DE JURE NEXUS LAW JOURNAL

Author:

Vishalakshi

Faculty of Law, Banaras Hindu University

1st Year, LL.B. (3 Years).

PROTECTION OF PRIVATE DATA OF ACCUSED FROM THIRD PARTY DURING TRIAL INVESTIGATION: VIRENDRA KHANNA V. STATE OF KARNATAKA & OTS.

OVERVIEW

On March 12, 2021 a single Judge bench of Karnataka High Court in **Virendra Khanna v. State of Karnataka (WP No.11759/2020)**[1] set aside the orders passed by Special court which directed the accused in sandalwood drug case, Virendra Khanna to furnish the password, passcode of his phone, email account and to undergo polygraph test. The Court held, the judgement passed by Special NDPS Court on 14-09-2020, as illegal and abusive process of law. Justice Suraj Govindraj while delivering the judgement held that examination of a smartphone, laptop or email account of an accused is of nature of search and a search warrant is necessary for that purpose. The Court in its judgement has also laid done the procedures for examining the smart phone or email account of the accused and stated that "the trial court, by merely directing the petitioner to cooperate with the investigating agency, cannot constrain him to provide details such as password, passcode, biometrics, etc., for opening the smartphone or an email account, much less without recording the reasons for it". However, Justice Govindraj said that the data retrieved during investigation by the police will not amount to violation of accused's fundamental Right to Privacy under **Article 21** and Protection against self-incrimination under **Article 20(3)** of the Indian Constitution.

Certain guidelines were also laid down by the court for the protection of private data of any accused from the third party and it was held that any private data seized from any electronic gadget by the police cannot be disclosed to any third party without the permission of the concerned court. And if an investigating officer does so, **he should be proceeded against for dereliction of duty or delinquency**, the High Court added.

FACTS AND ISSUES BEFORE THE COURT

In this case two applications were filed by the respondent before NDPS Court. One seeking court's order to direct the petitioner to unlock his mobile phone and to open two of the e-mail accounts belonging to him

which the petitioner has refused to do. And the other, asking for permission to subject the appellant for polygraphy test because he has not given his password and passcode for mobile phone and e-mail accounts as the accused according to the police had been lying about the same during the course of investigation. Both of these applications were immediately allowed by the court but the copy of these applications were not served to the appellant or to the counsel appearing on his behalf and the petitioner was not given chance to be heard and defend the application filed by the police. Since the order of the test was not known to him, the petitioner refused to give consent for the polygraphy test which was passed without his knowledge. Hence, the petitioner challenged this order before High Court.

Now the issues before the court were:

1. Can a court issue order to an accused to furnish his password, passcode or biometrics?
2. Whether the order of the court is violative of Article 21 of the constitution or not?
3. What is the recourse available to the investigating officer in case of refusal by the accused and what are the procedures to be followed by the police to seek access of the digital device for pursuing its investigation?
4. Would the data gathered in such way as stated in the fact proved the guilt of the accused?
5. What role, if any does Article 20(3) plays in the present case and up to what extent?
6. Up to what extent can the contents of digital devices can be explored by the enforcement agencies for investigation purposes?
7. Can the investigating officer share the private information of an accused without his consent?

IMPORTANT PROVISIONS

Article 21: Under this article of the constitution **"No person shall be deprived of his life and personal liberty except according to the procedure established by law"**[2]. This article is one of the fundamental rights of the constitution where the term 'life' includes all those aspects of life which makes man's life meaningful, complete and worth living. Right to Life under article 21 has been interpreted by courts at different instances as something which is more than mere survival or animal existence. And hence for the existence as human beings it is necessary that the privacy should be given to them. Privacy means personal space without any unwanted interference. There are certain things which a person cannot share in the public domain. These confidential and furtive part of a person's life has to be free from invasion and therefore it is his '**right to be left alone**'. The hunger for development and the race of who comes first has made humans unstoppable. Today men have achieved a lot and all because of technology. Decade ago, whatever seemed impossible to common people has been made possible by the scientists working in the field of technology across the globe. Man has reached beyond space and smart devices have been developed which can read and narrate the mind of human beings. 21st century is the era of technology which has proved to be boon and bane simultaneously. Man is so indulged in flourishing the technology to prove himself smarter than the other that he has forgotten the catastrophic effects that follows the positive impact of technology. Today when every person has a smart device in his hand in the form of smart phone, smartwatch, laptop, etc. which keeps a track of all the activities done by the person, for example what is he searching on internet, where is he going, with whom is he talking, his personal photos, confidential passwords, bank account details etc., theft has also taken new form of digital theft of soft data via internet. Physical theft is much more difficult offence to commit as compared to the digital theft as anyone sitting in any corner of the world with a little knowledge of internet can hack any data of a person and use it against him for his own benefit. Considering this, it was so important for the world to come up with different ways and concepts for protecting the personal data of persons residing all over the world. Hence, different countries and organizations brought up the concept of giving protection to the privacy of the person under laws. In India, Right to Privacy has been much discussed topic by the Courts and Hon'ble courts in different cases interpreted the concept as per the need of the hour. It was hence, the need of that hour when the highest court of land in landmark case of Justice **K.S. Puttaswamy v. Union of India**[3] accepted the Right to

privacy as an integral part of Article 21, without which human life cannot be imagined based on current technological reforms and declared it a Fundamental Right.

The scope of Right to Privacy is very wide and one such privacy enshrined under right to privacy is the password or passcode of a person's mobile phone and e-mail account and the biometrics have also been considered under it. And no one has the right to access the data of any person's mobile phone or read his e-mails without his permission. In the current case, where the order was passed to direct the appellant to unlock his mobile phone and the e-mail account which contains his personal information had been challenged on the basis that it is violative of Right to Privacy.

In this regard counsel appearing on behalf of the accused took the reference of **Maneka Gandhi's Case**[4] where the Supreme Court stated that to take away the Right of any person even the accused under Article 21, law must be enacted by the act of Parliament to meet the test of article 21 and it must be just, fair and reasonable and not illusionary. It was further argued that no specific law exists till date that empowers court to give direction with regards to the password and information contained in mobile phone of the accused and in the absence of such law, the order of Special Court is not a substantive law.

Article 20(3): The constitution of India provides immunity against self-incrimination under Article 20(3). This article is based on the principle of **"nemo teneteur prodre accussare seipsum"**, which means no man is obliged to be a witness against himself. And it says **"No person accused of an offence shall be compelled to be a witness against himself"**[5]. In **Gobind Singh v. State of Madhya Pradesh**[6], the apex court ruled that the mental stage of an individual also come under Right to Privacy.

In landmark case of **Selvi v. State of Karnataka**[7], the Supreme Court held that the answers given by the person during these tests are not consciously and voluntarily given and the individual is unable to decide whether or not to answer a question, hence it amounts to 'testimonial compulsion' and amounts to self-incrimination which attracts protection under Article 20(3). The Court held that "these tests are cruel and inhuman treatment which violates the right to privacy of the individual which cannot be permitted by the courts against the will of the individual".

The counsel of petitioner in this regard took reference of **Nandini Sathpathy v/s P.L.Dani**[8] where the apex court thereby protecting the rights of the accused person held that it is right of the accused to remain silent and the accused person cannot be forced to answer any question which he thinks may expose his guilt and so the petitioner has the right to remain silent during police interrogation also and insisting him to give the password of his mobile phone is contrary to the right confirmed by the apex court is above stated case.

Arguments given on behalf of the State were that in order to avail the benefit of this provision, the Petitioner must demonstrate that the disclosure of the password is in the nature of personal testimony and the disclosure of the password would lead to self-incrimination and here neither of the conditions are violative of Petitioner's right under Article 20(3) of the Constitution. Further, the disclosure of password is not in the nature of personal testimony.

Section 161 (2) of Cr.P.C.[9]**:** Section 161 deals with the provisions of 'Examination of Witness by Police' and section 161(2) says "Such person shall be bound to answer truly all questions relating to such case put to him by such officer, other than questions the answers to which would have a tendency to expose him to a criminal charge or to a penalty or forfeiture".

Section 161(2) and Article 20(3) covers the same area and the accused is protected by the right against self-incrimination in the view of requirements of section 161(2).

The State further argued in this case that interpretation of **Section 54-A**[10] of the Code of Criminal Procedure, 1973 a person charged with any offence may be directed by the court to subject himself to identification by any person as the court deems fit and in the present case the passwords is nothing but an 'identification mark' by the service provides hosting his data and hence, is sanctioned by law. Therefore,

the order of trial court does not violate any of his right under Article 20(3) and Article 21 of the Constitution and Section 161(2) of the Code of Criminal Procedure.

COURT'S DECISION

Justice Suraj Govindaraj in the present case stated that documents present on smartphone or available in the e-mail account of the accused would not establish the guilt of the accused and both the prosecution and the defence would be required to prove the said document before the court by other evidence also.

The direction to provide password or biometrics does not amount to testimonial compulsion because there is no oral statement or a written statement being made by the accused and it is only a direction to produce evidence.

The use of data given to the investigating officer is covered under exception craved out in Justice Puttuswamy's case and hence it would not violate the Right to Privacy of the accused. But the disclosure making public or otherwise in the court would be determined by the concerned judge by passing judicial order.

However, no investigating officer in any case has no right to disclose the private data of the accused seized during investigation to any of the third parties and the investigating officer would be liable and should be proceeded against for the dereliction of duty or delinquency, if he is found furnishing any data to any third party. It is his duty and responsibility of safeguarding the information or data which could impinge on the privacy of the person. A prior written permission of the court would be needed for that purpose.

Moving ahead the court first looked into the legal basis on which police could access the digital device for the purpose of investigation. In this regard, it was observed by the court that this legal basis lies in the existing search and seizure regime of Cr.P.C., concluding the regime- which it admitted only applied to a "place"- was also applicable for accessing a digital device. This search and seizure regime is stated in **section 93/94**[11] of the Cr.P.C. and in emergent circumstances they could dispense with this requirement and act under **section 165**[12] of Cr.P.C, while the obligations of the accused in both scenarios would be same i.e., to assist the police in providing access to any lock as provided under **section 100**[13] Cr.P.C.

In this case, the court set aside the order issued by the court asking the accused to furnish the password while directing him to co-operate with the investigating agency. Justice Govindraj stated that "the examination of smartphone or e-mail accounts is of nature of search being carried out" and so it cannot be carried out without a search warrant and the petitioner cannot be forced or constrained to provide such information without recording reasons for the same. The court in this regard cited the procedures to be followed for examining the smartphones, email accounts etc. as under:

- Prosecution would be required to approach the court to seek the search warrant to search the smartphone or email account. After the issuance of search warrant it is up to the provide password, passcode, etc.
- In case accused is not providing the password, the investigating agency could also serve a notice that an adverse inference may be drawn against the accused. Then accused in order to avoid the adverse inference can then furnish the password.
- The court may also direct the service provider or manufacturer to unlock/open the device/email account if in case, the accused of any person has refused to comply with the application made by the prosecution.
- If the manufacturer and the service provider is not facilitating the opening of the smart phone or email account, the court may direct the investigating agency to hack into the smartphone and/or email account.
- The investigating agency would be empowered to engage the services of such persons as may be required to hack into the smartphone and email account and make use of the data available therein,

which would akin to breaking open a lock or door or the premises wen the accused were to refuse to co-operate with the investigating agency.

- If the investigating agency is unable to hack into the device or the email account and during this course, if the data is destroyed the investigating agency would be free to rely upon the notice which was issued to the accused warning him about the adverse inference being drawn.

It was also held that while issuing the warrant the court shall indicate as to what smartphone, equipment or email account is to be searched, the nature of search to be done, place where search has to be done and the role of the same in the crime. The court in this regard also laid down certain guidelines for search of electronic gadgets and email accounts.

The court in this event also set aside the order passed by the trial court on 23.03.2020 directing the accused to undergo polygraphy test. It was held that the said order was passed on oral request without any application being filed by prosecution and no opportunity being provided to the Petitioner. The petitioner was not heard and his consent was also not obtained by the trial court,

Mere silence of the accused does not amount to his consent and if the person were to refuse the administration of polygraph test, no such test could be conducted and if conducted, it would not be considered by the court. And the consent in writing should be obtained from the said person before administration of polygraph test.

CONCLUSION

The crux of the case deals with sharing the personal information of the accused with third party by the investigating officer to which the court held that no such details can be shared by anyone not even before the court for court proceeding without the prior permission of the court. While this decision is likely to be the first case in series of cases in near future where the courts grapple with issues posed to criminal investigations by mobile phones and similar digital devices. Such issues require the courts to consider the wide scope of constitutional protections along with interpreting the existing procedures of Code of Criminal Procedure and Information Technology Act, 2000. In the era of advancing technology, the courts are required to be extra cautious while dealing with constitutional rights of the persons which are meant to equip the individuals to protect themselves against unlawful incursions into enjoyment of one's personal liberty by the state. With the advancement of technology today many countries are extending their existing laws relating to search and seizure regimes from the realm of physical space to that of electronic/digital space. Inclusion of judicial supervision by requiring search warrants to be sought before digital devices can be accessed helps keeps a check on imbalance of power in such situations and also keeps law enforcement activities tailored to the needs of investigation and avoid roving inquiries into personal data.

As noted by High Court, disclosure of data to third party were possible and could constitute a breach but nowhere in its judgement did the court mentioned the remedies to the aggrieved person in this regard. Another High Court in such case has already noted that searches being conducted without following the procedures amount to a breach of the right to privacy

Prima facie the Virendra Khanna case appeared to be an open-and-shut case having the straightforward issue of administering the polygraph test without the consent of the accused. But the high court went beyond to address the underlying legal question which are becoming critical and will be coming to different courts across the country in upcoming future in the relevance to law enforcement needs and ordinary life. The court chose to contribute to the discourse by offering clear answers and framing important guidelines to some crucial question which by far have been left unanswered was a welcome move.

REFERENCES

[1] https://indiankanoon.org/doc/87379349/

[2] https://indiankanoon.org/doc/1199182/

[3] 2017(10) SCC

[4] 1978 AIR 597, 1978 SCR (2) 621

[5] https://indiankanoon.org/doc/366712/

[6] 1975 AIR 1378

[7]2010[10]SCC263

[8] 1978 AIR 1025, 1978 SCR (3) 608

[9]https://indiankanoon.org/doc/447673/

[10]https://devgan.in/crpc/section/54A/#:~:text=Where%20a%20person%20is%20arrested,direct%20the%20person%20so%20arrested

[11] https://devgan.in/crpc/index.php?q=93&a=2; https://devgan.in/crpc/index.php?q=94&a=2

[12] https://devgan.in/crpc/index.php?q=165&a=2

[13]]https://devgan.in/crpc/index.php?q=100&a=2

https://www.livelaw.in/news-updates/action-should-be-taken-against-investigating-officer-who-leaks-private-data-of-accused-:-karnataka-high-court-171147?infinitescroll=1

https://taxguru.in/corporate-law/karnataka-hc-guidelines-search-seizure-electronic-devices.html

https://www.newindianexpress.com/states/karnataka/2021/mar/13/relief-for-virendra-khanna-hc-sets-aside-orders-passed-by-special-court-2275934.html

https://theproofofguilt.blogspot.com/