



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief– Dr. Muktai Deb Chavan Publisher– Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

DIGITAL EVIDENCE AND FUNDAMENTAL RIGHTS: A CASE COMMENTARY ON ARJUN PANDITRAO KHOTKAR v. KAILASH KUSHANRAO GORANTYAL & ORS. (2020) AND IN RE: GUIDLINES FOR DIGITAL DEVICE SEIZURE (FOUNDATION FOR MEDIA PROFESSIONALS / RAMASWAMY VS UNION OF INDIA)

SIDRA MALIK

ABSTRACT

The increasing reliance on electronic records in legal proceedings has raised significant questions concerning their admissibility, authenticity, preservation, and the protection of fundamental rights. This paper examines the evolving legal framework governing digital evidence in India through the Supreme Court's decision in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal & Ors.* (2020) and the constitutional concerns surrounding the search and seizure of digital devices. The paper analyses the mandatory requirement of certification under Section 65B of the Indian Evidence Act, 1872, particularly in relation to secondary electronic evidence, while distinguishing it from primary electronic evidence produced from the original device. It further considers the constitutional implications of indiscriminate seizure and extraction of data from smartphones, laptops, and other personal digital devices, with particular reference to the right to privacy under Article 21, the protection against self-incrimination under Article 20(3), and professional confidentiality, including journalistic and legal privileges. The paper highlights the need for procedural safeguards such as judicial warrants, generation of hash values, proper seizure documentation, preservation of digital evidence, and restrictions on overly broad searches. It

argues that an effective digital-evidence regime must balance the legitimate investigative needs of law-enforcement agencies with individual constitutional freedoms. The study concludes that technological advancement in criminal investigation must be accompanied by clear procedural safeguards to ensure both evidentiary reliability and the protection of fundamental rights.

1. ARJUN PANDITRAO KHOTKAR v. KAILASH KUSHANRAO GORANTYAL & ORS. (2020)

CASE DETAILS

Court: Supreme Court of India (3-Judge Bench)

Bench: Hon'ble Justices R.F. Nariman, S. Ravindra Bhat, and V. Ramasubramanian

Citation: AIR 2020 SC 4908 / (2020) 7 SCC 1

Primary Subject: Admissibility of Electronic Evidence under Section 65B of the Indian Evidence Act, 1872.

BACKGROUND OF CASE

The case arose out of an election petition challenging the election of Arjun Panditrao Khotkar to the Maharashtra Legislative Assembly. The petitioner relied heavily on video recordings produced by Election Commission cameras to show that nomination papers were submitted past the deadline.

Although the election officers failed to produce the statutory Section 65B certificate verifying the authenticity of the electronic records, the Bombay High Court accepted the video evidence, holding that there was "substantial compliance" with the law. The matter was appealed to the Supreme Court to settle conflicting precedents regarding whether a Section 65B certificate is mandatory.

ISSUE

Is a certificate under Section 65B(4) of the Indian Evidence Act mandatory for admitting secondary evidence of an electronic record, or can oral/secondary evidence substitute for it?

JUDGMENT

Mandatory Requirement: The Supreme Court held that obtaining a certificate under Section 65B(4) is an absolute condition precedent for admitting secondary electronic evidence (e.g., printouts, CDs, hard drive copies).

Primary vs. Secondary distinction: If the original physical device containing the primary data (e.g., the owner bringing the actual laptop or phone to court) is produced directly into the witness box, a Section 65B certificate is not required.

Overruling Precedents: The Court explicitly overruled *Shafhi Mohammed v. State of H.P.* (which had made the certificate optional for parties not in possession of the device) and reaffirmed the strict rule established earlier in *Anvar P.V. v. P.K. Basheer* (2014).

DOCTRINE OF IMPOSSIBILITY (Lex non cogit ad impossibilia): If a party cannot obtain a certificate because a third party refuses to cooperate, they can approach the Court. The Court can use its powers under the Code of Criminal Procedure / Civil Procedure Code to compel the production of the certificate or device.

CRITICAL ANALYSIS

Procedural Clarity: The judgment brought much-needed clarity to trial courts, making it clear that Section 65B is a complete code in itself and cannot be bypassed via oral testimony.

Preservation Directives: Recognizing that digital data is easily lost or overwritten, the Court directed telecom companies and authorities to preserve call records (CDRs) and digital logs for longer durations while trial proceedings are pending.

2. IN RE: GUIDLINES FOR DIGITAL DEVICE SEIZURE (FOUNDATION FOR MEDIA PROFESSIONALS / RAMASWAMY VS UNION OF INDIA)

CASE DETAILS.

Court: Supreme Court of India

Bench: Hon'ble Justices S.K. Kaul and Sudhanshu Dhulia (and connected benches)

Key Parties: Foundation for Media Professionals (FMP) & Ram Ramaswamy v. Union of India

Primary Subject: Constitutional safeguards and guidelines against arbitrary search, seizure, and extraction of personal digital devices by investigative agencies.

BACKGROUND OF CASE

Investigative agencies (such as police forces, ED, and CBI) frequently seize personal laptops, smartphones, and storage drives during raids and arrests. In many instances, devices were confiscated without generating "hash values" (digital fingerprints that prevent tampering), without providing seizure memos, and while demanding passwords from the accused.

Petitions filed by journalists, academics, and civil society groups argued that an individual's digital device is virtually an "extension of the self," containing private, professional, and intimate data far beyond the scope of a standard criminal investigation.

ISSUES

Right to Privacy (Article 21): Indiscriminate search and cloning of personal devices violate the fundamental right to privacy established in *K.S. Puttaswamy v. Union of India*.

Right Against Self-Incrimination (Article 20(3)): Compelling an accused person to reveal device passwords, PINs, or encryption keys threatens their constitutional protection against being forced to witness against themselves.

Press Freedom & Professional Privilege: Blanket device seizures compromise confidential journalistic sources, attorney-client communications, and privileged academic research.

KEY TAKEAWAYS & PROPOSED SAFEGUARD

The Supreme Court urged the Union Government to establish standardized operational guidelines governing digital searches. Key guidelines proposed and under active consideration include:

Prior Judicial Warrant: Requiring agencies to obtain a judicial warrant before seizing a digital device, except in urgent, documented emergency situations.

Hash Value Generation: Creating an immediate cryptographic hash value of seized drives at the site of seizure to guarantee data integrity and prevent post-seizure tampering or planting of evidence.

Cloned Copies & Seizure Memos: Providing a mirror copy/cloned image to the owner so their professional work is not indefinitely halted.

Scope Restriction: Restricting searches only to files directly connected to the alleged crime rather than conducting "fishing expeditions" across personal data.