2026:KER:21429

IN THE HIGH COURT OF KERALA AT ERNAKULAM

PRESENT

THE HONOURABLE MR. JUSTICE BECHU KURIAN THOMAS

TUESDAY, THE 10TH DAY OF MARCH 2026 / 19TH PHALGUNA, 1947

WP(C) NO. 7090 OF 2026

PETITIONERS:

1 DR. RASHEED AHAMMED P.,
AGED 49 YEARS, S/O. MUHAMED P.,
ASSOCIATE PROFESSOR, KTM COLLEGE,
MALAPPURAM,
RESIDING AT NOOR MAHAL,
MELATTUR P.O.,
MALAPPURAM DISTRICT, PIN - 679326

2 ANIL KUMAR K.M.,
AGED 49 YEARS, S/O G. KUNJUKRISHNAN,
CLERICAL ASSISTANT,
GOVERNMENT SECRETARIAT,
GENERAL ADMINISTRATION,
THIRUVANANTHAPURAM,
RESIDING AT GREENVILLA,
PUTHURAL, VENKADAMBU (PO),
NEYYATINKARA,THIRUVANANTHAPURAM, PIN - 695506

BY ADVS.
SMT.NISHA GEORGE
SRI.GEORGE POONTHOTTAM (SR.)
SRI.A.L.NAVANEETH KRISHNAN
SMT.KAVYA VARMA M. M.

RESPONDENTS:

1 THE STATE OF KERALA,
REPRESENTED BY CHIEF SECRETARY,
GOVERNMENT SECRETARIAT,
THIRUVANANTHAPURAM, PIN - 695001

2 THE DEPARTMENT OF FINANCE,
REPRESENTED BY ITS PRINCIPAL SECRETARY,

2026:KER:21429

GOVERNMENT SECRETARIAT,
THIRUVANANTHAPURAM, PIN - 695001

3 THE DEPARTMENT OF PUBLIC RELATIONS,
REPRESENTED BY ITS SECRETARY,
GOVERNMENT SECRETARIAT,
THIRUVANANTHAPURAM, PIN - 695001

4 DEPARTMENT OF ELECTRONICS & INFORMATION
TECHNOLOGY (IT CELL),
REPRESENTED BY ITS SECRETARY,
GOVERNMENT SECRETARIAT,
THIRUVANANTHAPURAM, PIN - 695001

5 KERALA STATE IT MISSION,
REPRESENTED BY ITS DIRECTOR,
SAANKETHIKA, VRIDAVAN GARDENS,
PATTOM P.O.,
THIRUVANANTHAPURAM, PIN - 695004

6 SRI PINARAYI VIJAYAN,
CHIEF MINISTER OF KERALA,
OFFICE OF THE CHIEF MINISTER,
3RD FLOOR, NORTH BLOCK,
GOVERNMENT SECRETARIAT,
THIRUVANANTHAPURAM, PIN - 695001

BY ADVS.
SHRI.V.MANU, SPL.GOVT. PLEADER

THIS WRIT PETITION (CIVIL) HAVING COME UP FOR ADMISSION ON 10.03.2026, THE COURT ON THE SAME DAY DELIVERED THE FOLLOWING:

2026:KER:21429

"C.R."

BECHU KURIAN THOMAS, J.

W.P.(C) No.7090 of 2026

Dated this the 10th day of March, 2026

JUDGMENT

Privacy of an individual has become an issue of substantial relevance, especially with the advent of information technology and the digital world. In this era of technology, protection of data has also assumed significance. The need to enact a statute is a reflection of the sentiment of all that data protection has to be a priority. Judicial consideration of the issue also prompted the Parliament to finally enact a law, balancing the need to protect data and the need to use the data made available for legitimate purposes of the State. Advent of new legislation however brings with it new challenges, giving rise to issues of seminal importance, as has arisen in the instant case, with allegations of intrusion into the privacy of data provided to the Government.

2. In February 2026, Government employees apart from members of the judiciary, allegedly received messages through WhatsApp messaging application, containing the photograph of the incumbent Chief Minister of the State of Kerala, bearing the title 'Chief Minister's Office' and addressing each recipient by name. The message intimated the enhancement of Dearness Allowance ('DA' for short), the date when the enhanced DA would be received and also mentions about the

reinstatement of Government employees 'House Building Advance' (for short 'HBA'). The message also conveyed that the Government will protect the welfare and rights of every employee and that it will continue in the days to come.

3. Petitioners allege that the bulk messaging campaign from the office of the Chief Minister, primarily targeting the State Government employees, has been carried out after illegally accessing the personal data of those recipients. According to the petitioners, the data provided for intimating the crediting of monthly salary was used, without their consent, on the eve of the legislative assembly elections, as a measure of election campaign, resulting in an intrusion into the right to privacy of the employees of the State. Petitioners allege that the intention is illegal as the data had been accessed and processed to disseminate a political party's perceived achievements. Petitioners assert that the collection of personal mobile numbers is in violation of the right to privacy protected under Article 21 of the Constitution of India. Pointing out grave concerns in the unsolicited nature of messages sent from the Chief Minister's office, petitioners contend that such procurement of personal contact numbers of even the Government employees by the Chief Minister, is illegal and unauthorised. It is also pleaded that messages have been sent not only to Government employees but also to those in the higher judiciary, all of which constitute a direct violation of the right to privacy. Petitioners thus primarily seek for a declaration that procurement of personal data by the Chief Ministers Office and using it for disseminating messages violates Article 21 of the Constitution of India.

4. The State has opposed the writ petition contending that the allegations in the writ petition are based on mere assumptions, without any supporting technical

evidence or documentary proof. According to the respondents, the communication made on behalf of the Chief Minister of Kerala, who is the repository of the constitutional powers as head of the Council of Ministers was in exercise of the executive functions of the State and addressing each employee of the State, regarding the grant of arrears of DA and reinstatement of HBA, which were all budgetary assurances, cannot, by any stretch of imagination, be termed to be political in nature. The respondents further pleaded that, to impute such a communication to be political in nature, is only a wrong perception of the petitioners, without any basis and such a communication by the head of the State to its employees, cannot even remotely be termed as soliciting votes for any election. It was also averred that since the Whatsapp message contained no reference to any political party and had only contained factual administrative data, it cannot be regarded as access to any personal data of the Government employees for any illegal or illegitimate purposes.

5. The respondents further pleaded that the Chief Minister's office does not independently hold or maintain any database of personal data of any of the employees and the communication sent was only a part of the governance of the State, especially when messages were with regard to service benefits provided to the employees. Respondents also pleaded that SPARK is a venture undertaken by the Government to digitise all HR related services and data relating to salary of Government employees and it is not merely an application for processing of salaries, but a comprehensive human resource management platform, intended to address all personnel matters of Government employees, including dissemination

of information and updates relating to such matters, both individually and collectively. Respondents also contended that the role of office of the Chief Minister was limited to facilitating coordination, to ensure that the relevant communication was routed through Kerala State Information Technology Mission (for short 'KSITM'), which provided the technological infrastructure for WhatsApp based messaging services as part of the broader initiative to establish a centralized notification hub for Government communications. It is also stated that in order to improve the communication effectiveness and ensure timely dissemination of important information, the Government utilizes WhatsApp business account and platform developed and operationalised by KSITM, which platform functions more as an interactive and responsive communication channel for various e-governance applications of the State thereby advancing the objectives of good governance. The impugned communication is stated to have been addressed to every employee which has been sent through a Meta business account operated by KSITM which displayed the sender ID set in the name of Chief Minister's office, Kerala. However the messages were sent from the platform of KSITM, which has been registered with Meta as a public and Government service without any access provided to private parties.

6. Sri. George Poonthottam, the learned Senior Counsel instructed by Ms. Kavya Varma, the learned counsel for the petitioners submitted that data mining has been carried out, without any informed consent of persons who parted with their data and that the use has not been for a legitimate purpose. The decision in **Justice K.S. Puttaswamy and Another v. Union of India and Others** [(2017) 10

SCC 1], was relied upon to contend that the three conditions mentioned in the said judgment have not been satisfied and that there is no freehand available for the State to deal as they like, with the data retained by them. It was also submitted that bulk messaging, allegedly done by KSITM, could only have been done with the help of third parties as the infrastructure available with the KSITM do not have the capacity to do so. The learned Senior Counsel also submitted that the KSITM could not have carried the photograph of the Chief Minister as the said office is different from the State and the messages that have been sent lack legal sanction. The learned Senior Counsel submitted that the nature of messages that have been sent does not fall within the function of the Chief Minister and is thereby an unauthorised act, which cannot be given the seal of approval by this Court.

7. Sri. Gopalakrishna Kurup, the learned Advocate General instructed by Sri. Manu, the learned Government Pleader, submitted that there is no transfer of data to the Chief Minister's office and on the other hand it was only the photograph of the Chief Minister that has been used by the KSITM.

8. I have considered the rival submissions.

9. The principles relating to the right to privacy need not be discussed extensively, as they have been elaborately considered in the decision in **Justice K.S. Puttaswamy** (supra). The right to privacy has been recognised an intrinsic part of the right to life and liberty under Article 21 of the Constitution of India. The consequence of such a judicial recognition is the legal imprimatur that without a proper procedure established by law, the said right cannot be intruded upon by any person, including the State or its instrumentalities. The Court had also declared that

the right to privacy is not absolute and that the extent of privacy in public places may differ from that in private space.

10. The Supreme Court had, in **Justice K.S. Puttaswamy** (supra), identified nine different types of privacy, (see paragraph 250 of SCC) which could be regarded as primary in nature. Of the nine, two i.e (iii) and (ix) are relevant which are extracted as follows:

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

11. Notwithstanding the right to privacy being regarded as the core of human personality, with the advent of information technology, communicational privacy and informational privacy have assumed significance. Technology has widened the horizon of the community within which an individual lives. The right to be let alone, can, in an era of information technology, be controlled by silent communications sent to the outside world, consciously or otherwise. There is an invisible shadow that follows or keeps track of everything a person does in the digital world leading to the coinage of the phrase 'ubiquitous dataveillance'. [See paragraph 305 of SCC]. Nevertheless, communicational privacy entitles restriction even on communications received from a third party. The nature of communication, its source and even the consequence of communication are all factors that can affect

the extent of privacy in that regard.

12. Despite the above right available, reasonable restraint on the extent of privacy an individual wields, is necessary, especially when interests of the State are involved. In **Justice K.S. Puttaswamy** (supra), the Supreme Court laid down (in paragraph 310 of SCC) that, when it comes to protecting legitimate State interests, a three-fold requirement must be satisfied. The first is the existence of a law, second, the existence of a need, which embodies a legislative State aim and the third, the means adopted to be proportional to the object. Pursuant to the above observations, a law has been enacted as the Digital Personal Data Protection Act, 2023 (for brevity 'the Act'). However, not all provisions of the said Act have come into force. By a notification published in the Gazette of India dated 13.11.2025, only sections 1(2), section 2, sections 18 to 26, 35, 38 to 43 and section 44(1) and 44(3) alone have come into effect.

13. Section 2 of the Act deals with definitions and some of the relevant definitions are reproduced below:

> *"(h) "data" means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means;*
> *(i) "Data Fiduciary" means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data;*
> *(j) "Data Principal" means the individual to whom the personal data relates and where such individual is— (i) a child, includes the parents or lawful guardian of such a child; (ii) a person with disability, includes her lawful guardian, acting on her behalf;*
> *(k) "Data Processor" means any person who processes personal data on behalf of a Data Fiduciary;*

(n) "digital personal data" means personal data in digital form;

(t) "personal data" means any data about an individual who is identifiable by or in relation to such data;

(u) "personal data breach" means any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data;

(x) "processing" in relation to personal data, means a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction;

14. The above definitions reveal that the data includes any information, while personal data refers to the information about an individual by which he can be identified, which no doubt will include his name and even the personal mobile numbers. Albeit the definition clause having been notified, some of the crucial provisions of the Act, including section 7 will come into effect only after 18 months from the date of notification i.e. by 13.05.2027. Notwithstanding the above, section 7 can give a useful guidance and hence the same, devoid of the illustrations, is extracted as below:

"7. A Data Fiduciary may process personal data of a Data Principal for any of following uses, namely:—

(a) for the specified purpose for which the Data Principal has voluntarily provided her personal data to the Data Fiduciary, and in respect of which she has not indicated to the Data Fiduciary that she does not consent to the use of her personal data.

Illustrations. (Omitted as not relevant)

(b) for the State and any of its instrumentalities to provide or issue to the Data Principal such subsidy, benefit, service, certificate, licence or permit as may be prescribed, where—

(i) she has previously consented to the processing of her personal data by the State or any of its instrumentalities for any subsidy, benefit, service, certificate, licence or permit; or

(ii) such personal data is available in digital form in, or in non-digital form and digitised subsequently from, any database, register, book or other document which is maintained by the State or any of its instrumentalities and is notified by the Central Government,

subject to standards followed for processing being in accordance with the policy issued by the Central Government or any law for the time being in force for governance of personal data.

Illustration. (Omitted as not relevant)

(c) for the performance by the State or any of its instrumentalities of any function under any law for the time being in force in India or in the interest of sovereignty and integrity of India or security of the State;

(d) for fulfilling any obligation under any law for the time being in force in India on any person to disclose any information to the State or any of its instrumentalities, subject to such processing being in accordance with the provisions regarding disclosure of such information in any other law for the time being in force;

(e) for compliance with any judgment or decree or order issued under any law for the time being in force in India, or any judgment or order relating to claims of a contractual or civil nature under any law for the time being in force outside India;

(f) for responding to a medical emergency involving a threat to the life or immediate threat to the health of the Data Principal or any other individual;

(g) for taking measures to provide medical treatment or health services to any individual during an epidemic, outbreak of disease, or any other threat to public health;

(h) for taking measures to ensure safety of, or provide assistance or services to, any individual during any disaster, or any breakdown of public order.

Explanation.—For the purposes of this clause, the expression "disaster" shall have the same meaning as assigned to it in clause (d) of section 2 of the Disaster Management Act, 2005; or

(i) for the purposes of employment or those related to safeguarding the employer from loss or liability, such as prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information or provision of any service or benefit sought by a Data Principal who is an employee." (emphasis supplied)

15. As and when section 7 of the Act comes into force, the State will be able to process personal data of a person, which is available with it, only for the limited purpose for which such data has been given. In other words, after coming into force of section 7 of the Act, if data has been given to the State for a specified purpose, without any restrictive covenant regarding use of such data, still, the data so provided, can be used only for that purpose. In other words, if data has been given to provide or issue a subsidy, benefit, service, certificate, licence or permit, such data can be used only for providing such a service or benefit. The data can also be used for the performance by the State or any of its instrumentalities of any function under any law. It cannot be used for any other purpose.

16. However, as mentioned earlier, section 7 of the Act will come into force only on 18.04.2027, and hence there is a vacuum regarding how and to what extent the data fiduciary may process the personal data of a Data Principal. The aforesaid vacuum, is concededly, filled up by the binding precedent in **Justice K.S. Puttaswamy's** case (supra). Paragraph 311 of the said judgment reads as follows:

"*Apart from national security, the State may have justifiable reasons for the collection and storage of data. In a social welfare State, the Government*

embarks upon programmes which provide benefits to impoverished and marginalised sections of society. There is a vital State interest in ensuring that scarce public resources are not dissipated by the diversion of resources to persons who do not qualify as recipients. Allocation of resources for human development is coupled with a legitimate concern that the utilisation of resources should not be siphoned away for extraneous purposes. Data mining with the object of ensuring that resources are properly deployed to legitimate beneficiaries is a valid ground for the State to insist on the collection of authentic data. But, the data which the State has collected has to be utilised for legitimate purposes of the State and ought not to be utilised unauthorizedly for extraneous purposes. This will ensure that the legitimate concerns of the State are duly safeguarded while, at the same time, protecting privacy concerns. Prevention and investigation of crime and protection of the revenue are among the legitimate aims of the State. Digital platforms are a vital tool of ensuring good governance in a social welfare State. Information technology - legitimately deployed is a powerful enabler in the spread of innovation and knowledge." (emphasis supplied)

17. Thus, if used for legitimate purposes, including for good governance in a social welfare State, the data collected can be utilized without falling within the vice of infringement of the right to privacy of an individual.

18. With the above principles in mind, when the facts as revealed from the pleadings in this writ petition are appreciated, it is discernible that the Whatsapp message assailed herein, though sent in the name of the Chief Minister's Office, actually emanated from an official Whatsapp account registered under KSITM. The State has appointed KSITM as a Nodal Agency for the Department of Information Technology of the Government of Kerala, with the mission to make Kerala a digitally inclusive State, through effective governance framework. The Service and Payroll Administrative Repository for Kerala, otherwise known as 'SPARK' is an e-governance system utilized by the

Government of Kerala for integrated personal, payroll and account information system. SPARK contains the data of all employees and others including those of the members of judiciary to whom salary and other benefits are paid or routed. KSITM has been appointed as the nodal agency for implementation of SPARK and also manages the State Data centre where SPARK data is also stored. The data so stored by KSITM, has been accessed and used for sending the messages. However, there are no materials to assume that the Chief Minister's Office had any access to those data.

19. Since KSITM is a part of the Government of Kerala, and the impugned message was sent through the Whatsapp account registered in the name of KSITM, by using the data in its possession, if the nature of the message was not for any illegitimate purposes, such messaging has to be regarded as irreproachable. Hence the question boils down to whether the data was used for legitimate purposes.

20. The message in Ext.P2 refers to three informational aspects which are (i) in addition to the 3% DA sanctioned with the February salary, an order has been issued sanctioning the remaining 10%, which has enhanced the DA to a total of 35%, (ii). the initially enhanced 3% DA will reach the employees along with the salary payable in March and the presently enhanced DA of 10% will be disbursed along with the salary of April, and (iii) that the House Building Advance has been restored. The message ends with the closing statement that the Government is always with the recipient to protect the welfare and right of its employees and the said care is a promise which will continue in the days to come.

21. It is evident that the nature of the message sent, relates to salary and other perquisites/benefits, which cannot by any stretch of imagination be regarded as a political campaign to impute the message with a colour of illegality or as something done for an illegitimate purpose. The message that has been sent to the employees of the State as well as to persons whose data is kept in SPARK portal, relates to DA and HBA, which are not extrinsic to the services for which their names have been enrolled. The message can hence be regarded as a measure of informing the employees of the Government, the benefits rolled out relating to salary and other perquisites, which can be viewed as a measure of good governance in a social welfare State. Such a step cannot be branded as illegal or for any illegitimate purpose, even if elections are on the anvil.

22. Yet another question that was canvassed with vehemence was whether the identity of the sender of the message shown as ‘Chief Minister’s Office’ is legally proper. Constitutionally, India follows the parliamentary system of Government. Though all executive action of a State, has to be expressed to be taken in the name of the Governor as per Article 166 of the Constitution, still, the Governor has to act on the aid and advice of the Council of Ministers. The Chief Minister is only the head of the Council of Ministers as stipulated in Article 163 and he cannot be attributed with any arbitrary power in the functioning of the Government. In the democratic system of governance under our Constitution, the Chief Minister is not synonymous with the Government. Communications to the public are to be generally made under the identity of the Government and not that of the Chief Minister. In fact, it is evident from Ext. P7, that processes are being set

up for ensuring that all official communications are disseminated using a unified sender identity namely "Government of Kerala". However, since there is no specific pleading or challenge on the above referred question, no finding need be entered into on that aspect, and the said question is left open.

23. As this Court has already held that, there is neither any material to indicate that any data had been transferred to the Chief Minister's Office nor are there any particulars available to conclude that the Chief Minister or his Office had any access to such data, there is no merit in this writ petition. The message sent by KSITM informing details about DA and HBA cannot be regarded as violating the right to privacy of the recipients of those messages.

Hence, this writ petition is dismissed.

Sd/-

BECHU KURIAN THOMAS
JUDGE

vps

Corrigendum dated 11.03.2026

The words "section 7 of the Act will come into force only on 18.04.2027" appearing in paragraph 16 of this judgment shall stand deleted and substituted by the words "section 7 of the Act will come into force only on 13.05.2027".

Sd/-

BECHU KURIAN THOMAS
JUDGE

vps

2026:KER:21429

APPENDIX OF WP(C) NO. 7090 OF 2026

PETITIONER'S/S' EXHIBITS

Exhibit P1	**A TRUE COPY OF THE ORDER DATED 11.02.2026 BEARING G.O.(MS)NO. 4/2026/ITD ISSUED BY THE 4TH RESPONDENT.**
Exhibit P2	**A COPY OF THE SCREENSHOT OF THE MESSAGE RECEIVED TO 1ST PETITIONER DATED NIL.**
Exhibit P2(a)	**A COPY OF THE SCREENSHOT OF MESSAGE RECEIVED TO THE 2ND PETITIONER DATED NIL**
Exhibit P3	**TRUE COPY OF THE SCREEN SHOT OF THE MESSAGE DATED NIL SENT FROM THE OFFICE OF THE CHIEF MINISTER FROM A BUSINESS ACCOUNT.**
Exhibit P4	**TRUE COPY OF THE COMMUNICATION No. 100226/OSD/12 issued by the OSD to Chief Minister DATED NIL.**
Exhibit P5	**TRUE COPY OF THE COMMUNICATION DATED 07.02.2026 ISSUED BY THE OSD TO CHIEF MINISTER.**
Exhibit P6	**A COPY OF THE GOVERNMENT ORDER GO(P)NO.76/2016/ FIN. DATED 27.05.2016.**
Exhibit-P7	**True copy of the said communication No. 100226/OSD/07 dated nil issued by the OSD to Chief Minister.**

RESPONDENT'S/S' EXHIBITS

Exhibit R1(a)	**A true photocopy of the Screenshot of the Whatsapp account titled Chief Minister's Office**
Exhibit R1(b)	**A true copy of G.O.(Ms.) No. 12/2022/ITD dated 07.04.2022**
Exhibit R1(c)	**A true copy of G.O. (Ms) No. 228/2025/ITD dated 29.09.2025**