COMPELLED DECRYPTION AND THE CONSTITUTION: A CRITICAL COMMENT ON VIRENDRA KHANNA V. STATE OF KARNATAKA (2021)

Kamini Yadav*

INTRODUCTION

The Karnataka High Court's decision in Virendra Khanna v State of Karnataka (2021)[1] sits uneasily at the crossroads of constitutional law and digital technology. The judgment is, in many respects, an ambitious one. It attempts to bring order to a largely unsettled area by laying down a detailed procedural framework for the handling of digital evidence. Yet embedded within this apparent progress is a deeper constitutional unease. By permitting the compelled disclosure of smartphone passcodes and biometric access, the Court significantly narrows the scope of the protection against self-incrimination. This raises difficult questions about how Article 20(3) is to operate in an era where personal data is protected by remembered codes and bodily identifiers.

The stakes of this question are far from technical. Modern smartphones are not merely tools of communication; they function as intimate records of everyday life. They store conversations, photographs, financial transactions, health information, location histories, and personal beliefs, often over long periods of time. As the United States Supreme Court recognised in Riley v. California, such devices effectively contain "the sum of an individual 's private life."[2] When courts treat access to this material as analogous to the production of physical evidence, they risk overlooking the qualitative difference between surrendering an object and being compelled to unlock the contents of one's own mind.

It is this conceptual slippage that makes Virendra Khanna's case a particularly troubling one. By characterising passcodes and biometric unlocking as non-testimonial, the High Court departs from the functional understanding of testimonial compulsion laid down in Selvi v. State

*BA LLB (HONS.), SECOND YEAR, NALSAR UNIVERSITY OF LAW, HYDERABAD.
[1] Virendra Khanna v State of Karnataka 2021 SCC OnLine Kar 13598 (Karnataka High Court).
[2] Riley v California 573 US 373 (2014) (Supreme Court of the United States).

of Karnataka,[3] where the Supreme Court emphasised protection against the extraction of cognitive content. At the same time, the judgment engages only superficially with the proportionality framework laid down in K.S. Puttaswamy v. Union of India,[4] despite the profound privacy implications of compelled digital access. Read together, these omissions suggest a retreat to pre-digital categories that sit rather awkwardly with contemporary realities. Of left unexamined, the reasoning in Virendra Khanna's case risks transforming mental compulsion from a constitutional red line into a routine investigative convenience.

FACTS AND PROCEDURAL HISTORY

In September 2020, the Bengaluru police arrested the petitioner, Virendra Khanna, in connection with an investigation under the Narcotic Drugs and Psychotropic Substances Act. His mobile phone and SIM card were seized during the inquiry. Alleging non-cooperation, the police sought judicial authorisation to conduct a polygraph test and to compel the petitioner to disclose passwords and provide biometric access to his device.

The Special Court allowed these requests without hearing the petitioner or his counsel. Aggrieved by this, the petitioner approached the Karnataka High Court and contended that both the polygraph order and any compulsion to disclose passwords or biometrics violated his right against self-incrimination under Article 20(3). The High Court quashed the polygraph order on the ground that such tests require informed consent. However, it is controversially held that an order directing disclosure of passcodes or biometrics does not, by itself, attract the protection guaranteed under Article 20(3). This decision analogised passwords to physical evidence such as fingerprints. Although the specific trial court order was set aside for procedural defects, the High Court laid down detailed standard operating procedures for the handling of digital evidence.

DOCTRINAL BACKGROUND: ARTICLE 20(3) IN A DIGITAL CONTEXT

Article 20(3), under the Indian Constitution, provides that "no person accused of an offence shall be compelled to be a witness against themselves."[5] Indian courts have traditionally distinguished between testimonial evidence, which involves personal knowledge, and physical evidence used for identification. In State of Bombay v. Kathi Kalu Oghad (1961), the Supreme

[3] Selvi v State of Karnataka (2010) 7 SCC 263 (Supreme Court of India).
[4] K.S. Puttaswamy v Union of India (2017) 10 SCC 1 (Supreme Court of India).
[5] Constitution of India 1950, art 20(3).

Court held that fingerprints, handwriting, and voice samples are non-testimonial because they are mechanical in nature and do not convey personal knowledge of facts.[6]

This formal distinction got significantly refined in Selvi v. State of Karnataka (2010). There, the Supreme Court was confronted with investigative techniques that could not be comfortably described as either purely physical or purely testimonial. Narco-analysis, polygraph examinations, and brain-mapping were outwardly procedural tools, but in substance they operated on a very different plane. The Court recognised that these methods worked by prying open the accused's mental processes and drawing out thoughts, memories, and associations that the State did not already possess. It was this intrusion into the inner domain of cognition that rendered them unconstitutional under Article 20(3). What Selvi's case ultimately clarified was not merely the illegality of certain techniques, but a deeper principle: any compelled act that reveals the contents of the mind or communicates personal knowledge is testimonial, regardless of the method employed.[7]

Furthermore, K.S. Puttaswamy v. Union of India (2017) added another layer to this evolving constitutional landscape. It recognised informational privacy as one of the fundamental rights, and the Court acknowledged that control over personal data is integral to individual autonomy. The Court held that any state intrusion into this domain must meet the demands of the proportionality test, including the necessity of the intrusion and the use of the least intrusive means available.[8] Read together, Selvi and Puttaswamy's case calls for a rethinking of older specimen-based doctrines in the newer digital age, where remembered codes and biometric identifiers unlock vast reservoirs of personal information.

DIGITAL EVIDENCE JURISPRUDENCE: INDIAN AND COMPARATIVE PERSPECTIVES

Indian courts have adopted inconsistent approaches to compelled digital access. While some High Courts have emphasised safeguards for phone contents, Virendra Khanna marks a significant step toward permissiveness by treating passcodes as physical evidence. Internationally, courts have approached the issue with greater caution.

[6] State of Bombay v Kathi Kalu Oghad AIR 1961 SC 1808 (Supreme Court of India).
[7] Selvi (n 3).
[8] Puttaswamy (n 4).

In the United States, while Riley v. California recognised the heightened privacy interests in smartphones,[9] lower courts remain divided on the issue of compelled decryption. Many treat passcodes as testimonial unless the State satisfies the doctrine of "foregone conclusion" developed in Fisher v United States,[10] which requires prior knowledge of the existence, possession, and authenticity of specific evidence. Biometric unlocking has been more variably treated, though recent trends increasingly recognise its functional equivalence to passwords when used to access device contents.

European jurisprudence under the European Convention on Human Rights emphasises proportionality and data protection,[11] while the United Kingdom's statutory regime, as outlined in the Regulation of Investigatory Powers Act (RIPA),[12] permits for compelled decryption but has been criticised for eroding the privilege against self-incrimination. The comparative lesson is one of consistent caution, i.e., compelled access must be narrowly tailored, strictly supervised, and treated as an exception.

CRITICAL ANALYSIS: THE DOCTRINAL FAILURE IN VIRENDRA KHANNA

The Karnataka High Court erred when it equated the passwords to physical specimens. Fingerprints and handwriting are mere bodily markers and exist without thought and say nothing on their own. A passcode is very different. It lives only in the mind. Forcing its disclosure compels the accused to part with a remembered secret, using their own knowledge to unlock potentially incriminating material. This kind of mental compulsion is precisely what Article 20(3) was intended to prevent.

The judgment also weakens the right to silence by allowing adverse inferences to be drawn from the non-cooperation of the accused. When silence itself is given evidentiary value, compliance no longer remains voluntary but is coerced through indirect pressure. Article 20(3) guards not only against physical force, but also against subtler forms of compulsion that make the accused an unwilling partner in their own prosecution.

The Court's superficial engagement with Puttaswamy is equally troubling. Although privacy concerns are acknowledged, the judgment stops short of a genuine proportionality analysis.

[9] Riley (n 2).
[10] Fisher v United States 425 US 391 (1976) (Supreme Court of the United States).
[11] European Convention on Human Rights (1950).
[12] Regulation of Investigatory Powers Act 2000 (UK).

The Court does not answer the obvious question, i.e., why should forcing disclosure be the first move when less intrusive investigative tools such as forensic imaging or targeted data requests are readily available? The procedural safeguards it lays down are useful in practice, but they lack a principled insistence that less invasive methods be exhausted first.

BIOMETRICS AND FUNCTIONAL EQUIVALENCE

Biometric access complicates the picture further. A fingerprint or facial scan may initially appear to be no different from other physical identifiers routinely collected by the State. That similarity, however, fades once biometrics are used to unlock a digital device. Then, they no longer serve as simple tools of identification and become gateways to an individual's private digital world. When biometric compulsion is used to gain access to the contents of a device, it operates no differently from forcing the disclosure of the password. Treating such access as "harmless" physical evidence overlooks the true nature of the intrusion and undermines the protection that Article 20(3) intends to provide.

TOWARD A PRINCIPLED FRAMEWORK

Restraint should be the starting point of any approach that claims constitutional fidelity. If there is any compelled disclosure of passcodes or biometric unlocking that grants access to digital content, it should be treated as exceptional and not routine. Moreover, it should come into play only when the State already knows what it is looking for and can show that gentler rotes have genuinely led nowhere. Even then, the access cannot be a free-for-all. The investigation must move in steps; methods that secure evidence without turning the accused into an unwilling collaborator must be exhausted. And where access is finally granted, it must be tightly supervised, with clear boundaries to ensure that what is opened does not become an invitation to rummage.

CONCLUSION

Virendra Khanna v. State of Karnataka highlights the fragility of constitutional protections when old categories are tasked with new technological work. The judgment's mistake is that it treats passwords and biometrics as ordinary physical evidence. In the modern world, the smartphone is a device locked by memory or biology and not just an object seized by the State. It is a portal into a person's thoughts, habits, and private world. This judgment completely misses the importance smartphones hold in today's world. Forcing it open is not a neutral

procedural step now, but a direct engagement with the autonomy that Article 20(3) exists to protect.

The real risk lies in what will follow if this reasoning is left unchecked. Once cognitive and biometric keys become equal to fingerprints, the privilege against self-incrimination would shrink, not through force, but through classification. The accused would no longer be beaten into speaking but would be quietly required to unlock the case against themselves. This move drains Selvi of its functional insight and dulls the rights-conscious edge of Puttaswamy.

Ultimately, compelled digital access must remain rare and carefully justified. It should be preceded by genuine attempts at less intrusive methods. Accessing information has become really easy due to technology, so it is high time for constitutional law to decide whether it will adapt to this ease or resist it. Virendra Khanna ultimately asks a simple but uncomfortable question: In the digital age, does Article 20(3) still protect the mind – or only the body left behind?