"C.R."

IN THE HIGH COURT OF KERALA AT ERNAKULAM

PRESENT

THE HONOURABLE MR.JUSTICE C.S.DIAS

THURSDAY, THE 19TH DAY OF FEBRUARY 2026 / 30TH MAGHA, 1947

CRL.MC NO. 8709 OF 2025

PETITIONER/COMPLAINANT:

MR. ANAGH,
AGED 28 YEARS
S/O SUBHAVU KUMAR K AMANAKARA MANA, ROHINI NAGAR,
THIRUVANATH TEMPLE ROAD, AYYANTHOLE PO, THRISSUR,
INDIA., PIN - 680003

BY ADVS.
KUM.GAYATHRI MURALEEDHARAN
SMT.ARCHANA B.
SHRI.AJIN K. KURIAKOSE
SMT.SRUTHILAKSHMI SHAJI

RESPONDENTS/STATE:

1 STATE OF KERALA,
REPRESENTED BY PUBLIC PROSECUTOR, HIGH COURT OF
KERALA, PIN - 682031

2* THE HIGH COURT OF KERALA,
REPRESENTED BY REGISTRAR GENERAL ERNAKULAM.

3** MS. FATHIMA @ GAURI,

***ADDL R2 IS IMPLEADED AS PER ORDER DATED 08/10/25 IN CRL.M.A.2/2025 IN CRL.M.C. 8709/2025.**

****ADDL R3 IS IMPLEADED AS PER ORDER DATED 08/10/25 IN CRL. M.A 4/2025 IN CRL.M.C. 8709/2025.**

BY
SRI.C.S.HRITHWIK, SR.PP.
ADV KUM.S.KRISHNA

THIS CRIMINAL MISC. CASE HAVING COME UP FOR ADMISSION ON 19.02.2026, THE COURT ON THE SAME DAY PASSED THE FOLLOWING:

C.S.DIAS, J. **“C.R.”**

Crl.M.C. No. 8709 of 2025

Dated this the 19th day of February, 2026

O R D E R

The Criminal Miscellaneous Case raises the question of procedural significance: Whether a private complaint can be returned by a Magistrate on the ground that the postal address of the accused has not been furnished?

2. The petitioner filed a complaint before the Court of the Judicial First-Class Magistrate–II, Thrissur, against the 3rd respondent alleging her to have committed the offences under Sections 356(2), 351, 61 and 77 of the Bharatiya Nyaya Sanhitha, 2023 (for brevity, ‘BNS’) and Section 66 of the Information Technology Act, 2000 (for short, ‘IT Act’).

3. The gravamen of the petitioner's case in the complaint is that he is the Joint Secretary of a Non-Governmental Organisation. On 23.06.2025, the 3rd

respondent, through a social media thread, posted false, malicious and defamatory allegations against the petitioner, disseminated defamatory materials through WhatsApp messages to the President of the petitioner's organisation and third parties, inflicting reputational harm and mental agony to the petitioner, and continues to repeatedly post unsubstantiated and malicious comments against the petitioner on Facebook, leading to unknown persons targeting the petitioner online. Although the petitioner issued a legal notice to the 3rd respondent via her WhatsApp, Facebook, and Instagram accounts, the 3rd respondent has not responded; instead, she continues to post sweeping, baseless, and defamatory allegations against the petitioner on social media. As the acts of the 3rd respondent attract the above offences, the petitioner was constrained to file the complaint. However, by Annexure A3 order, the learned Magistrate has returned the complaint on the sole ground that the postal address of the 3rd

respondent has not been furnished. The order returning the complaint is *ex facie* erroneous and unjustifiable.

4. Aggrieved thereby, the petitioner has filed this Criminal Miscellaneous Case, invoking the inherent jurisdiction of this Court, inter alia, contending that neither the Bharatiya Nagarik Suraksha Sanhitha ('BNSS', for short) nor the BNS prescribe the furnishing of the postal address of the accused as a precondition to entertain the complaint. Under Sections 174, 195 and 225 of the BNSS, the learned Magistrate is empowered to issue directions for assisting in tracing the accused's address through telecom operators and social media intermediaries. G.O.(M.S) No.172/2025/Home dated 17.09.2025 permits service of summons through a disclosed electronic communication address. The petitioner is unaware of the postal address of the 3rd respondent, who has committed the offences through social media. Perpetrators who commit offences in cyberspace often operate under pseudonymous or partially

disclosed identities, making it impossible to locate their postal addresses. Insisting for postal address at the threshold would leave the petitioner remediless. Therefore, the learned Magistrate may be directed to accept the complaint on file.

5. Pursuant to the orders of this Court, the Registrar (District Judiciary) has filed a counter affidavit on behalf of the High Court (2nd respondent), *inter alia*, stating that under the provisions of the BNSS and the Kerala Electronic Processes (Issuance, Service and Execution) Rules, 2025, it is permissible to send summons through electronic means such as WhatsApp and Telegram, at the discretion of the Court. The Magistrates insist on disclosure of the accused's postal address, not as a matter of technical rigidity, but with a legitimate objective of ensuring that the process of taking cognizance is meaningful and purposeful, and that the case does not merely remain on paper. If the summons is issued electronically and the accused does not appear,

the Court would find it difficult to take coercive proceedings against such a person. Similarly, if a warrant is issued in such a case, the police will find it difficult to execute the warrant unless their physical presence is known. Another predicament is that, with merely an electronic identifier such as a Facebook URL or an Instagram ID, it may not be possible to properly identify a person. In a criminal case, it is essential to identify the accused. A Facebook account or Instagram ID may not reveal a person's true identity. As in the present case, the accused's name is shown as Fathima alias Gauri in the complaint, but her name on the Facebook page is Fathima. However, if the Magistrate refers the complaint to the police under Section 175(3) of the BNSS, the identity of the accused can be ascertained through investigation. In the Criminal Rules of Practice, there is no rule that the address of the accused is to be furnished in the complaint. The insistence on the postal address is relevant at the second

stage, but it cannot be elevated to a jurisdictional requirement at the first stage, especially when the statute expressly recognises complaints against unknown persons. In practice, Magistrates insist on an address of the accused at the time of filing the complaints to ensure that this statutory requirement is effectively complied with. When a complaint is made against an unknown person, the Magistrate can either examine the complainant and/or witnesses on oath under Section 223 BNSS or direct an inquiry/investigation under Section 225 BNSS. Defamation, cyberbullying, arrest threats, impersonation and similar offences committed on social media or online platforms have increased in the country. At the same time, practical difficulties may arise in the issuance process if no physical address for the accused is available on record. There is a compelling need to evolve and adhere to a structured standard of procedure in such cases. Electronic identifiers– including Digital Profile IP addresses, email IDs, phone

numbers, and other online traces – may constitute the only available means of identifying the accused. Therefore, the Courts must be empowered to issue process on such material, while ensuring that the identity of the accused is subsequently established through lawful investigation, technical assistance, and social providers.

6. I have heard Smt. Gayathri Muraleedharan, the learned counsel for the petitioner, Shri.C.S. Hrithwik, the learned Senior Public Prosecutor and Shri. S. Krishna, the learned counsel appearing for the 2nd respondent.

7. In order to resolve the question at hand, it is apposite to refer to the relevant statutory provisions in the applicable enactments.

8. Section 2(1)(h) of the BNSS, defines a complaint in the following manner:

> "2(1). In this Sanhita, unless the context otherwise requires,- xx xx
> (h) "complaint" means any allegation made orally or in writing to a Magistrate, with a view to his taking action under this Sanhita, that some person, whether known or unknown, has committed an offence, but does not include a police report."
>
> (emphasis given)

9. The above definition is of significance in the above context because a complaint can be filed against a known or an unknown person who has committed an offence. So, if the accused is an unknown person, then there is no question of furnishing his postal address. For example, a complaint can be filed against an identified accused and other unidentified accused persons, as is normally done before a Station House Officer at the nascent stage of registering a crime.

10. Section 2(1)(q) of the BNSS and Section 2(24) of the BNS, define an offence in the following manner:

> “S.2(1)(q) of the BNSS: "'offence' means any act or omission made punishable by any law for the time being in force and includes any act in respect of which a complaint may be made under section 20 of the Cattle Trespass Act, 1871 (1 of 1871)”
>
> “S.2(24) of the BNS: “In this Sanhita, unless the context otherwise requires,--
> (24) "offence".--Except in the Chapters and sections mentioned in sub-clauses (a) and (b), the word "offence" means a thing made punishable by this Sanhita, but—
> (a) in Chapter III and in the following sections, namely, sub-sections (2), (3), (4) and (5) of section 8, sections 9, 49, 50, 52, 54, 55, 56, 57, 58, 59, 60, 61, 119, 120, 123, sub-sections (7) and (8) of section 127, 222, 230, 231, 240, 248, 250, 251, 259, 260, 261, 262, 263, sub-sections (6) and (7) of section 308 and sub-section (2) of section 330, the word "offence" means a thing punishable under this Sanhita, or under any special law or local law; and

> (b) in sub-section (1) of section 189, sections 211, 212, 238, 239, 249, 253 and sub-section (1) of section 329, the word "offence" shall have the same meaning when the act punishable under the special law or local law is punishable under such law with imprisonment for a term of six months or more, whether with or without fine”

11. The above definition focuses on the punishable act or omission. Neither definition requires that the offence be alleged against an identified individual at the threshold stage. The above definitions also expressly recognise complaints against unknown persons.

12. It is also profitable to refer to some of the provisions under CHAPTER VI of the BNSS, which deals with the processes to compel appearance.

> “Section 63: Form of summons.--
> Every summons issued by a Court under this Sanhita shall be,--
>
> (i) in writing, in duplicate, signed by the presiding officer of such Court or by such other officer as the High court may, from time to time, by rule direct, and shall bear the seal of the Court; or
>
> (ii) in an encrypted or any other form of electronic communication and shall bear the image of the seal of the Court or digital signature.
> Section 64: Summons how served.--
> (1) Every summons shall be served by a police officer, or subject to such rules as the State Government may make in this behalf, by an officer of the Court issuing it or other public servant:
>
> Provided that the police station or the registrar in the Court shall maintain a register to enter the address, email address, phone

number and such other details as the State Government may, by rules, provide.

(2) The summons shall, if practicable, be served personally on the person summoned, by delivering or tendering to him one of the duplicates of the summons:

Provided that summons bearing the image of Court's seal may also be served by electronic communication in such form and in such manner, as the State Government may, by rules, provide."

13. The above provisions enable summons to be issued and served by electronic communication.

14. Chapter XVI of the BNSS deals with complaints to Magistrates. It is necessary to refer to Sections 223 and 225, which read as follows:

"S.223: Examination of complainant.-- (1) A Magistrate having jurisdiction while taking cognizance of an offence on complaint shall examine upon oath the complainant and the witnesses present, if any, and the substance of such examination shall be reduced to writing and shall be signed by the complainant and the witnesses, and also by the Magistrate:

Provided that no cognizance of an offence shall be taken by the Magistrate without giving the accused an opportunity of being heard:
Provided further that when the complaint is made in writing, the Magistrate need not examine the complainant and the witnesses--
*** *** *** *** ***
Section 225: Postponement of issue of process.-- (1) Any Magistrate, on receipt of a complaint of an offence of which he is authorised to take cognizance or which has been made over to him under section 212, may, if he thinks fit, and shall, in a case where the accused is residing at a place beyond the area in which he exercises his jurisdiction, postpone the issue of process against the accused, and either inquire into the case himself or direct an

> investigation to be made by a police officer or by such other person as he thinks fit, for the purpose of deciding whether or not there is sufficient ground for proceeding:
>
> Provided that no such direction for investigation shall be made,--
> (a) where it appears to the Magistrate that the offence complained of is triable exclusively by the Court of Session; or
>
> (b) where the complaint has not been made by a Court, unless the complainant and the witnesses present (if any) have been examined on oath under section 223.
>
> (2) In an inquiry under sub-section (1), the Magistrate may, if he thinks fit, take evidence of witnesses on oath:
>
> Provided that if it appears to the Magistrate that the offence complained of is triable exclusively by the Court of Session, he shall call upon the complainant to produce all his witnesses and examine them on oath.
>
> (3) If an investigation under sub-section (1) is made by a person not being a police officer, he shall have for that investigation all the powers conferred by this sanhita on an officer in charge of a police station except the power to arrest without warrant."

15. BNSS does not stipulate any particular format for filing a complaint. Instead, it permits the filing of an oral complaint against an unknown person, which necessarily means that no address need be furnished. Nowhere does it elevate the furnishing of a postal address as a condition precedent for filing a complaint. The above statutory architecture also acknowledges digital communication as a legitimate mode of judicial procedure, and furnishing the

name or postal address of the accused is not a condition precedent to the presentation or acceptance of a complaint on file.

16. Section 223 of the BNSS lays down the procedure for a Magistrate to take cognizance of an offence on a complaint. The first proviso to Section 223(1) mandates that no cognizance shall be taken without giving the accused an opportunity of being heard. Whereas, under the erstwhile Code of Criminal Procedure, the interpretation was that cognizance is taken at any stage where the magistrate has applied their mind to a complaint.

17. The BNSS regime has brought about a radical change in the procedure to be followed for taking cognizance of a complaint.

18. This Court in **Suby Antony v. Susha** [2025 (1) KHC 596], has recognised the transformative procedural shift introduced in the BNSS, by holding thus:

> "7. Indeed, a radical change in procedure is brought about by the proviso to S.223(1) of BNSS. Pertinently, in spite of the proviso to

> S.223(1) making it mandatory to provide an opportunity of hearing to the accused before taking cognisance, S.226 does not reckon the accused's objection at the stage of taking cognisance as a relevant factor for dismissing the complaint. Being guided by the precedents on S.200 and S.202 of the Code and the plain language of the proviso to S.223(1) of the BNSS, this Court is of the opinion that, after the complaint is filed, the Magistrate should first examine the complainant and witnesses on oath and thereafter, if the Magistrate proceeds to take cognisance of the offence/s, opportunity of hearing should be afforded to the accused. xx xx xx"

19. It is here that the importance of Intermediaries comes into play. Under the IT Act, Section 67C deals with preservation and retention of information by intermediaries; Section 69 deals with power to issue directions for interception or monitoring or decryption of any information through any computer resource; Section 69A confers power to issue directions for blocking of public access of any information through any computer resource; and Section 69B gives power to authorize, monitor and collect traffic data or information through any computer resource for cyber security.

20. The above provisions cast a clear statutory obligation on the intermediaries to preserve and retain

information relating to their users and subscribers to facilitate the investigation and prosecution of offences committed through computer resources. Section 67C of the IT Act expressly mandates every intermediary to preserve and retain such information for such duration and in such manner as may be prescribed by the Central Government, thereby creating a positive legal duty to maintain subscriber data, access logs, and other identifying information. The powers conferred under Sections 69, 69A, and 69B of the IT Act recognise the lawful collection, monitoring and access to traffic data and information through computer resources for investigation and cybersecurity purposes. The above provisions demonstrate that the intermediaries are custodians of subscriber-related data and are legally bound to retain and disclose such information when required by law, thereby enabling the identification of offenders operating under anonymous or concealed digital identities. This obligation is reinforced by

the conditional nature of the exemption from liability granted to intermediaries under Section 79 of the IT Act, which is available only as long as the intermediary observes due diligence and complies with lawful directions issued by courts or authorised agencies.

21. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 require intermediaries to observe due diligence and to provide information in their possession or control to lawfully authorised courts or government agencies pursuant to valid orders, thereby recognising their role as custodians of user and subscriber data. In addition to the above, intermediaries, particularly significant social media intermediaries, are mandated to designate nodal contact persons for round-the-clock coordination with law-enforcement agencies, ensuring expeditious access to subscriber information when required for investigation. Under the Unified Licence and directions issued by the

Department of Telecommunications, telecom service providers and internet service providers are required to retain: (a) Subscriber information and Customer Application Forms, including name, address, and identity documents, for the entire duration of the subscriber relationship and typically for at least one year thereafter; (b) Internet Protocol Detail Records and traffic logs, including IP address allocation, session logs, and related metadata, generally for one year; and (c) Location and usage-related records, to the extent generated, for periods prescribed under licence conditions and lawful directions.

22. Under the Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009, retention of traffic data is conceived as incident-specific and direction-based rather than as a general or indefinite obligation. The Rules proceed on the premise that traffic data generated, transmitted, received, or stored in computer resources will

be retained and made available during the subsistence of lawful directions issued by the competent authority under Rule 3 and handled through authorised agencies under Rule 4. Rule 5 and Rule 6 impose duties on intermediaries and persons in charge of computer resources to maintain effective internal controls, as well as the secrecy and confidentiality of such data while it is lawfully held. Rule 8 expressly governs retention and destruction of records. Thus, the Rules recognise temporary, but legally enforceable, retention of traffic data sufficient to support investigations and judicial processes, subject to strict safeguards and eventual destruction.

23. Rule 3(1)(h) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 mandate that intermediaries shall preserve information and associated records for a minimum period of one hundred and eighty days after any content is removed or access to it is disabled, and for a longer period if

required pursuant to a lawful order of a court or a competent authority. This obligation applies to user data, logs, and identifiers that are within the control of the intermediary and is central to post-incident investigation, including identification of anonymous users. These requirements apply irrespective of the gravity of the offence and are not confined to cases involving serious crimes.

24. The Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016 (as amended) further reinforce the obligation to preserve electronic records and associated information for prescribed periods. The Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules governing monitoring and collection of traffic data also contemplate lawful access to metadata, logs, and routing information retained by intermediaries.

25. Collectively, the above rules proceed on the clear legislative assumption that intermediaries must retain subscriber and usage data for a reasonable duration and disclose the same in accordance with law, so that offences committed through anonymous or disguised digital identities do not escape investigation merely due to the initial absence of physical address particulars of the accused.

26. Rule 3(1) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (as amended) directs the intermediaries to observe due diligence and to provide information to lawfully authorised agencies. The Rule, by itself, does not create an unconditional duty to disclose subscriber data in response to a judicial request in all criminal cases. It operates subject to the statutory framework of the IT Act. Rule 4(2) of the said Rules obliges significant social media intermediaries to enable identification of the first originator

of information, only upon an order passed under Section 69 of the IT Act and only in respect of specified categories of offences, namely those relating to the sovereignty and integrity of India, security of the State, friendly relations with foreign States, public order, or offences relating to rape, sexually explicit material, or child sexual abuse.

27. Rule 6 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 permits disclosure of sensitive personal data to government agencies.

28. A problem arises when Intermediaries contend that disclosure in defamation cases, like the one at hand, especially on the basis of a private complaint and without a police investigation or executive authorisation, does not meet the threshold contemplated under the Rule. Though the structural generality may dilute the ability of courts to compel disclosure in cases involving lesser offences, it does not preclude the court from ordering any person to produce

any document under Section 94 of the BNSS. Non-compliance with a direction passed under Section 94 of the BNSS warrants punishment under Section 210 of the BNS. Therefore, the court is not entirely helpless in such circumstances.

29. The Government of Kerala, in consultation with the High Court, has framed the Kerala Electronic Processes (Issuance, Service and Execution) Rules, 2025, which enable private complaints to be filed even when details of the accused and witnesses are not available. Rule 2(1)(b) and (f) specifically define a ‘disclosed electronic communication’ and ‘investigating agency software’, respectively. Rule 3 deals with the requirements of the process through electronic communication. Rule 3(6) postulates that when the disclosed electronic communication address of the required person or organisation is available, such process shall be sent through electronic communication from the Court, which is

in line with Section 64(2) of the BNSS. Similarly, Rule 3(8) stipulates that when the court does not have the disclosed electronic communication address of the required person or organisation, or when it deems fit, the Court may direct that the same be served by a Police Officer or any Officer notified under sub-rule (7) of Rule 3. Rule 5 lays down the duties of the Investigating Officer.

30. In the internet era, offences such as cyberbullying, online impersonation, digital stalking, identity theft, and social media defamation have become rampant and assumed alarming proportions. In offences involving cyberspace, the offenders often operate through fake or anonymous digital identities. Hence, the complainant may possess only electronic identifiers, and the accused's postal address is often unascertainable without technical intervention. In such cases, insisting on disclosure of a postal address at the threshold stage would deny access to justice, render victims remediless, encourage deliberate

anonymity and frustrate criminal law enforcement. However, until regulations or a proper standard operating procedure are promulgated, the criminal justice delivery system cannot remain anchored in procedural formalism unsuited to technological advancements and realities of this digital age. Courts cannot express helplessness for the want of the accused's address to issue process in a private complaint. On the contrary, when a cognizable offence is made out, the Officer In-charge of the police station is empowered to register a crime and proceed against the accused persons, including tracing details of the unknown persons. Ultimately, processual rules are the handmaid of justice. If the law recognises registration of crimes against unknown persons when a cognizable offence is made out, it would be incongruous to insist on the disclosure of a postal address as a jurisdictional prerequisite for private complaints alleging non-cognizable offences. Therefore, merely because the Criminal Rules of Practice do not

contain any provisions for the issuance of summons through electronic communication, the same cannot be a reason to return a complaint for want of a postal address. Going by the present framework under the BNSS, the IT Act and Rules framed thereunder and the Kerala Electronic Processes (Issuance, Service and Execution) Rules, and that the BNSS does not mandate the furnishing of the postal address, it would be too rustic to direct the furnishing of the postal address of the accused to entertain a complaint. To return a complaint solely for want of a postal address is to subordinate substantive justice to procedural rigidity. Courts must interpret procedural laws that further justice in a technologically evolving society. Hence, I am convinced that the order returning the complaint for want of the accused's postal address is *ex facie* erroneous and unsustainable in law. The learned Magistrate ought to have accepted the complaint on file, issued process to the accused through her social media platforms by way of

electronic communication, and followed the procedure discussed above. Thus, I am satisfied that this is a fit case to exercise the inherent powers of this Court under Section 528 of the BNSS.

In the above conspectus, I allow the Crl. M.C. by answering the question that a complaint cannot be returned for the want of a postal address. Accordingly, I set aside the order dated 14.08.2025, and direct the learned Magistrate to accept the complaint on file and issue a process to the 3rd respondent/accused in the disclosed electronic communication address mentioned in the complaint. In the event of the 3rd respondent's failure to respond to the process, steps shall be taken in accordance with the BNSS and the above-referred Rules. Taking into consideration the seriousness of the matter, the Registrar (District Judiciary) is directed to place the matter before the competent authority of this Court to examine whether suitable amendments to the Criminal Rules of Practice are

warranted to deal with complaints against cyber offences. This Court places on record its appreciation for the able assistance rendered by the learned Counsel for the parties and the learned Public Prosecutor.

Sd/-

C.S.DIAS, JUDGE

SRS/dkr

APPENDIX OF CRL.MC NO. 8709 OF 2025

PETITIONER ANNEXURES

Annexure A1	**THE ELECTRONICALLY FILED APPLICATION BEARING NO: E-FILE NO: EF-DCK-2025-0038989 RE-PRESENTED ON 05.08.2025**
Annexure A2	**THE TRUE COPY OF THE RECEIPT OF PAYMENT IN E-FILE NO: EF-DCK-2025-0038989 DATED 05.08.2025**
Annexure A3	**THE TRUE COPY OF THE DEFECTS MARKED DATED 14.08.2025 IN IN E-FILE NO: EF-DCK-2025-0038989 OF JFCM, THRISSUR**
Annexure A4	**THE TRUE COPY OF THE G.O (MS) 172/2025/HOME DATED 17.09.2025.**