HIGH COURT OF JUDICATURE FOR RAJASTHAN AT JODHPUR

S.B. Criminal Miscellaneous Bail Application No. 7940/2025

Adnan Haidar Bhai S/o Haidar Bhai, Aged About 22 Years, R/o Flat No 38 Rajiv Nagar 28 Jamnagar Road Bajrang Wadi Rajkot Gujarat. (At Present Lodged In Central Jail Jodhpur)

----Petitioner

Versus

State Of Rajasthan, Through PP

----Respondent

AND

S.B. Criminal Miscellaneous Bail Application No. 7943/2025

Rahul Jagdish Bhai Jadhav S/o Shri Jagdish Bhai, aged about 23 years, resident of Khandiyasar, Kripa 2, Punit Nagar, Jamnagar Road, Rajkot, Gujrat.
(Presently lodged at Central Jail, Jodhpur)

----Petitioner

Versus

State of Rajasthan

----Respondent

For Petitioner(s)	:	Mr. Ram Singh Rawal Mr. Surendra Bagmalani
For Respondent(s)	:	Mr. Rajeev Kumar Sharma- Director General of Police, Mr. Sachin Mittal-Additional Director General (SCRB & Cyber) (presently Commissioner of Police, Jaipur), Mr. Om Prakash- Commissioner of Police, Jodhpur Mr. Deepak Choudhary Additional Advocate General-cum-GA Mr. Nisheeth Dixit- Advocate -Amicus Curiae Mr. Urja Ram Kalbi, PP Mr. Prakash Bishnoi Mr. Mahipal Singh Mr. Shiv Singh for complainant Mr. Pushpendra Singh, RPS-ACP, PS. Cyber Jodhpur

---

Mr. Tej Karan Parihar
Mr. Nitin Dave, SHO, PS Basni
Mr. Barshi Lal, SHO, PS Jhanwar

HON'BLE MR. JUSTICE RAVI CHIRANIA

Order

REPORTABLE

1.	Date of conclusion of arguments	17.10.2025
2.	Date on which the judgment was reserved	17.10.2025
3.	Whether the full judgment or only operative part is announced	Full Order
4.	Date of pronouncement	27.11.2025

1. The instant bail applications have been filed by petitioner Adnan Haidar Bhai S/o Haidar Bhai Aged about 22 years R/o Gujarat & Rahul Jagdish Bhai Jadhav S/o Shri Jagdish Bhai who are presently lodged in the Central Jail, Jodhpur in connection with FIR No. 3/2025 Cyber Police Station, Jodhpur for the offences under Sections 308(2), 308(6), 318(2), 318(4), 319(2), 336(3), 338, 66C, 66D and 61(2) of the BNS. The petitioners were arrested in the impugned FIR and therefore, they moved Criminal Misc. Bail Applications before the learned trial court, which came to be rejected by order impugned date 26.06.2025 and 02.07.2025 passed by Additional Sessions Judge No. 2, Jodhpur.

2. Learned counsels submitted that the petitioners are innocent person and they have not committed any offence as alleged in the impugned FIR bearing No. 3/2025 registered on 14.05.2025. They further submitted that they have not received any amount as mentioned in the FIR and have nothing to do with the facts as stated. It was further stated that the offences as alleged in the impugned FIR are triable by a Judicial Magistrate. In view of the above, they prayed that the petitioners may be enlarged on bail by this Court.

3. Learned Public Prosecutor strongly opposed the bail application on the ground that the present case is of a serious nature as the petitioners extorted money from two elderly persons, namely Prem Mohan Govila and his wife. He further submitted that the petitioners along with two other persons, namely Vikram Goswami and Priya Agarwal impersonated themselves as Sub-Inspectors of Cyber Police, Mumbai and other officials and extorted a total sum of rupees two crores and two lakhs between 30.04.2025 and 08.05.2025. He further submitted that by putting the complainant and his wife, who are **more than 84 years of age**, under illegal arrest **(named as digital arrest but not defined in any Act),** the aforementioned amount was taken from them. He further submitted that as per the impugned orders passed by the learned trial court only two persons have been arrested so far. He further submitted that investigation is at a nascent stage and other persons in the chain are yet to be arrested. In view of this, the petitioners are not entitled to be enlarged on bail by this Court.

4. This Court considering the seriousness of the offences more specifically offences under **Sections 308(2) and 308(6) which are punishable with imprisonment for 7 years, notes that they are serious, though triable by a Magistrate.** Furthermore, cases, of digital arrest, committed by misuse of Information Technology, are growing at a fast pace and modus operandi in all cases is almost same. The Co-ordinate Bench of this Court by order dated 22.08.2025 directed the Investigating Officer of the case to remain present before the Court. On 03.09.2025 the Investigating Officer was present and informed the Court about the investigation conducted by him so far.

Thereafter, this matter was again listed before this Court on 09.10.2025 and this Court directed AAG-cum-GA Mr. Deepak Choudhary to call the Investigating Officer and senior police official holding charge of the Cyber Wing of the Police Commissionerate, Jodhpur. In pursuance to the order dated 09.10.2025, the matter was listed before this Court on 15.10.2025. This Court appointed Advocate Mr. Nisheeth Dixit as Amicus Curiae to assist the Court on the issue of cyber-crime in the State. On 15.10.2025 Additional Director General (ADG) State Crime Record Bureau (SCRB) & Cyber, Mr. Sachin Mittal appeared before this Court through video conferencing and Commissioner of Jodhpur, Mr. Om Prakash IPS; ACP, Police Station Cyber, Jodhpur, Mr. Pushpendra Singh; Mr. Tejkaran Parihar CI Police Station Cyber, Jodhpur and Barshilal SHO along with other IO's of connected cases, present physically.

4.1. This Court interacted with ADG, SCRB & Cyber, Mr. Sachin Mittal who is holding the charge of Director General, SCRB & Cyber Crime in state of Rajasthan. In terms of the order dated 15.10.2025, the matter was again listed before this Court on 17.10.2025 and In continuation of the previous orders, this Court on 17.10.2025 also interacted with Director General of Police, Rajasthan, Mr. Rajeev Kumar Sharma, IPS, through video conferencing. Further, the interaction, was also done with the, Commissioner of Police Jodhpur, Mr. Om Prakash, IPS; AAG-cum-GA Mr. Deepak Choudhary and other SHOs/IOs of the respective police stations, who are also the Investigating Officers of the connected matters. This Court heard the arguments of the

respective counsels as well as officials as mentioned above and the order was reserved on 17.10.2025.

4.2. As far as the facts of this case are concerned, this being a serious case of illegal arrest, commonly termed as digital arrest. The contents of the FIR as lodged by the complainant on 14.05.2025, being relevant, is reproduced as under:

सेवा में,

श्रीमान सहायक पुलिस आयुक्त
साइबर पुलिस थाना
जोधपुर आयुक्तालय।

विषयः– मुकदमा दर्ज करवाने बाबत।

महोदयजी,

उपरोक्त विषयान्तर्गत निवेदन है कि मैं प्रेम मोहन गोविला उम्र 84 निवासी प्लॉट नम्बर 9, मान महल, शेरविलास, एयरफोस ऑफिसर मैस के सामने जोधपुर की अर्ज इस प्रकर है कि दिनांक 29.04.2025 को मोबाईल नम्बर 9863878204 से वॉट्सएप कॉल आया तथा अपने आप का परिचय हेमराज कोहली सबइंस्पेटर, साईबर पुलिस मुम्बई से दिया और बताया कि पंकज अग्रवाल के द्वारा 538 करोड़ का फ्रॉड किया जिसमें 238 बैंक खाते काम में लिये गये है, एक व्यक्ति को हमने गिरफ्तार किया हैं जो आपका नाम ले रहा हैं और बोल रहा हैं कि एक केनरा बैंक का खाता है जो आपका हैं जिसे ठगी से पैसे ट्रांसफर करने के लिये काम में लिया गया है, जिसमें फ्रॉड की राशि आई है उसमें से आपने 10 प्रतिशत कमिशन प्राप्त किया हैं तो सबसे पहले जॉईन्ट खाता होने के कारण आपको और आपकी पत्नी को गिरफ्तार करके मुम्बई लायेंगे फिर आप दोनों से ई.डी. के द्वारा इनवेस्टिगेशन किया जायेगा इस संबंध में प्रिया अग्रवाल इंस्पेटर, पुलिस थाना कोलावा आपके बात करेगी उसके बाद मुझसे प्रिया अग्रवाल से बात करवाई तो उसने बताया कि पंकज अग्रवाल ने 538 करोड़ का घोटाला किया है उसमें आपका केनरा बैंक खाता काम में लिया गया है जिस संबंध में आपसे अनुसंधान किया जायेगा, आपके केस की प्राईमरी इन्वेस्टिगेशन मैं करूंगी तथा मुख्य इन्वेस्टिगेशन सीबीआई के विक्रम गोस्वामी करेंगे जिस पर मेरे द्वारा उनको बताया गया कि मैं 84 साल का हूं और शारीरिक रूप से भी कमजोर हूं तो उन्होंने कहा कि आप बुजुर्ग हो और हमें केस में सपोर्ट कर रहे हो तो ई.डी. और हम आपसे ऑनलाईन इन्वेस्टिगेशन करेंगे, इस तरह से दिनांक 29.04.2025 से आज तक हेमराज कोहली, प्रिया अग्रवाल एवं विक्रम गोस्वामी नाम के लोगों के मेरे पास लगातार वीडिया/ऑडियो आते रहे तथा इन्वेस्टिगेशन एवं गिरफ्तार करने की धमकी दी तथा मुझे डराया धमकाया जिससे मैं डर गया, उनके कहे अनुसार मैंने डर के कारण मेरे सारे बैंक खातों की जानकारी उनको दे दी तो उन्होंने कहा कि आपसे इन्वेस्टिगेशन चल रहा है तब तक आपके बैंक खातों में जितनी भी राशि जमा है उसे निकाल कर हमें भेज दो, अगर आपके द्वारा कोई भी अपराध करना नहीं पाया गया तो आपकी सारी राशि आपके बैंक खातों में हमारे द्वारा वापिस जमा करवा दी जायेगी। मैंने अपने आपको सही साबित करने एवं उनके द्वारा

गिरफ्तार करने की धमकी से डर जाने और इस परेशानी से बचने के लिए व अपने आपको सही साबित करने के लिए मैंने मेरे और मेरी पत्नी के अलग–अलग बैंक के नौ बैंक खातों से उनके द्वारा दिए गए बैंक खातों में करीब 2 करोड़ रूपये भेज दिए, भिजवाई गई राशि का विवरण निम्नानुसार है।

Account No. 090101000009912 Indian Overseas Bank Rs. 1400000 Date 05-05-2025
Account No. 310002010213889 Union Bank of India Rs. 1500000 Date 30-04-2025
Account No. 004152200000266 Yes Bank Rs. 3000000 Date 29-04-2025
Account No. 0712000100263705 PNB Rs. 2800000 Date 30-04-2025
Account No. 5593004569 Central Bank of India Rs 2600000 Date 03-05-2025
Account No. 26001101120001806 Jodhpur Central Corporative Bank Rs 2600000 Date 02-05-2025
Account No. 057010100034724 AXIS BANK Rs 1900000 Date 03-05-2025
Account No. 2213225841492996 AU SMALL FINANCE BANK Rs 2600000 Date 02-05-2025
Account No. 159829425245 INDUSIND BANK Rs 1800000 Date 08-05-2025

जिन बैंक खातों में राशि जमा करवाई गई है उनका विवरण निम्नानुसार है :–
Account No. 10225829904 IFSC CODE IDFB0041359 RS 1400000 DATE 05-05-2025
Account No. 104788700000102 IFSC CODE YESB0001047 RS 1500000 DATE 30-04-2025
Account No. 50200056693601 IFSC CODE HDFC0001885 RS 3000000 DATE 29-04-2025
Account No. 104788700000102 IFSC CODE YESB0001047 RS 2800000 DATE 30-04-2025
Account No. 257874709605 IFSC CODE INDB0001387 RS 2600000 DATE 03-05-2025
Account No. 006563400000674 IFSC CODE YESB0000065 RS 2600000 DATE 02-05-2025
Account No. 257874709305 IFSC CODE INDB00078 RS 1900000 DATE 03-05-2025
Account No. 006563400000674 IFSC CODE YESB0000065 RS 2600000 DATE 02-05-2025
Account No. 20100045968641 IFSC CODE BDBL0001796 RS 1800000 DATE 08-05-2025

अतः निवेदन है कि तक हेमराज कोहली, प्रिया अग्रवाल एवं विक्रम गोस्वामी नाम के फर्जी लोगों के द्वारा मुझे गिरफ्तारी के नाम से डरा धमकाकर संगठित रूप से अपराधियों ने बेईमानी से ठगी करके मेरे 2 करोड़ 2 लाख रूपये अपने विभिन्न बैंक खातों में डलवा लिये जो डिटेल में ऊपर दिए हैं। मेरे द्वारा जितने भी पैसे जमा करवाए गए उनकी भारत सरकार मोहर लगी हुई रसीद उनके द्वारा मुझे भेजी जाती थी वो सभी रसीदें फर्जी बनाई पाई गई, अपराधियों ने भारत सरकार की मोहर लगाकर फर्जी कूटरचित रसीदें तैयार कर उनका प्रयोग कर धोखाधड़ी की है। अपराधियों खिलाफ कानूनी कार्यवाही करते हुए मेरे से ठगी गई राशि मुझे वापिस दिलाने की कृपा करावे।

5. A perusal of the contents of the FIR shows that the complainant Prem Mohan Govila aged about 84 years and his wife were placed

under illegal arrest (**digital arrest**) under the threat that some persons had committed cyber fraud of Rs. 538 crore in which 230 bank accounts were used including the bank account of the complainant and his wife. The contents of the FIR further show that the accused informed the complainant that the alleged illegal/ fraud amount, transferred into their account, due to this the complaint, under fear(as instructed), transferred, through RTGS/NEFT, etc. a total sum of rupees two crores and two lakhs between 30.04.2025 and 08.05.2025 into 9 bank accounts of the petitioners and other person details of which have already been mentioned in the FIR, as reproduced above.

5.1 During the course of arguments, the counsel for the petitioner failed to dispute the fact that the amount was received by them. The Investigating Officer and Pushpendra Singh (RPS) ACP, Cyber, Police Commissionerate, Jodhpur, submitted two reports dated 11.08.2025 and 14.10.2025 to the Court. In the report dated 11.08.2025 it was informed that the complainant, under serious threat of false implication in serious criminal cases, from the petitioners and other persons, **deposited a sum of rupees two crore and two lakh from his nine bank accounts into nine bank accounts of the petitioners and other persons as instructed.** Report further shows that, out of two crores and two lakhs, a sum of **rupees forty-five lakh was deposited by the complainant into the bank account of the present petitioners.** The Investigating Officer supported this fact on the basis of the bank statement as collected by him during the investigation. This shows that the bail applications were filed by

stating false and incorrect facts that the petitioners have been falsely implicated and the petitioners did not receive any amount.

6. After the report dated 11.08.2025, this Court ordered for listing of the bail applications after the order dated 09.10.2025 on 15.10.2025 before which, ACP Pushpendra Singh submitted another report dated 14.10.2025. In the report dated 14.10.2025 the complete **nexus** between the present petitioners Adnan Haidar Bhai, Rahul, Jagdish & Dilkhush Saini was shown on the basis of investigation. On the basis of the two reports dated 11.08.2025 and 14.10.2025, this Court noted that the amount extorted from the complainant and his wife from their nine bank accounts was transferred into nine bank accounts of the above-mentioned persons and other unknown persons. Out of two crores and two lakhs only forty-five lakhs remained in the account of the present petitioners and the rest went into the bank accounts of the other persons which are yet to be traced.

7. Considering overall facts and circumstances of the case, without making any comments on the merits of the present case, this Court is not inclined to enlarge the present applicants on bail.

8. Consequently, S.B. Criminal Miscellaneous Bail Application No. 7940/2025 & 7943/2025 are dismissed.

Why have the cyber crimes become a serious challenge today?

This Court while hearing many bail applications involving cyber crime noted improper/insufficient investigation, lack of knowledge and understand of the investigating machinery of the

State about cyber crime and connected technical issues and the plight of the victims of cyber crimes.

Prior to origin of digital society, life of common man and the system in government and private establishments was moving/working at a usual or snail pace because changes were happening at a normal speed and people and the system were easily able to adjust or race with it. But the speed with which the digital world is moving has put the entire system, including the society, in difficult conditions as they are not able to adjust and move along with it rather they are seriously lagging far behind due to various factors.

The concern of almost all Courts etc. in the country from Hon'ble Supreme Court, All High Courts, All District Courts, all States/ UT’s ,the Police and other Investigating Agencies etc. is how to handle this new, unstoppable and exponentially growing problem which is before them due to fast changing digital technology. The digital world/information technology has seriously affected the following: (i) society and personal life of common man (ii) the economy of the country (iii) law and order (iv) the education system (v) the banking system etc.

Above are some of the segments which are adversely affected. Majorly all the cyber crimes are committed for money or for destroying or damaging the infrastructure, the reputation or restricting the working of the people/system. As far as the cyber crimes, which are committed for money are concerned, the major problem lies with the banking system which has been put into precarious situation by the cyber criminals who are far ahead with the system. This Court, on the basis of the interaction with Amicus

Curiae, Advocate Nisheeth Dixit, ADG Mr. Sachin Mittal & Commissioner of Police Jodhpur Mr. Om Prakash, noted that the Central Government by acting proactively has directed RBI and other banks to take all necessary steps to detect and control cyber crimes. On the basis of the interaction, this Court also noted that the banks, even after taking all necessary steps, are facing the following problems in dealing with digital crimes which are:

(1) Issue of mule account and mule money

(2) Misuse of internet banking by small account holders who are illiterate or have zero digital literacy

(3) bulk posting/transfer of mule money/fraud money in multiple bank accounts

(4) Misuse of ATMs of mule account holders by unauthorized persons

(5) Fast and easy conversion of money received through cyber fraud into digital assets i.e. crypto currency, etc.

(6) Lack of control on daily payments and UPI etc.

If the banks & financial institutions, etc. are able to put complete check on their banking activities in respect of the above issues, then they can control the serious problem of cyber crimes to a large extent. Therefore, necessary directions are required to be issued to Additional Chief Secretary, Home, for issuance of further directions to all the public and private banks, financial institutions, etc. in this regard.

9. This Court was further informed by Amicus Curiae that whenever such amounts are taken by the accused while committing cyber crimes, the amount is immediately transferred to different/multiple accounts through various layers. Initially the

amount is transferred into countable bank accounts as the first layer and thereafter it is further distributed/transferred in hundreds of accounts using digital banking technology and thereafter in third and/or fourth layer it is further either transferred/withdrawn by the other persons. In many cases at the third and forth layer or even thereafter the money is converted into digital currency like bitcoin, ether, binance etc. which is then transferred to foreign nationals outside the country faster than the speed of light. These kinds of transactions, as noted from the two reports and also as informed by Amicus Curiae Adv. Mr. Nisheeth Dixit, are not easily understandable & trackable/traceable by normal police officials & their sub-ordinate officials who are IO's in the cases and they are unable to investigate properly due to a lack of knowledge and understanding of technology and also of the manner and method required for an in-depth investigation and how to arrest the real hidden culprits.

10. The Information Technology Act, 2000 i.e., the cyber law of India, was enacted in the year 2000 and notified on 17.10.2000. Even after more than 25 years, the police machinery in all states is struggling to handle the serious challenges posed by the digital era to the police force and/or Investigating Agencies, which are trained to handle and investigate traditional crimes only. The growing cyber crimes in the country and the world have been taken seriously by the Government of India through the Ministry of Home Affairs and various special wings have been created in this regard. The Ministry of Home Affairs (MHA) has established **I**ndian **C**yber **C**rime **C**oordination **C**entre (hereinafter and commonly referred as **I4C-MHA**). This centre and the MHA work

to freeze and put on hold fraud money collected using digital technology, while committing various cyber & other offences, and to seize virtual digital assets that is crypto currencies, etc. Apart from this, the Government of India has also formed **Financial Intelligence Unit (FIU)**, which also keeps a track on money trail of various financial crimes committed by cyber criminals. Apart from this, the MHA has also provided a toll-free number 1930 through which the victims/complainants can report regarding the cyber crimes in respect of digital financial fraud as committed against them. The concerned agencies controlling and running the 1930 number/facility take steps only to track and block the money as involved in the cyber crimes.

11. Through 1930, MHA, I4C & other connected wings controls all the acts of banks and financial institutions and tries to take speedy action in respect of money as involved in the offences as and when they are reported.

12. Apart from 1930, a general awareness exercise is done by the Government of India, the Reserve Bank of India and other agencies from time to time to create awareness among the citizens about the growing cyber crimes and the precautions that need to be taken while using digital technology not only in commercial space but also in routine life.

13. This Court noted that 1930 is meant only for the purpose of reporting of the financial crimes on time and through the agencies/wings efforts are made to block the money and track the trail, however, that is insufficient & ineffective many a times. The challenges which digital technology has presented not only to the Central Government but also to all State Governments including

the investigating agencies of all levels, Public and Private establishments and the common man in his daily affairs are very serious. This Court was informed by the Amicus Curiae that Government of India and the Ministry of Home Affairs are though working proactively in this regard, however, the complete dependence of the States on the MHA in this regard is not understandable. The speed with which these crimes are committed using digital technology and the time taken to understand and report these offences to the local police/cyber police of the respective area and their consequent reporting to MHA and its agencies loses its significance because of the serious time lag. The total dependence of the States on **I4C** and other agencies of the MHA shows that States and all its agencies are not prepared to handle these offences on their own.

14. In May 2025, MHA initiated a pilot project for automatic conversion of cyber crimes reported/filed at National Crime Record Bureau or 1930 into First Information Report (FIR). A press note in this regard was also issued, as informed to this Court & provided by learned Amicus Curiae, the same is reproduced as under:

> *This is a significant step to achieve Prime Minister Shri Narendra Modi's vision of a Cyber Secure Bharat. Union Home Minister and Minister of Cooperation. Shri Amit Shah had given instructions for implementation of this initiative in a recent review meeting of Indian Cybercrime Coordination Centre (14C) keeping in view the difficulties faced by victims of cyber financial crimes in recovery of the money lost.*
>
> *The National Cybercrime Reporting Portal (NCRP) and the National Cybercrime Helpline 1930 has enabled easy reporting and prompt actioning on complaints related to cyber financial crimes. The newly introduced process involves integration of 14C's NCRP system, Delhi Police's*

e-FIR system and National Crime Record Bureau's (NCRB) Crime and Criminal Tracking Network & Systems (CCTNS).

Now complaints related to financial losses above the threshold limit of 210 lakh made to NCRP and 1930 will automatically lead to registration of a Zero FIR with the e-Crime Police Station of Delhi. This will be immediately routed to the territorial Cybercrime Police Stations. Complainants can visit the cybercrime Police Station within 3 days and get the Zero FIR converted into a regular FIR.

Delhi Police and Indian Cybercrime Coordination Centre (14C), Ministry of Home Affairs (MHA) have worked together to put in place a process for registration of cases in accordance with the new provisions of Section 173 (1) and 1(ii) of Bhartiya Nagrik Suraksha Sanhita (BNSS). This process of issuing FIRs electronically irrespective of territorial jurisdiction (e-Zero FIR) will initially start in Delhi as a pilot. Subsequently it will be extended to other States and UTs. The e-Crime Police Station of Delhi has been notified for the registration of e-FIRs and transferring them to jurisdictional police stations in Cybercrime complaints of a specified nature reported on NCRP.

This initiative will improve the conversion of NCRP/1930 complaints into FIRs enabling easy restoration of money lost by victims and facilitate punitive action against cyber criminals. It leverages the provisions of the recently introduced new criminal laws.

A similar exercise and initiative, as per learned Amicus, requires to be done by the State of Rajasthan also. The conversion of complaints into FIR in the state is negligible.

It is also informed to this Court by the learned Amicus Curiae that a question was raised in the Parliament regarding the establishment of **Regional Cyber Crime Coordination Center** in the State/UTs. In response based to this question the Minister of State, Ministry of Home Affairs in its response in the Parliament dated 21.03.2023 made the following statements **"police and public order are state subject as per the 7th Schedule of the Constitution of India and the State/UTs are primary responsible for prevention, detection, investigation and prosecution of cases related to various crimes including**

cyber crime. The Central Government has set up "Indian Cyber Crime Co-ordination Centre, to deal with all types of cyber crime in the country, in coordinated and comprehensive manner, all States/UTs have also been requested to set up regional cyber crime coordination centre (R4C) at States/UTs in conversions with 'Indian Cyber Crime Co-ordination Centre' (I4C). However, there is no proposal under consideration with the central Government to establish R4C at State/Uts."

In view of the above response, as made in the Parliament by the Minister of State, it is clear that government of India has already requested the States/UT's to set up their regional cyber crime co-ordination center in convergence with I4C. Though this statement was made in the year 2023 and the Parliamentary Committee submitted its report on 20.08.2025, still there is no effort or initiative on the part of the State Government to establish **Regional Cyber Crime Coordination Centre (R4C)**.

15. Every State is required to have its own system in place to monitor, control, investigate and take such other measures so as to control the menace of growing cyber crimes.

Need of Digital Experts and Inspectors to control & investigate cyber crimes in the State

16. Under the IT Act, 2000, the investigation of cyber crimes can be done by Inspector or higher officials in terms of Section 78 of the Act. The traditional police force, in which persons are recruited from arts, commerce and science backgrounds with zero or very little knowledge and hardly any understanding of fast changing

Information Technology, cannot handle the digital challenges even with some part-time/temporary/contractual assistance of technical experts. The problem which the State of Rajasthan is facing is not new. A similar problem was faced by the Government of Punjab, which issued a special recruitment advertisement for appointment of Inspector with IT qualification and experience. This recruitment was initiated for various segments in the TSS Cadre, Punjab Police Department. The various posts as advertised in different domain are reproduced as under for reference:

S. No.	Domain		Specialization/Function
1.	**Information Technology Services (IT)**	**Grouping 1**	Cyber Security
2.			Geographical Information System (GIS)
3.			Data Mining
4.			OSINT Analysis
5.			Network Management
6.		**Grouping 2**	Data Analytics
7.			Wireless & Telecommunications
8.			Website Administration
9.			Computer/ Digital Forensic Analysis
10.		**Grouping 3**	System Administration
11.			Programming/Coding
12.			Database Administration
13.			IT Support
14.			Cyber Crime
15.	**Community & Victim Support and Counselling Services**		Community and Victim Support
16.			Community Counselling
17.	**Forensic Sciences (FS)**		Forensic Analysis
			Computer/Digital Forensic Analysis
18.	**Human Resource Management**		

When such persons are recruited on the post of Inspector only then proper investigation can be conducted, which would further lead to fair trial and be of major help in the administration of justice. As the present Investigating Officers (Inspectors as per Section 78) are not technically qualified, proper investigation is not being conducted by them and consequently the fate of the trial can be well imagined. In order to have the IT experts in the office of the DG Cyber for the investigation of cyber crimes, the

ACS, Home, in consultation with the Department of Personnel, by making necessary amendments in the existing service rules or by framing new recruitment rules, can have persons having IT qualifications with experience of respective domain for the post of Inspector.

17. The State of Rajasthan is one of the states which specifically created the office of Director General, Cyber Crime exclusively for handling the cyber crimes in the year 2024. This approach and effort needs appreciation, however, the speed and the infrastructure with which the office of the DG, SCRB & Cyber is working and intends to proceed is not **understandable** and therefore, even after the creation of the office of DG Cyber, there is no proper system in place to control, investigate cyber crimes and take other measures in the State of Rajasthan. There are many parts in the State namely Mewat etc. which have become hotbeds for the cyber crimes. It was informed to this Court that the State in order to control the growing menace of cyber crimes in certain parts of the State started special operations namely **Operation Anti Virus , Operation Cyber Shield etc.** through which they have tried to control the cyber crimes in those areas to some extent. It was informed to the Court that the State is continuously working in those areas to control cyber crimes. After this order was reserved, this Court, through various news reports as published in the news papers noted that few serious cyber crimes have been caught in the State which shows some serious action on the part of the State. This needs appreciation but catching only can’t help as various technical issues are to be handled as well as to be proved in the trial which is difficult when

the investigation has not been done with the assistance of IT professionals/experts. This court is also aware of the fact that the State is taking some help of the IT Experts however the same is insufficient as there is no regular/permanent team of IT experts in the office of DG Cyber to work 24/7 on such issues.

17.1 Recently the Parliamentary Standing Committee on Home Affairs under the Chairmanship of the then Member of Parliament Dr. Radha Mohan Das Agarwal submitted 254th Report on the subject **"Cyber Crime-Ramifications, Protection and Prevention"** to both the Houses of the Parliament on 20.08.2025. As the digital penetration is growing in all parts/segments/wings of the Government, the private sector, and society, therefore, the Committee took replies, suggestions etc. from the Ministry of Home Affairs, Indian Cyber Crime Coordination Centre (I4C), Ministry of Electronics and Information Technology (MeitY), Ministry of External Affairs (MEA), Ministry of Corporate Affairs (MCA), Department of School Education and Literacy (DoSEL), Telecom Regulatory Authority of India, CBI, NIA, Department of Financial Services, Financial Intelligence Unit-India (FIU-IND), RBI, important nationalized Banks etc.. The above Report was provided to this Court by the learned Amicus Curiae. This Court noted, after going through the Report, the serious concern of Central Government including the Parliament about the growing cyber crimes in the country. The Government and Parliament, both, are seriously concerned in this regard as these crimes have seriously disturbed not only the economy & security of the nation but also the social, economic and cultural fabric of the country. The Report shows that MHA has started a toll free helpline no.

1930 on which people report a large number of financial offences daily as committed against them in digital space. The five year data (2019-2024) as placed before and considered by the Committee shows that the **number of complaints as reported in year 2019 were 26,049 and the conversion into FIR was 1032, this has increased to 20,33,316 complaints and the conversion into FIR is 49,532. This shows that in last five years the number of complaints have grown manifold however the conversion into FIR is very low.**

17.2. The report even shows that for the financial cyber fraud, MHA has created a system known as **Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS),** a platform which facilitate the reporting and management of financial fraud incidents. In 2021 the number of complaints were 1,37,254 which increased to 15,42,254 in the year 2024. On the basis of the complaints as received, the system as put in place by the Central Government, works proactively so as to stop the fraud amount from being transferred further for which the lien is created. **As per the Report, the total fraud amount reported in year 2024 was Rs.21,181 crore however, the lien could be created only on Rs.2530 crore.** The reason, as per the fact informed to this Court by Amicus Curiae, AAG, ADG Mr. Sachin Mittal and other officials is the pace with which the cyber criminals work to transfer the cyber fraud amount using digital technology in banking system is lightning fast and in just few seconds and minutes, hundreds and thousands of crores of rupees are transferred very easily without any proper KYC & other checks about those transactions. This amount will continue to grow

exponentially because in last two decades the country has undergone a remarkable digital transformation & is now moving fast towards adoption of Artificial Intelligence in the system.

The e-Commerce, internet banking, UPI payments, digital literacy, mobile connectivity, digital connectivity, etc. upto the remotest village/part of the country have also grown manifolds. On one hand this digital transformation has provided fast growth to the country, however, the same has been misused by criminals for committing various cyber crimes which is obstructing the growth. The report contains discussions about various crimes, their impact and various bodies and authorities, as instituted, which are working 24/7 to keep a complete check on such crimes, as they have posed a serious danger to not only the economy but also to the lives of the people.

18. The Government of India and the Ministry of Home Affairs for the purpose of controlling the crimes have formed I4C and all the authorities/bodies etc. which work in coordination with I4C in the MHA. India is a country with a population of more than 140 crore and at present is the fourth largest economy of the world, growing at fast pace, in which digital revolution has a key role so the country and each State need specific/separate mechanism and well-equipped system to control cyber crimes. As the economy and population of every state is growing and digital penetration is also increasing every day, so it is necessary that State of Rajasthan must also have a proper system in place to handle this problem.

This court is aware of the fact that even for investigation of traditional crimes, the cooperation and

assistance of technical experts in the IT field is a must, therefore the office of DG, Cyber needs major structural reforms from the level of Inspector to high up in the ladder (under section 78 of the IT Act 2000) and at various other levels also. The cyber crimes can be investigated by officer of the level of Inspector as per Section 78 and above officials. Presently, Sub Inspectors (who are promoted to Inspector) are appointed either through promotion or direct recruitment under the Rajasthan Police Sub-ordinate Rules, 1989. The persons who, through direct recruitment and promotion channel, are appointed as Sub Inspectors are further promoted as Inspector are completely ignorant about the technological challenges and even some trainings and academic courses cannot make them experts and competent to handle the challenges of digital world.

This Court also noted the order dated 21.07.2025 as passed by Division Bench in D.B. Civil Writ (PIL) No. 1311/2025 titled as Suo-Moto Vs. Union of India and Others.

The reason this Court took up the present issue while hearing the present bail applications relating to digital arrest is that present machinery/system in the State under DG SCRB & Cyber is not equipped to handle not only the traditional cyber crimes but also the upcoming serious future challenges of artificial intelligence and deep fake & other such technological challenges. The country and the economy is now moving fast towards adoption of artificial intelligence in the system and to handle/counter the challenges which have started coming due to artificial intelligence and deep fake but the Government and all its departments, wings, etc., at the state level are hardly prepared.

As this Court is issuing certain directions to the State machinery by this order, however, is conscious of the fact that the issue of cyber crime is so vast that all the issues cannot be covered/examined by this Court by this order. The issue of cyber crimes is related to law and order which is the state subject, therefore, the directions would be issued to Additional Chief Secretary, Home, Director General of Police, Director General, SCRB & Cyber for issuance of necessary notifications, circulars, SOPs etc., to handle the issues as discussed in the previous paras.

DIRECTIONS :

This Court, after detailed interaction with the DGP, ADG (Cyber, holding the charge of DG Cyber), Commissioner of Police, Jodhpur, Mr. Deepak Choudhary, Additional Advocate General cum GA, Amicus Curiae Mr. Nisheeth Dixit, Advocate and other IOs, in order to have a proper system and infrastructure in the State for handling the present and future challenges relating to cyber crime, issues following directions: -

DIRECTIONS TO ACS HOME, DGP, DG SCRB & CYBER :

1. ACS Home is directed to issue a notification or circular for the establishment of the **Rajasthan Cyber Crime Control Centre (R4C) on the lines of Indian Cyber Crime Co-ordination Centre (I4C)**, which will work in coordination and co-operation with **I4C** for prevention, detection and investigation etc. of cyber crimes in the State of Rajasthan and for providing all assistance to all the enforcement agencies, Department, etc. of the State of Rajasthan and Central Government agencies.

2. ACS Home would ensure that R4C shall have all the powers in the State similar to I4C and must act in coordination, but not in conflict with the working of I4C. He would also form such wings as may be required, similar to and in addition to as formed by MHA.

3. The State shall start a toll free number (**separate from 1930)** for automatic registration of FIRs on reporting of a complaint which must start from **01.02.2026**. The respective FIR shall be registered on Central Portal, which would then be transferred to the respective Cyber Police Station having jurisdiction.

4. As per Section 78 of the IT Act, 2000, cyber crimes can be investigated by Inspectors and higher officials. As there are no technically qualified, competent and eligible Inspectors in the entire investigative machinery of the State (common problem in all States'/UTs), therefore, ACS Home after consultation with Department of Personnel (DOP) & other Departments, and also after considering and examining all relevant factors/issues shall take steps for appointment of Inspectors exclusively for the office of DG (Cyber) without taking much time in administrative consent / approvals. For this appointment, the State, may refer to the recruitment process followed by the State of Punjab & other State, shall do the following :-

(i) The State, shall appoint IT Inspectors, who must have the IT qualifications required to handle, monitor, detect, prevent, and investigate cyber crimes with required experience of the field/subject/domain.

(ii) Necessary amendments, if required, be made in the existing recruitment Rules or new rules be made to fulfil the need for recruitment of IT Inspectors only for the office of DG, Cyber for investigation of cyber crimes as per the requirement of Section 78 of IT Act, 2000.

(iii) The IT Inspectors so recruited shall be posted only in Cyber Police Station & other departments/places in the entire State under direct control of DG Cyber and their cadre would be designed accordingly keeping the promotion channel & other applicable Rules, etc. while taking into consideration the issue of special/higher pay-scale.

5. The IT Inspectors would not be transferred to any other department except on deputation or until and unless required by other investigation agencies with due permission of ACS, Home and DG, Cyber.

6. Mr. Sachin Mittal, ADG (Cyber), informed this Court, that the required accredited lab as per Section 79(a) of the IT Act, 2000 would be established soon. ACS Home is directed to expedite the process and shall ensure that the required accredited Lab as per Section 79(a) becomes effective from **01.02.2026**.

7. ACS Home shall also ensure, considering the fact that in all criminal cases and in all investigations by different Investigating Authorities/agencies digital evidence and forensic report of the digital device or digital information is very crucial, therefore, the accredited Lab must have all the required latest digital technology and infrastructure including qualified man-power in place so that

all the digital forensic reports are prepared and provided in time to the respective Investigating Officers and/or Investigating Agencies in the most reasonable and shortest possible time not more than 30 days from the date of deposition of devices, etc. or request for information by IOs for the timely completion of investigation and for taking necessary action against the accused persons for proper administration of Justice.

8. ACS Home, DGP and DG Cyber would jointly take quarterly meetings with the all Investigating and Law Enforcement Agencies of the State apart from Banks, Telecom Service Providers, Internet Service Providers & Intermediaries etc., and would issue necessary directions for coordination, so as to prevent, detect, for investigation etc., among them to effectively control cyber crimes in the State and shall also take such steps as required for performance of their duties and functions in this regard.

DIRECTIONS IN RESPECT OF BANKS, FINANCIAL INSTITUTIONS, FINTECH COMPANIES ETCS.:

9. ACS Home and DG, Cyber shall instruct all banks, financial institutions, fintech companies etc., including those companies which maintain/provide ATM facilities, to use AI Tools in ATM software to detect and stop/block the use of multiple ATM cards when it is used by unauthorized person.

10. ACS, Home shall ensure that all nationalised & private banks, fintech companies etc., along with the Authority of RBI in the State, strictly act to control and monitor mule accounts in the State.

11. All banks and financial institutions etc. must use the Mule Hunter (AI) tool as developed by RBI & other AI tools & other softwares, etc. to detect mule accounts and trace mule money.

12. The KYC of all mule accounts detected and suspected one be re-done and be investigated and if Bank officials are found to be involved in opening of such accounts then necessary instructions would be issued by ACS, Home to highest authorities of the banks, etc. to take necessary disciplinary action against them and would also take legal action against them in accordance with BNS & BNSS, 2023 and/or applicable laws.

13. All dead/inactive bank accounts be put under strict vigil and their KYC must be done again. ACS, Home shall instruct all banks, financial institutions, etc. to do physical inspection/verification of such account holders while doing the KYC.

14. All banks, financial institutions, etc. shall be directed by ACS, Home and DG Cyber, to not to permit and/or stop internet banking facilities for account-holders whose activities appear to be suspicious, and/or which have annual transactions of less than Rs.50,000/- per annum in last 3 years and/or who are not digitally literate, in accordance with law. The daily UPI limits be also set for such account holders.

15. The ACS, Home shall ensure that all banks and financial institutions, fintech companies etc., strictly monitor and control bulk transfers/posting of amounts by unknown person/unauthorised and suspicious person etc., **excluding** Central Government, State Government and the authorities controlled by them.

16. The ACS, Home would also issue directions to the top authorities/ Manegement of banks, financial institutions, etc. to strictly monitor the working of their officials, etc. posted in branches in areas with a considerable increase in cyber crimes.

Directions for regulation of sale and purchase of all digital device and SIM cards, Call Centre/BPO etc; social networking sites in the State, etc.:

17. The ACS, Home shall issue directions for the registration of and regulation of the sale and purchase and other connected activities of all companies, shopkeepers etc. (physical shops, offices and shops in digital space) which are engaged in the commercial activity of sale and purchase of original and second-hand devices. The concerned SHO of the area shall carry out this exercise with physical visits to all such companies, shops etc., located in its jurisdiction. This shall come into effect from 01.02.2026.

18. The details of sale and purchase of all digital devices (first-hand, second-hand and even further), must contain all particulars of the device including technical specifications and must be immediately uploaded on the system under the control of DG Cyber. The DG Cyber shall create the system in the form of software for such registration and regulation of connected activities but shall ensure that there is no violation of privacy, any applicable law etc.. Any sale or purchase made, in violation of this requirement or such other condition as may be fixed, must lead to cancellation of their registration and other consequential acts for

which detailed circular would be issued and this shall come into effect from **01.02.2026**.

19. The ACS Home, DG, SCRB & Cyber, in coordination with DOIT, Rajasthan, telecom service providers and other interested /affected /concerned parties (based in the state) shall ensure that no individual person (not a commercial establishment as presently) is issued more than three SIM cards in the State. Before discontinuation of old SIM card and for issuance of any new SIM card (after 3 SIM cards), the necessary check and verification shall be done for which a detailed SOP shall be issued to prevent misuse of SIM cards for prevention of cyber crime.

20. All Call Centre, BPO, etc. involved in any kind of telemarketing, digital communication & for providing any other digital service, etc., operating in the State must be registered with DG, cyber. The ACS, Home shall issue detailed circulars and/or SOP for registration of Call Centres, BPO etc. and shall also take undertakings from them that they shall not indulge in any illegal/prohibited/unauthorized activity. The companies would not be asked to disclose their client details and other confidential business information.

21. The ACS, Home, by a detailed circular, shall ensure that all users of digital/social networking sites who are residents of the State or residing in the State shall have genuine IDs connected with their Aadhar No. or such identity details so as to ensure that no impersonation is done by any person in the State. It shall also be ensured that all fake profiles/IDs are blocked in accordance with law.

22. ACS Home shall issue notification/circular regulating the affairs of all youtubers or other such didgital/internet influencers having their youtube channels, etc. and/or who commercially work in the digital space interests who are either resident of the Sate or residing in the State. In regulating the affairs the due care and caution must be taken with regard to protection of Freedom of Speech and other Fundamental Rights under the Constitution and other laws.

DIRECTIONS IN RESPECT OF E-COMMERCE COMPANIES, COURIER DELIVERY COMPANIES ETC. AND GIG WORKERS: -

23. The State has enacted the Rajasthan Platform-Based Gig Workers (Registration and Welfare) Act, 2023, which was published in the Gazette on 14.09.2023. All gig workers must be registered with DG Cyber and a common uniform/dress with a QR code and ID card for their identification shall be made mandatory **w.e.f. 01.02.2026**. All gig workers shall carry their ID cards while performing their duties and shall produce them as and when demanded by authorities or consumers.

24. All Ola, Uber etc. cars and bike riders and all gig workers of companies like Swiggy, Zomato, etc. must be compulsorily registered with the State Transport Department with commercial number plate. They must also be registered with DG Cyber. Only the person registered with the company/authorised driver shall drive the vehicle while performing the duties; for any impersonation by driver of the vehicle the respective company would be liable for which DG Cyber shall issue detailed SOP in

consultation with Commissioner, State Transport Department, the companies providing services and also after taking public suggestions. This shall be made effective **w.e.f. 01.03.2026.**

25. All E-commerce and other such companies(courier companies, deliver partners of E- commerce companies etc.) shall be directed by ACS, Home to appoint a GIG worker after Police verification and complete background check. The Documentation of police verification shall be submitted/provided to DG Cyber. No person with any criminal antecedents be employed. The above companies shall also conduct monthly thorough checks on all activities of gig workers using AI tools, and must submit a **quarterly report** in respect of any suspicious activity, if noted, to the DGP and DG Cyber Cell, Rajasthan.

26. ACS Home, for the safety of female passengers, who very frequently use the service of above companies for transportation, shall ensure that the companies like Ola, Uber, etc. are encouraged to have at least **15% female drivers (in six months from the date of this order and would further increase to 25% in next 2-3 years) of cars/bike/scooter** for the security of female passengers. The companies shall ensure that on starting this service the female passengers must have the preference, in the software, to opt for female drivers first.

Directions in respect of Government Departments, Authorities, etc. for Digital Audit

27. ACS Home would direct all Government departments, authorities etc., which deals with financial matters to conduct a monthly audit of all the digital transactions & digital activities of

the department so as to detect and stop any financial and other digital fraud in the government/department machinery which involves public money.

SOP FOR DIGITAL ARREST CASE

28. In order to save persons from being victims of digital arrest, ACS Home shall direct all banks, financial institutions, fintech companies etc., to issue a joint SOPs to be followed mandatorily by their officials up to the bottom level to closely monitor sudden high-value transactions by elderly couple or vulnerable account holders etc. **On noticing any sudden high value transaction a physical visit shall be mandatorily made to the house of the account-holder within 48 hours so as to check any suspicious activity or to save them from any cyber fraud.**

29. The ACS, Home shall direct-Banks, financial institutions etc., to identify customers vulnerable to fraud and shall monitor their activities for protection. They would also educate their customers in regard to digital arrest and other cyber crimes on a regular basis.

30. For sudden use of F.D. of high value by vulnerable account holder/senior citizen, due-care and caution would be taken by the banks.

DIRECTIONS TO ACS HOME, DIRECTOR PROSECUTION, GOVERNMENT OF RAJASTHAN

31. ACS, Home & Director Prosecution, State of Rajasthan, in consultation with the Department of Law & Justice (State), shall appoint:-

i. At least one Special Public Prosecutor(SPP) in each district, who has technical and other knowledge including experience to deal the issue of cyber crimes, trials and other issues in the district courts. Further, regular training and other infrastructure shall be provided to such SPP

ii. One Special PP each, for Principal Seat of Rajasthan High Court at Jodhpur and the Bench at Jaipur, shall be appointed to defend the investigating agencies in all matters relating to cyber crimes.

iii. One Cyber Law Consultant in the Office of Director Prosecution, who must have vast understanding of cyber law, cyber crimes and all digital laws in the matters of filing and defending of cases before the appropriate authorities, courts, etc.

Directions for issuance of circular/ SOP for children below 16 years of age for use of mobile phones in school, online games, social networking sites, etc.

32. ACS, home shall issue, in consultation and coordinate with Education Department, all schools, parents association and other stakeholders, detailed circular/SOP regarding the use of smart phones and/or for use of keypad phones in schools for children up to class 9th or below the age of 16 years for safety and protection of children from being the victim of cyber crimes with a period of **four months from the date of order.**

Directions in respect of Data Protection Act, 202 3 and Digital Personal Data Protection Rule, 2025 & other digital laws.

33. ACS, Home and DG Cyber, in coordination with the other departments, shall ensure timely and strict compliance/adherence to Digital Personal Data Protection Act, 2023 and Digital Personal Data Protection Rules, 2025 and other digital laws in the State.

DIRECTIONS FOR AWARENESS

34. The Member Secretary, Rajasthan State, Legal Service Authority may also initiate necessary actions/steps for prevention of cyber crimes by starting awareness drive and creating/establishing **CYBER SECURITY AWARENESS CELL** and may also appoint IT experts, lawyers with knowledge of Cyber Laws for providing legal assistance and information to the litigants up to the District and Taluka level in the State for which the issue be placed before the Hon'ble Executive Chairman and Acting Chief Justice, RSLSA.

35. DG, Cyber shall initiate awareness drive about the cyber crimes in all government departments, colleges, schools and other institutions etc. through which efforts shall be made to prevent and control the number of cyber crimes from increasing in the State.

The above directions are not exhaustive and the ACS, Home and other departments/wings of the State in coordination with each other shall take all such other steps as may be needed for handling the issue of cyber crimes apart from the issue of artificial

intelligence and deep fake for digital safety and security of the State and its residents.

Before closing, this Court appreciates the valuable assistance and information provided by Director General of Police Mr. Rajeev Kumar Sharma, Additional Director General (SCRB & Cyber) Mr. Sachin Mittal (presently Commissioner of Police, Jaipur), Mr. Om Prakash, Commissioner of Police, Jodhpur, Additional Advocate General-cum-GA Mr. Deepak Choudhary and Mr. Nisheeth Dixit- learned Amicus Curiae in examining the present issue and passing the above direction for the object as discussed in this order.

Copy of this order be send to Member Secretary, RSLSA and other parties as mentioned in the title of the order.

(RAVI CHIRANIA),J

7-Jatin/-