhi), (2016) 8 SCC 307,*** more particularly para 7, 8, 9, 10, 11, 13 thereof which are hereunder reproduced for easy reference:

7. *The order of the ACMM was questioned before the Delhi High Court. By a judgment and order dated 11-2-2015 [Sudhir Chaudhry v. State, 2015 SCC OnLine Del 7457] , a learned Single*

Judge held that the purpose of a voice sample is to facilitate the process of comparing it with a recorded conversation. The voice sample is not a testimony in itself since it only constitutes what was described as "identification data". A voice sample, in the view of the High Court is not a substantive piece of evidence. The High Court rejected the submission that the direction to furnish a voice sample was in violation of the fundamental right under Article 20(3) of the Constitution since firstly, the appellants had not been forced or coerced into furnishing such a sample since it was they who had furnished their consent; secondly, a voice sample is not evidence since its purpose is only to compare it with the questioned text. In the view of the High Court, once the appellants had furnished their consent to furnishing their voice samples, it was not open to them to dictate the course of investigation. This order is called into question.

8. *The learned Senior Counsel appearing on behalf of the appellants submitted that while it is true that the appellants have consented to the drawing of their voice samples (a concession which was reiterated before this Court in the course of the submissions) yet the process of drawing the samples must be fair, so as to be consistent with the right of the appellants under Article 21 of the Constitution. The requirement of a fair investigation, it was urged, is implicit in Article 21 and the procedure which is adopted for drawing a voice sample must be fair and reasonable.*

9. *The appellants expressly consented to a voice sample being drawn in their response to the Application that was filed by the investigating officer before the Court of Metropolitan Magistrate. This was reiterated before the High Court. In the submissions which have been urged in these proceedings, the learned counsel has specifically stated that the appellants would*

abide by the consent which they had furnished to their voice samples being drawn. That being the position, the only surviving issue for this Court is to ensure that the underlying process for drawing the voice samples is fair and reasonable, having due regard to the mandate of Article 21. On the one hand, it is not open to the accused to dictate the course of investigation. Hence, we do not find substance in the submission that the text which is to be read by the appellants in the course of drawing their voice samples should contain no part of the inculpatory words which are a part of the disputed conversation. A commonality of words is necessary to facilitate a spectrographic examination.

10. *By our order dated 17-11-2015 [Sudhir Chaudhary v. State (NCT of Delhi), 2015 SCC OnLine SC 1689, wherein it was directed:"Heard. Mr S. Guru Krishna Kumar, learned Senior Counsel appearing for the respondent State, seeks a short adjournment to take instructions from the experts concerned whether or not a sample of words, in such number as the experts may suggest, would suffice for the experts to give their opinion by scientific voice sampling methods. He may do so by Tuesday, 1-12-2015. Post on Tuesday, 15-12-2015."] , this Court allowed an adjournment to the Respondent to seek instructions from the expert concerned whether or not a sample of words in such number as the expert may suggest would suffice for the experts to give their opinion by scientific voice sampling methods. Accordingly, a brief note has been filed on the record stating that:*

"That the experts of the Central Forensic Science Laboratory (CFSL) have informed that two separate texts/scripts have been prepared in the laboratory from each speaker/accused, which are different from the received transcripts.

That the text/script prepared by the CFSL experts cannot be provided to the petitioners in advance as there is apprehension that the Petitioner may practice the texts/scripts thereby adversely affecting the voice sampling examination. Accordingly it is submitted that the sample/modal text/script can only be supplied to the speakers/accused if this Hon'ble Court deems it appropriate."

11. *By an order of this Court dated 1-7-2016 [Sudhir Chaudhary v. State (NCT of Delhi), 2016 SCC OnLine SC 1707, wherein it was directed:"Arguments heard. Judgment reserved. In the meantime, the investigating officer shall file the transcript of the disputed conversation in a sealed cover. We further direct that the Director, Central Forensic Science Laboratory (CFSL) shall file in a sealed cover proposed passage of a written text, which the petitioners herein shall be required to read out, for purposes of giving their voice samples using words but not the sentences appearing in the disputed conversation in such number as the Director/Scientific Officer may consider necessary for purposes of comparison. Needful be done within four weeks."] , the investigating officer was directed to file a transcript of the disputed conversation in a sealed cover. The Director CFSL-CBI, was called upon to file in a sealed cover a proposed passage of a written text which the appellants shall be required to read out for the purpose of giving their voice samples using words, but not the sentences, appearing in the disputed conversation in such number as the Director/Scientific Officer may consider necessary for the purpose of comparison.*

12. *We are of the view that the aforesaid directions which have been issued by this Court would allay the apprehension of the appellants in regard to the fairness of the process involved in*

drawing the voice sample. Our directions ensure that the text which the appellants would be called upon to read out for the purpose of drawing their voice samples wiii not have sentences from the inculpatory text. Similarly, permitting the text to contain words drawn from the disputed conversation would meet the legitimate concern of the investigating authorities for making a fair comparison.

13. *In pursuance of the directions issued by this Court the investigating officer has filed in sealed cover: (i) transcripts of the disputed conversations; and (ii) a proposed passage of a written text required to be read out by the appellants for the purpose of giving their voice samples. The passage contains words but not the sentences appearing in the disputed conversation. Having perused the contents of the sealed covers, we are satisfied that the investigating officer has complied with our directions. We order accordingly.*

14. *The order [Sudhir Chaudhry v. State, 2015 SCC OnLine Del 7457] passed by the High Court shall accordingly stand modified and be substituted by the aforesaid directions.*

5.20. In **Justice K. Puttaswamy's case (supra)** the Supreme Court of India held that "***prevention and investigation of crime***" are among the legitimate interests of the state. The disclosure of the password is sought for investigating crimes under the

NDPS Act. Therefore, the order dated 14.09.2020 pursues a legitimate aim.

5.21. The action is proportionate because, it is merely seeking disclosure of the password in aid of the investigation. There is a rational nexus with the objective and means to achieve the objective.

5.22. In ***Selvi v. State of Karnataka (2010) 7 SCC 263, paragraph 262***, the Supreme Court of India has held that compulsory administration of polygraph tests violates "*right against self-incrimination*" enshrined in Article 20(3) of the Constitution of India.The order dated 23.09.2020 merely ordered the Petitioner to undergo a polygraph test. There is no order whatsoever for the test to be compulsorily conducted on the Petitioner.

Thus, if such a test is conducted with the Petitioner's consent, there will be no infraction of Article 20(3) of the Constitution of India.

5.23. The investigating officer has acted within the four corners of Law so as to conduct proper investigation; hence this Court ought not to interfere in the matter by relying on ***P. Chidambaram v. Directorate of Enforcement, (2019) 9 SCC 24*** more particularly paragraphs 64, 66, 67 and 68 thereof which are hereunder reproduced for easy reference:

> *64. Investigation into crimes is the prerogative of the police and excepting in rare cases, the judiciary should keep out all the areas of investigation. In State of Bihar v. P.P. Sharma [State of Bihar v. P.P. Sharma, 1992 Supp (1) SCC 222 : 1992 SCC (Cri) 192] , it was held that : (SCC p. 258, para 47)*
>
> *"47. … The investigating officer is an arm of the Law and plays a pivotal role in the dispensation*

of criminal justice and maintenance of Law and order. … Enough power is therefore given to the police officer in the area of investigating process and granting them the court latitude to exercise its discretionary power to make a successful investigation…."

66. As held by the Supreme Court in a catena of judgments that there is a well-defined and demarcated function in the field of investigation and its subsequent adjudication. It is not the function of the Court to monitor the investigation process so long as the investigation does not violate any provision of Law. It must be left to the discretion of the investigating agency to decide the course of investigation. If the Court is to interfere in each and every stage of the investigation and the interrogation of the accused, it would affect the normal course of investigation. It must be left to the investigating agency to proceed in its own manner in interrogation of the accused, nature of questions put to him and the manner of interrogation of the accused.

67. It is one thing to say that if the power of investigation has been exercised by an investigating officer mala fide or non-compliance of the provisions of the Criminal Procedure Code in the conduct of the investigation, it is open to the Court to quash the proceedings where there is a clear case of abuse of power. It is a different matter that the High Court in exercise of its inherent power under Section 482 CrPC, can always issue appropriate direction at the instance of an aggrieved person if the High Court is convinced that the power of investigation has been exercised by the investigating officer mala fide and not in accordance with the provisions of the Criminal Procedure Code. However, as pointed out earlier that power is to be exercised in rare cases where there is a clear abuse of power and non-compliance of the provisions

falling under Chapter XII of the Code of Criminal Procedure requiring the interference of the High Court. In the initial stages of investigation where the Court is considering the question of grant of regular bail or pre-arrest bail, it is not for the Court to enter into the demarcated function of the investigation and collection of evidence/materials for establishing the offence and interrogation of the accused and the witnesses.

Whether direction to produce the transcripts could be issued

68. The contention of the appellant is that it has not been placed before the Court as to what were the questions/aspects on which the appellant was interrogated on 19-12-2018, 1-1-2019 and 21-1-2019 and the Enforcement Directorate has not been able to show as to how the answers given by the appellant are "evasive". It was submitted that the investigating agency Enforcement Directorate cannot expect the accused to give answers in the manner they want and the investigating agency should always keep in their mind the rights of the accused protected under Article 20(3) of the Constitution of India. Since the interrogation of the accused and the questions put to the accused and the answers given by the accused are part of the investigation which is purely within the domain of the investigation officer, unless satisfied that the police officer has improperly and illegally exercised his investigating powers in breach of any statutory provision, the Court cannot interfere. In the present case, no direction could be issued to the Respondent to produce the transcripts of the questions put to the appellant and answers given by the appellant.

5.24. Hence, the order dated 23.09.2020 does not warrant interference.

5.25. On the above grounds, he sought for dismissal of the Writ Petition.

6. Heard Shri Hasmat Pasha, learned senior counsel for the Petitioner, Shri Veerana Tigadi, learned Special prosecutor for the Respondent state and perused papers.

7. On the basis of the pleadings filed and the arguments advanced the points which arise for determination by this Court are:

7.1. **Can a direction be issued to an accused to furnish the password, passcode or Biometrics in order to open the smartphone and/or email account?**

7.2. **Can a Court issue a *suo moto* order to the accused to furnish a password, passcode or Biometrics?**

7.3. **In the event of a direction being issued and the accused not furnishing the password, passcode or Biometrics, what is the**

recourse available to an Investigating Officer?

7.4. **What is the consideration for the issuance of a search warrant in order to search a smartphone or computer system?**

7.5. **Would the data gathered from a smartphone and/or email account *ipso facto* prove the guilt of the accused?**

7.6. **Would providing a password, passcode or Biometrics amount to self-incrimination or testimonial compulsion?**

7.7. **Would providing of password, passcode or Biometrics violate the right to privacy of a person providing the said password, passcode or Biometrics?**

7.8. **What steps could be taken if the accused or any other person connected with the investigation were to refuse to furnish a password, passcode or Biometrics despite issuance of a search warrant and or a direction to provide a password, passcode or Biometrics of that person?**

7.9. **What are the protection and safeguard that the Investigating Officer would have to take in respect of the smartphone and/or electronic equipment?**

7.10. **Whether the order dated 14.09.2020 passed by the Trial Court directing the Petitioner to co-operate with the investigating agency and provide a password to open the smartphone and email account is proper?**

7.11. **Whether the order dated 23.09.2020 passed by the Trial Court directing the Petitioner to undergo a polygraph test violates the rights of the Petitioner under Article 20 of the Constitution of India?**

7.12. **Whether the order dated 15.10.2020 passed by the Trial Court dismissing the Recall Application was in accordance with Law?**

7.13. **What order?**

8. **INTRODUCTION:**

8.1. Today technology has become all-pervasive, a telephone which was used in the past for communication now called a landline has given way to sophisticated instruments like smartphones which have computing powers probably thousand times more than that of computers of 90's leading to the mobile phone or a smartphone becoming the central device for running the affairs of the person.

8.2. The mobile phone,now called a smartphone, is truly smart and today is used for all purposes, one of which is as a phone for conversing with people.It may also not be wrong to say that the usage of a smartphone as a phone is the least used of its features.

8.3. The smartphone is being used today for various activities, including sending messages, conversing on social media like WhatsApp, Facebook, Twitter, Instagram, Telegram, Signaletc., sending and receiving e-mails from various accounts, be their personal or official.Usage of the smartphone for the purpose of accessing the internet, browsing world wide web, etc. carrying out online transactions, online purchases either by internet browser or through specified and specific applications, storage of photographs,

documents, retrieval of the documents stored in the cloud or on a remote server etc., etc., the list could go on and on.

8.4. Essentially today, a smartphone,in many cases, has replaced the laptop, which had replaced the office, and the smartphone by itself is an office for several persons.

8.5. The Law of Evidence and the Criminal Procedure Code that had been enacted long ago have also been amended from time to time to try and cater to the tremendous technological improvements, apart thereform the Information Technology Act, 2000 (***IT Act***) has been enacted and amended from time to time to cater to these technological improvements.

8.6. The following definitions under IT Act would be relevant for consideration of the present matter:

> ***2(ha)*** *"**Communication device**" means cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image;]*
>
> ***(i)*** *"**computer**" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network;*
>
> ***(j)*** *"**computer network**" means the inter-connection of one or more computers or computer systems or communication device through;*
>
> > ***(i)*** *the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and*
> >
> > ***(ii)*** *terminals or a complex consisting of two or more*

interconnected computers or communication device whether or not the inter-connection is continuously maintained;

(k) *"**computer resource**" means computer, computer system, computer network, data, computer data base or software;*

(l) *"**computer system**" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;*

(o) *"**data**" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;*

(r) *"**electronic form**" with reference to information, means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;*

(t) *"**electronic record**" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;*

(v) *"**information**" includes [data, message, text,] images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche;*

8.7. The following definitions in the interpretation clause of Section 3 of the Indian Evidence Act would be relevant:

3. Interpretation clause. *—In this Act the following words and expressions are used in the following senses, unless a contrary intention appears from the context:*

"Fact". *—"Fact" means and includes:-*

(1) any thing, state of things, or relation of things, capable of being perceived by the senses;
(2) any mental condition of which any person is conscious.

"Document":- *"Document" means any matter expressed or described upon any substance by means of letters, figures or marks, or by more than one of those means, intended to be used, or which may be used, for the purpose of recording that matter.*

"Evidence":- *" Evidence" means and includes—*
(1) all statements which the Court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry, such statements are called oral evidence;

(2) [all documents including electronic records produced for the inspection of the Court], such documents are called documentary evidence.

8.8. In the past, when any document was marked in evidence, it was more often than not, restricted to a document in a physical format viz., one either written or printed on

a paper.Today a document could be both physical and electronic, in any form or formatsin different combination like binary, encrypted, etc.

8.9. Juxtaposing the above to the definitions of an electronic form and electronic record under the IT Act, it can be seen that the definition of these two phrases seek to encompass and cover all kinds of methodology of storing data, documents as an image, photographs, documents or otherwise.Essentially all kind of images, documents, etc. can be classified as data inasmuch as the data being information stored in a particular kind of media.

8.10. Though even earlier documents were referred to and used for the purpose of

evidence, essentially even at that point of time what it referred to was the data in the said document viz., the printed or written word in the document, therefore whether documentary evidence or electronic evidence essentially what one is dealing with is data.

8.11. It is this data that is required to be accessed by an Investigating officer for the purposes of carrying out an investigation; this data is required for the purposes of being referred to while a charge sheet is being laid, it is the data that would be considered by a Court of Law during the course of evidence and/or rendering of the Judgment.

8.12. In the past, letters, postcards, Island letters, telex, fax were used for the purpose of communication.This communication essentially resulted in a hard copy being sent or printed at the recipient's end.This document, in its physical form,wasconsidered, relied upon as original document during the investigation process and later-on produced and marked during the course of evidence being led in a proceeding and considered by a Court.

8.13. Smartphones and/or computer equipment are becoming ubiquitous, hard copies/print outs/ books, filing cabinets, essentially anything on paper is becoming obsolete.

8.14. As aforestated, today this physical document has taken on an electronic

appearance, and these electronic documents/data could be stored on the mobile phone, computer or the like.More often than not, these smartphones, computers, servers, etc., are accessed only by using a password/passcode, including that by biometrics technology, facial recognition, iris recognition etc.Thus without having the said password, passcode, biometric, no one can access either a mobile phone, computer or server.Some times even safes, filing cabinets, etc., are also locked using the above methodology.

8.15. It is in this background that the above matter would have to be considered.

9. **<u>ANSWER POINT No.1:</u> Can a direction be issued to an accused to furnish the password, passcode or Biometrics in order to open the smartphone and/or email account?**

9.1. The Investigating Officer, during the course of an investigation, could always issue any direction and/or make a request to the accused or other persons connected with the matter to furnish information, to provide material objects or the like. These directions are routine in any investigation. Thus, during the course of the investigation, the Investigating Officer could always request and/or direct the accused to furnish the password, passcode or Biometrics, enabling the opening of the smartphone and/or email account. It is up to the accused to accede to the said request and or directions. If the accused were to provide such a password, passcode or Biometrics, the Investigating Officer could make use of the same and gain an access to the same.

10. <u>ANSWER TO POINT NO.3:</u> Can a Court issue a *suomoto* order to the accused to furnish a password, passcode or Biometrics?

10.1. The Court cannot *per se* issue any directions to the accused to furnish the password, passcode or Biometrics and direction to cooperate would not amount to a direction to furnish password, passcode or Biometrics. The gathering of information and/or evidence, mode and methodology of investigation is in the *exfacie*domain of the Investigating Officer.

10.2. The court by itself cannot *suo moto* order for furnishing of the password, passcode or Biometrics. The Court is not part of the investigation. The Court can only act on an application being filed by either of the parties.

11. **<u>ANSWER TO POINT NO.4:</u> In the event of a direction being issued and the accused not furnishing the password, passcode or Biometrics, what is the recourse available to an Investigating Officer?**

11.1. In the event of the accused not providing the password, passcode or Biometrics, the Investigating Officer can approach the Court seeking for necessary directions to the accused to provide the same and/or carry out a search of the smartphone or any electronic equipment.

11.2. The Investigating Officer could approach the concerned Court seeking for issuance of a search warrant to carry out a search of the smartphone and/or electronic equipment.

12. **<u>ANSWER TO QUESTION NO.5:</u> What is the consideration for the issuance of a search warrant in order to search a smartphone or computer system?**

12.1. The requirement for a search of a smartphone and/or electronic instrument could arise under two circumstances.

12.1.1. Emergent circumstances

12.1.2. During the regular ordinary course of the investigation

12.2. It is in light of these two circumstances that the nature and methodology of a search would have to be considered.

12.3. The Cr.P.C. provides a framework for carrying out a search of any premises or the like. There is no particular or different framework provided for the purposes of search of a smartphone or electronic equipment, computer, server etc. Thus, it is the framework under Cr.P.C. and to some extent

under the Information Technology Act, which would have to be made applicable to searches of these kinds.

12.4. Chapter VII of Cr.P.C. provides for search, seizure, production etc. Section 91 of Cr.P.C. enables any Court or any officer in charge of a police station to issue summons or order to the person in whose possession or power such a document or thing are believed to be requiring him to attend and produce it at the time and place indicated in the said summon or order.

12.5. Section 92 of Cr.P.C. provides the power to the District Magistrate, Chief Judicial Magistrate, Court of Sessions or High Court to require the postal or telegraph authority for the purposes of investigation, enquiry or trial

to order the postal or telegraph authority to deliver the document, parcel or thing in the custody of postal or telegraph authority. Similarly, the Commissioner of Police or District Superintendent of Police may require the postal or telegraph authority to cause search, detain the document or parcel and produce the same before the Court. It is pertinent to mention here that the correspondence email etc., would be covered under the Telegraph Authority.

12.6. Section 93 of the Cr.P.C. provides powers to the Court to issue a search warrant

12.6.1. On a person not willing to produce a document or a thing as directed under Section 91 of Cr.P.C., or

12.6.2. Where the document or thing is not known to be in possession of any

person or

12.6.3. Where the Court considers that for the purpose of any enquiry, trial or other proceedings, a general search or inspection would serve the purpose.

12.7. In terms of Section 93 (2) of Cr.P.C., the Court could also restrict the search to a specific place, a specific time or a specific purpose.

12.8. Section 94 of Cr.P.C. confers power on certain Courts to search places suspected to contain stolen property, objectionable article, forged documents, counterfeit material, obscene objects, instruments or materials used for the production of any item under Section 94 (2) of Cr.P.C., and to take such action as may be required in terms of Section 94(1) of Cr.P.C., thereof.

12.9. In terms of Section 100 of Cr.P.C., in the event of any place being closed, any person residing in or being in charge of such place shall on demand of the officer or other person executing the warrant and on the production of the warrant allowing free ingress thereto. As also afford all reasonable facilities for a search therein. In the event of any person suspected to be concealing any article, a search of such person could also be made subject to however restrictions that a search of any woman could be made by a woman.

12.10. During the process of search in terms of Section 102 of Cr.P.C., any particular item could be seized by a person conducting a search on fulfilling certain criteria.

12.11. In view of the above, the said Chapter VII provides several powers to the Police or Magistrates, which could include the power to search and seize a smartphone, computer, server or any other electronic item or equipment.

12.12. A search and seizure of a smartphone can also be permitted in terms of the above provisions as contained in the Cr. P.C. As observed above, in terms of Section 100 of Cr.P.C., even a closed place can be searched by the persons searching directing any person incharge of a place to open the same and provide all facility. It is in the background of the above provisions that the aspect of search of a smartphone or electronic equipment, including an e-mail account will have to be considered.

Search and Seizure in Emergent circumstances

12.13. It may happen that there may arise certain emergencies or exigencies for a search of a smartphone or electronic equipment to be carried out like if the data is going to be immediately destroyed, there is a danger of equipment itself being destroyed, the possibility of the equipment not being available, etc.

12.14. In terms of Section 102 of Cr.P.C., if there are any emergency circumstances, the Police Officer could seize the equipment; if there is any suspicion that either the object has been stolen or which create suspicion of commission of any offence.

12.15. The second aspect as regards of suspicion of

any commission of any offence is wide enough to cover a plethora of situation. Thus, in an emergent situation, the Police Officer could seize the electronic equipment.

12.16. In emergent circumstances, it cannot be expected of the Investigating officer to rush to a court of Law to obtain a warrant, such a requirement would amount to negating their powers and impinging on their functions. When there is adequate time to obtain a warrant, the same ought to be obtained, however, if an urgent search is to be conducted and it may be difficult to get a search warrant, certain safeguards will have to be observed and conditions fulfilled.

12.17. There must exist reasonable grounds for believing that it is necessary for carrying out

a search of the Smartphoe or Electronic Equipment with expediency and that if such a search is not conducted immediately, the conduct of the offence may be expedited and/or the evidence thereof be lost.

12.18. In such a scenario, there must be a recording in writing made by the Investigating officer, specifying in writing as far as possible the reasons for conducting such a search without a warrant. The objective satisfaction by such officer of the emergent nature of the search has to be recorded in writing in sufficient detail. Unless these conditions are fulfilled, a search without a warrant would be without jurisdiction, these conditions are necessary to safeguard the interest of the person and or organization searched, more so when a search so conducted would also impinge on

the right to privacy of such a person.

12.19. In terms of Section 165 of Cr.P.C., if the investigating officer during the course of investigation has reasonable grounds for believing that anything required for the purpose of investigation would be found in a place within the limits of his police station of which he is incharge of or attached to, he may without delay after recording in writing the grounds for belief and specifying in writing as far as possible, the thing for which search is to be made, search any place within his limits of jurisdiction. However, the copies of any record made to conduct such a search would have to be sent to the Magistrate empowered to take cognizance of an offence and a record of the same. Though a search without reasons and without following the

procedure may be illegal, the illegality of the search would not make any seizure made during the search inadmissible as held by the Hon'ble Apex Court in the case of ***Dr.Pratap Singh vs. Director of Enforcement Foreign Exchange Regulation and others*** *reported in* ***(1985) 3 SCC 72***. However, the Courts would have to be cautious while dealing with the evidence collected in such an illegal search.

Search and Seizure during the regular ordinary course of the investigation

12.20. If the search is required to be carried out in a normal and regular course of an investigation, in that situation, the investigator or investigating agency would have sufficient time to plan out the manner of carrying out such a search as there being no

emergency or immediate requirement of carrying out such search.

12.21. The investigating officer could issue a notice under Section 91 of Cr.P.C., calling upon the accused or any other person to produce any particular document or equipment as stated above. If not so produced, a search warrant could be sought for from the Court of law. Be that as it may without issuance of a notice under Section 91 of Cr.P.C., a search warrant could be issued inasmuch as the issuance of a notice under Section 91 of Cr. P.C. is not a pre-condition for issuance of a search warrant under Section 93 of Cr. P.C. Once a search warrant is issued and received by the accused or any other person it would be the obligation of such person to permit the search and/or to provide document or thing called upon.

12.22. While issuing a search warrant, the concerned Court would have to indicate as to what smart phone, electronic equipment or email account is to be searched. The role of the same in the crime, the nature of search to be done, place where the search has to be done as also specifically interdict the persons carrying out the search from disclosing the material and/or data procured during the course of the said search to a third party. So as to preserve the privacy of the concerned.

12.23. The provisions referred to and mentioned deals with search and seizure. Electronic equipment occupies a slightly different position, in that it is not only the seizure of the phone and equipment, but once it is seized, the said equipment is required to be opened more often than not such equipment

are locked by password, passcode or biometrically. Thus, for the purpose of opening and/or accessing the data on the said equipment, it would be required for the accused or person in charge of the said equipment to provide a password, passcode or open the same using the biometrics.

12.24. As mentioned above, in terms of Section 100 of Cr.PC., a person in charge of a closed place is also required to permit such search and, in fact, facilitate such search.

12.25. Applying the said principle to a smartphone, electronic equipment or an email account, it would but be required for the accused or a person in charge of electronic equipment to provide the password, passcode or biometrics to open the Smartphone, computer

equipment or email account.

12.26. It is these aspects which have to be considered in the present circumstances. Section 69(1) of the IT Act empowers the specified officers to pass orders compelling the decryption of any information, generated, transmitted, received or stored in a computer resource which would also include a smartphone.

12.27. When the said authority is satisfied that it is necessary for the purpose of any investigation into any offence, however, an officer, before ordering such decryption, is required to record in writing the reasons for calling upon for such decryption and inform the person of the possibility of prosecution if he does not comply with a request.

12.28. Search and seizure are important weapons in the hands of the officers concerned therefore it is but required that such powers should be exercised with due circumspection and discretion, and the same should not result in harassment of innocent persons. When a search is made with a warrant, the procedure required to be followed is stated in the Cr. P.C, which need to be so followed. Even when a search is made without a search warrant, it would be treated that such a search or consequent seizure is conducted/made the safeguards enshrined under the Cr. P.C.

12.29. As observed above, the officers conducting a search are required to comply with the procedural requirements of Cr.P.C, some of them though not exhaustive,are enumerated

hereunder:

12.29.1. A lady officer is required to be present if the accused is a lady or if the equipment is located in a place where there are ladies present.

12.29.2. The search and seizure should normally be done after sunrise and before sunset. However, if it is conducted after sunset and before sunrise, the grounds as to why it was felt necessary to take such action should be recorded and copy of the grounds so recorded must be sent within 72 Hours to the immediate official superior.

12.29.3. The officers before starting the search are required to disclose their identity

by showing their identity cards to the owner of the premises.

12.29.4. Search should be made in the presence of two independent and respected witnesses of the locality.

12.29.5. A Panchnama / Mahazar, should be prepared on the spot which contains the proceedings of the search. A list of all goods, documents recovered and seized/detained should be prepared and annexed to the Panchnama/Mahazar. This document and the list of things seized needs is to be signed by the witnesses and the owner of the premises before whom the search is conducted and also by the officers who are carrying out the

said search.

12.29.6. After examination of the seized goods or things by the authority, the same to be sent for any technical/forensic examination within a period of 72 hours thereof.

12.29.7. A search and seizure report to be prepared containing the details of the conduct of the search and outcome, containing the names of the officers and other persons including the panchas and witnesses who participated in the search.

12.29.8. A copy of the Panchnama / Mahazar prepared to be furnished to the person in- charge/owner of the premises being searched under

acknowledgement.

13. **<u>ANSWER TO QUESTION NO.6:</u>Would the data gathered from a smartphone and/or email account *ipso facto* prove the guilt of the accused?**

13.1. Since, as stated above, a smartphone can contain humongous data, which could also be incriminatory insofar as the person owning the said electronic equipment, including the smartphone, is concerned and it is in this background, we have to consider the providing of a password, passcode or biometrics and whether making available, this incriminatory material would amount to giving of testimony and or a statement in terms of Section 161 of Cr.P.C.

13.2. On a notice being issued under Section 160 of Cr.P.C., any witness could be examined by

the police, the witness could be the accused himself.

13.3. Such a statement needs to be reduced to in writing wherein such person is required to answer all questions relating to such case, other than the questions, the answer to which would have the tendency to expose him to a criminal charge or a penalty or forfeiture. That being a right to protection of self-incrimination as enshrined under Article 20 of the Constitution of India.

13.4. Though Mr Tigadi, learned counsel for the Respondent contended that the disclosure of password is in the nature of giving specimen signatures or handwriting and therefore a direction could be issued under Section 311-A of the Cr. P.C, I'm of the considered opinion

that the providing of a password, passcode or biometrics is more than that, and a direction cannot be issued in that manner.

13.5. In the event of password, passcode or Biometrics being provided and the Investigating Officer gaining access to the said smartphone and/or electronic equipment or email account, the data so gathered would have to be treated as any other document and/or object secured during the course of investigating like in the case of securing a murder weapon. The same does not by itself prove that the accused has committed the murder, similarly, the data gathered by itself would not prove the guilt of the accused. The data gathered would have to be proved during the course of the trial as done in any other matter.

14. **<u>ANSWER TO POINT NO.7:</u>Would providing a password, passcode or Biometrics amount to self-incrimination or testimonial compulsion?**

14.1. As regards the contention that providing of the password/pass code will amount to testimonial compulsion, I am of the considered opinion that there is no testimony which is given by the accused by providing the said password, passcode or biometrics by which the document is being accessed by the Investigating officer.

14.2. The XI Judge Bench of the Apex Court in ***Kathi Kalu Oghad's*** case has categorically held that providing of a thumb impression or impression of the palm or foot or fingers or specimen in writing or exposing a part of the body of an accused person for the purpose of identification would not amount to testimonial

compulsion. Mere providing of an access of to smartphone or e-mail account would not amount to being a witness, the information that is accessed by the Investigating officer on the smartphone and or the e-mail account being only access to the data and/or documents, it is for the Investigating officer to prove and establish the same in a Court of Law by following the applicable Rules of evidence.

14 3. Merely because any document is present or available on the smartphone and or the e-mail account would not by itself establish the guilt or innocence of an accused. Both the prosecution, as also the accused/defence would be required to prove the said document or data by other evidence also.

14.4. If the submission of Mr.Hasmath Pasha, learned Senior counsel would be accepted, the same would result in a chaotic situation:

14.4.1. No blood samples can be taken;

14.4.2. no sample for DNA analysis could be taken;

14.4.3. no handwriting samples can be taken;

14.4.4. no other body sample for the purpose of DNA analysis could be taken

14.4.5. No search of a house or office could be undertaken.

14.4.6. The data of a laptop or computer or server cannot be accessed by the Investigating officer.

14.4.7. offences like cyber crime could never be investigated.

14.4.8. Offences like pornography, child pornography which are more often than not, on the internet, could not be investigated.

14.5. A direction to provide a password, passcode, biometrics would not amount to testimonial compulsion. It is only in the nature of a direction to produce a document. Mere providing access to a smartphone or e-mail account would not amount to self-incrimination since it is for the investigating agency to prove its allegation by cogent material evidence.

14.6. The data available on a smartphone or e-mail account would also have to be proved by the investigating agency in accordance with Law. Mere providing of password, passcode or

biometrics would not amount to answering any question put forward by the Investigating Officer, and as such, it would not amount to a violation of Section 151(2) of the Cr.P.C.

14.7. As contended by Sri.Veranna Tigadi, learned counsel providing of the password, passcode, pin, biometrics is akin to finger printing and/or taking imprints of the shoes, soles and or taking sample of the clothes, biological samples, chemical samples, etc, same cannot amount to forced testimony on part of the accused. On the examination of the data in the telephone/mobile and or on the computer, etc, prosecution would have to prove the same by cogent evidence.

14.8. By providing of password, passcode or biometrics, there is no oral statement or a

written statement being made by the accused like the Petitioner herein, therefore it can not be said to be testimonial compulsion.

15. **<u>ANSWER TO QUESTION NO.8:</u>Would providing of password, passcode or Biometrics violate the right to privacy of a person providing the said password, passcode or Biometrics?**

15.1. This aspect is to be considered in light of the principles propounded by the Hon'ble Apex Court in ***Justice Puttaswamy's*** case supra. More so, in view of the fact that the data which could be available on the said electronic equipment being personal in nature could also be misused by the investigating agency and/or the investigating agency would come into possession of personal data which are held secret by that person which have nothing to do with the investigation at all more so since there cannot be a strict

compartmentalisation of data as personal or not personal in the said equipment belonging to a person or in the e-mail account.

15.2. Once the investigating agency has an access to a electronic equipment more particularly smart phones and/or laptops, the Investigating Officer has a free access to all data not only on the said equipment but also any cloud service that may be connected to the said equipment, which could include personal details, financial transactions, privileged communications and the like.

15.3. The rules which are applicable to physical document where a particular document could be classified as a privileged communication and/or strictly private and confidential cannot apply to the data which is stored on a

smartphone or any other electronic equipment since once an investigating officer has an access to the said smartphone, electronic equipment or e-mail account, he would have complete access to the data.

15.4. Such data though may not be incriminatory, may be very private or secret to the person or such data could incriminate the said person in any particular offence.

15.5. The use of such data during the course of the investigation would not amount to a violation of the right to privacy and would come within the exceptions carved out in ***Justice Puttaswamy's*** case supra, however, the disclosure, making public or otherwise in court proceedings would have to be determined by the concerned judge by

passing a judicial order. In no case could such details or data be provided by the investigating officer to any third party during the course of investigation without the written permission of the court seized of the matter. The responsibility of safeguarding the information or data which could impinge on the privacy of the person will always be that of the investigating officer, if the same is found to have been furnished to any third party the investigation officer would be proceeded against for dereliction of duty or such other delinquency as provided.

16. **ANSWER TO POINT NO.9:What steps could be taken if the accused or any other person connected with the investigation were to refuse to furnish a password, passcode or Biometrics despite issuance of a search warrant and or a direction to provide a password, passcode or Biometrics of that person?**

16.1. Though not argued or contended this Court would also have to take into consideration the possibility of the accused not co-operating inspite of above directions having been issued and/or providing apassword, passcode which is incorrect.

16.2. In the event of the accused not co-operating and not providing necessary password, passcode adverse inference could be drawn subject to the prosecution pointing out the nature of such adverse inference which could be drawn.

16.3. The second situation is even more dangerous inasmuch as the accused may provide a wrong password or passcode and or provide biometrics of a wrong person, and sometimes by way of the usage of such wrong password,

passcode or biometrics for more times than one, the device could either get locked and/or the data on the said device and the e-mail account could be wiped out automatically because a wrong password, passcode or biometrics has been used multiple times. The Investigating agency therefore has to be aware of and careful of this possibility.

16.4. The accused in such a situation is therefore required to be given only one chance to provide the proper password, passcode or biometrics to open the smartphone and e-mail account.

16.5. In both the above situations, the Investigating Agency would also be at liberty to engage such specialised agency as may be required in order crack the password,

passcode or biometrics so as to have access to the smartphone and or the e-mail id. The accused cannot thereafter contest the methodology used by the Investigating Agency to access the information on the smartphone or e-mail account since the accused having been given an opportunity to co-operate and provide the password, passcode, or biometrics, has refused to co-operate and do so,

16.6. The rules of electronic device would apply to any data if sought to be made use of by the Investigating agency in a Court of Law. The Investigating agency would be at liberty to clone the smartphone and or hard disk of the smartphone, as also any data available on any cloud service to which the smartphone is connected to and make use of the same

during the course of investigation and/or trial.

16.7. Similarly the Investigating agency would be at liberty to block the access to the e-mail accounts once opened by changing the password so that no one else apart from the designated officers would have access to the said smartphone, computer equipment or e-mail accounts. The data available on the said e-mail account could be downloaded and preserved, as also made use of by the Investigating agency for the investigation.

16.8. Thus the procedure that would have to be followed would be as under:

16.9. It would be required for the prosecution to approach the Court to seek a search warrant to search the smartphone and or e-mail

account. Once a search warrant is issued, it is upto the Petitioner- accused to provide the password, passcode, biometrics etc.,

16.10. The investigating agency could also serve a notice on the accused indicating that in the event of the accused not furnishing the said password, passcode, biometrics etc., an adverse inference would be drawn against the accused as regards the aspects notified in the said notice. The accused can then,in order to avoid the adverse inference from being drawn, furnish the password, passcode or biometrics to the Investigating authorities.

16.11. In the event of the accused or any other person not providing the password, passcode or biometrics, on an application made by the prosecution, the court could direct the service

provider viz., manufacturer of the smartphone and/or e-mail service provider, to open or unlock the smartphone and/or email account to enable access to the said smartphone and/or email account.

16.12. In the event of the manufacturer and the service provider not facilitating the opening of the smartphone, email account or computer equipment, then the Court on an application being filed in that regard permit the Investigating Officer to hack into the smartphone and/or email account.

16.13. The investigating agency would be empowered to engage the services of such persons as may be required to hack into the smartphone and or e-mail account and make use of the data available therein, which would

be akin to breaking open a lock or door of the premises when the accused were to refuse to co-operate with the Investigating officer and open the door of locked premises.

16.14. In the event of the investigating agency is unsuccessful in hacking into the smartphone and or the e-mail account and during the course of such a procedure, if the data on the smartphone and or the e-mail account being destroyed then, the Investigating agency/prosecution would be free to rely upon the notice by which the accused was warned of adverse inference being drawn.

17. **ANSWER TO POINT NO.10:What are the protection and safeguard that the Investigating Officer would have to take in respect of the smartphone and/or electronic equipment?**

17.1. It is required for the Investigating Officer or

the search team to carry out the search in a proper and scientific manner, more so since what has to be searched in the electronic equipment, smartphone or email account.

17.2. Apparently, there are no rules formulated by the police department regarding the manner of carrying out a search and/or for preservations of the evidence gathered during the said search in respect of smartphone, electronic equipment or email account.

17.3. It would be in the interest of all the stakeholders that detailed guidelines are prepared by the police department in relation to the same.

17.4. Pending such formulation, it would be required that the following minimum

guidelines are implemented:

17.5. In the case of a personal computer or a laptop:

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

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

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

17.5.4. The front and back of the computer and/or the laptop while connected to all the peripherals to be taken.

17.5.5. A diagram should be prepared showing the manner in which the computer and/or the laptop is connected.

17.5.6. If the computer or laptop is in the power-off mode, the same should not be powered on.

17.5.7. If the computer is powered on and the screen is blank, the mouse could be

moved and as and when the image appears on the screen, the photograph of the screen to be taken.

17.5.8. If the computer is powered on, the investigating officer should not power off the computer. As far as possible, the investigating officer to secure the services of a computer forensic examiner to download the data available in the volatile memory i.e., RAM since the said data would be lost on the powering down of the computer or laptop.

17.5.9. If the computer is switched on and connected to a network, the investigating officer to secure the services of a forensic examiner to

capture the volatile net work data like IP address, actual net work connections, net work logs, etc.,

17.5.10. The MAC address also to be identified and secured.

17.5.11. In the unlikely event of the Forensic examiner not being available, then unplug the computer, pack the computer and the wires in separate faraday covers after labeling them.

17.5.12. In case of a laptop if the removal of the power cord does not shut down the laptop to locate and remove the battery.

17.5.13. If the laptop battery cannot be removed, then shut down the laptop and pack it in a faraday bag so as to block any communication to the said

laptop since most of the laptops, nowadays have wireless communication enabled even when the laptop is in the stand by mode.

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

17.6.1. To ascertain as to whether the said equipment is connected to any remote storage devices or shared network drives, if so to seize the remote storage devices as also the shared network devices.

17.6.2. To seize the wireless access points, routers, modems, and any equipment connected to such access points,

routers, modems which may some times be hidden.

17.6.3. To ascertain if any unsecured wireless network can be accessed from the location. If so identify the same and secure the unsecured wireless devices since the accused might have used the said unsecured wireless devices.

17.6.4. To ascertain who is maintaining the network and to identify who is running the network - get all the details relating to the operations of the network and role of the equipment to be seized from such network manager.

17.6.5. To obtain from the network manager, network logs of the machine to be searched and/or seized so as to

ascertain the access made by the said machine of the net work.

17.7. Mobile devices:Mobile devices would mean an include smartphone, mobile phone, tablets GPS units, etc., during the course of seizure of any of the mobile devices, apart from the steps taken in respect of a computer and/or laptop, the following additional steps to be taken:

17.7.1. Prevent the device from communicating to network and/or receiving any wireless communication either through wifi or mobile data by packing the same in a faraday bag.

17.7.2. Keep the device charged throughout, since if the battery drains out, the data available in the volatile memory could

be lost.

17.7.3. Look for slim-slots remove the sim card so as to prevent any access to the mobile network, pack the sim card separately in a faraday bag.

17.7.4. If the device is in power-off mode, the battery could also be removed and kept separately.

17.7.5. If the device is powered on, then put it in an aeroplane mode in android device or airplane mode in a IOS device.

17.8. In all the cases above, the seized equipment should be kept as far as possible in a dust-free environment and temperature controlled.

17.9. While conducting the search, the investigating officer to seize any electronic

storage devices like CD, DVD, Blu-Ray, pen drive, external hard drive, USB thumb drives, solid-state drives etc., located on the premises, label and pack them separately in a faraday bag.

17.10. The computers, storage media, laptop, etc., to be kept away from magnets, radio transmitters, police radios etc., since they could have an adverse impact on the data in the said devices.

17.11. To carry out a search of the premises to obtain instructions manuals, documentation, etc., as also to ascertain if a password is written down somewhere since many a time person owning equipment would have written the password in a bok, writing pad or the like at the said location.

17.12. The entire process and procedure followed to be documented in writing from the time of entry of the investigation/search team into the premises until they exit.

18. **ANSWER TO POINT NO;11:Whether the order dated 14.09.2020 passed by the Trial Court directing the Petitioner to co-operate with the investigating agency ad provide a password to open the smartphone and email account is proper?**

18.1. The trial court in the present case has directed the Petitioner accused to co-operate with the Investigating agency and provide the password, passcode for the smartphone, as also for the e-mail account of the Petitioner, I am of the considered opinion that the examination of a smartphone or an e-mail account is in the nature of a search being carried out, such a search cannot be so

carried out without a search warrant. The trial Court by merely directing the Petitioner to co-operate with the Investigating agency, the Petitioner cannot be forced or constrained to provide such a password, passcode, biometrics etc., for the purpose of opening of the smartphone and or an e-mail account, much less without recording reasons for the same. The process and procedure as discussed and detailed above would have to be followed.

18.2. For all the aforesaid reasons the order dated 14.09.2020 passed by the trial directing the Petitioner to co-operate with the investigating agency ad provide a password to open the smartphone and email account is not proper or legal and is therefore set aside. Liberty is, however, reserved to the prosecution to file

necessary applications, which would be considered by the trial court in accordance with applicable law and discussion above

19. **ANSWER TO POINT NO;12: Whether the order dated 23.09.2020 passed by the Trial Court directing the Petitioner to undergo a polygraph test violates the rights of the Petitioner under Article 20 of the Constitution of India?**

19.1. The Trial Court, by its order dated 29.03.2020, had directed the administration of polygraph test on the Petitioner. This order was passed on an oral request without there being an application filed by the prosecution and no opportunity having been provided to either the Petitioner or his counsel. The Petitioner was also not heard on the same nor was his consent obtained by the trial Court before the order dated 23.09.2020 was

passed.

19.2. Though it is contended by Sri. Veerana Tigadi learned Special prosecutor that the order dated 23.09.2020 only directed administration of a polygraph test and that no polygraph test would have been administered without the consent of the Petitioner; in my considered opinion, no such order could have been passed without having obtained the consent of an accused like the Petitioner.

19.3. In my considered opinion, there is no question of post-decisional hearing or consent, any consent of the accused would have to be obtained by the Court ordering the administration of polygraph test before directing so. The Apex Court in **Selvi's case (supra),** the relevant paragraphs which has

been extracted hereinabovehas categorically held that there cannot be an administration of a compulsive polygraph test which would also mean that no order for administration of polygraph test made without obtaining the consent of the person on whom it is administered.

19.4. Merely because an accused is silent, neither accepts or rejects the administration of polygraph test would also not amount to consent being provided by the accused. Such a consent has to be categorical without any doubt and be made after being informed and made aware of the implication of the polygraph test and effect thereof.

19.5. The Judgment of the Apex Court in **Selvi's case** is categorical and clear about the

aspects of the administration of polygraph test. The details of Law as laid down by the Apex Court in **Selvi's case (supra) would** have to be followed by investigating agency, as also by the trial Court.

19.6. In the present case, the Petitioner having not consented to administration of a polygraph test and in fact having challenged the same, refusing the administration thereof, had categorically indicated that he does not wish to be subjected to a polygraph test, I am of the considered opinion that no polygraph test could be administered on the Petitioner.

19.7. **Hence, I answer the above question by holding that no polygraph test can be administered without obtaining the consent of the person to whom the**

polygraph test is to be administered.

19.8. **An application if any for such polygraph test has to be served on the said person on whom the polygraph test is to be administered, as also on the lawyer of the said person if so appearing. The effect and impact of the polygraph test and any answers given during the conduct of the polygraph test has to be clearly made known to the said person. The consent in writing to be obtained from such person before directing the administration of the polygraph test. Mere silence of the said person would not amount to consent on behalf of such person. If a person were to refuse the administration of polygraph test, no such polygraph test could be administered**

and even if administered, the result of the said test would be void and cannot be considered by a Court of Law.

20. **ANSWER TO POINT NO.:13: Whether the order dated 15.10.2020 passed by the Trial Court dismissing the Recall Application was in accordance with Law?**

20.1. An application was filed by the accused to recall the order dated 23.09.2020 passed by the trial Court directing the petitioner to undergo a polygraph test.

20.2. On account of the answer given to Point No.12 above, I am of the considered opinion that the trial Court ought to have taken into consideration the decision of the Hon'ble Apex Court in **Selvi's case (supra)** and once the trial Court had been informed and/or it was brought to the notice of the trial Court

that on account of the decision of the Hon'ble Apex Court a polygraph test could not be conducted without a consent of the person who has to be subjected to such a test, the trial Court ought to have recalled its order rather than dismissing the same.

21. **ANSWER TO POINT NO.13: What order?**

21.1. In view of the answers to the above question, the petition is partly allowed.

21.2. The order dated 14.09.2020 passed by the trial Court, directing the petitioner to furnish the password, passcode or Biometrics of his mobile phone and e-mail account is set-aside.

21.3. The order dated 23.09.2020 passed by the trial Court, directing the petitioner to undergo a polygraph test is set-aside.

21.4. The order dated 15.10.2020 passed on the recalling application does not survive for consideration.

21.5. Parties to bear their respective costs.

Sd/-
JUDGE

ln