NARI GURSAHANI LAW COLLEGE

organises

17th DADA NARI GURSAHANI FEST-

VIDHI MANTHAN

National Level Moot Court Competition

Sponsored by

D. M. HARISH FOUNDATION

MOOT PROPOSITION

I. BACKGROUND AND LEGISLATIVE FRAMEWORK

1. The Republic of Aryavarta is a sovereign, democratic republic governed by a written Constitution. Its constitutional framework guarantees fundamental rights, including the Right to Life and Personal Liberty under Article 21, the Freedom of Speech and Expression under Article 19, and safeguards against self-incrimination, arbitrary arrest and detention under Articles 20 and 22. The constitutional scheme of Aryavarta is substantially analogous to that of the Republic of India.
2. Aryavarta is a State Party to the International Covenant on Civil and Political Rights (ICCPR) and has affirmed its commitment to the principles embodied in the Universal Declaration of Human Rights (UDHR).
3. Over the preceding five years, Aryavarta witnessed a substantial increase in:
    a. cross-border cyber-attacks;
    b. ransomware attacks on critical infrastructure;
    c. coordinated attacks on energy and financial systems;
    d. large-scale digital disinformation campaigns; and
    e. the use of encrypted communication platforms for allegedly coordinated acts of sabotage.
4. The Government of Aryavarta constituted several expert committees to examine the threat posed by emerging technologies, artificial intelligence and encrypted digital communications. The Government subsequently asserted that conventional intelligence-gathering mechanisms were inadequate to address the evolving nature of "hybrid warfare".
5. In response to these concerns, the Parliament of Aryavarta enacted the following legislation.

A. Protection of Critical Infrastructure and Digital Security Act, 2024

6. The Protection of Critical Infrastructure and Digital Security Act, 2024 (PCIDSA) was enacted with the stated objective of protecting critical infrastructure and preventing cyber-enabled threats to national security.
7. Section 12 of the PCIDSA empowers the Central Government to establish the National Digital Surveillance Programme (NDSP) for the detection, prevention and investigation of threats to critical infrastructure and national security.
    a. Pursuant to Section 12, the Government established the NDSP, under which designated State agencies are authorised to employ, inter alia:
    b. Automated Facial Recognition Systems (AFRS) in publicly accessible places;
    c. Deep Packet Inspection (DPI) of specified categories of communications transmitted through public telecommunications networks;
    d. AI-assisted analysis of publicly available and intercepted digital communications; and
    predictive threat-scoring mechanisms for identifying persons, accounts, devices or networks allegedly associated with potential threats.
8. The NDSP provides that information collected under the Programme may be retained, analysed and shared among designated security agencies in accordance with protocols prescribed by the Executive. Oversight of the NDSP is vested in the National Security Oversight Committee (NSOC), an executive body chaired by the Home Secretary and

comprising senior officials from the security, telecommunications and intelligence establishments.

9. Section 12(4) of the PCIDSA provides that prior judicial authorisation shall not be required where the competent authority is satisfied that interception, surveillance or search is necessary in circumstances involving an immediate threat to national security, public order or critical infrastructure.
10. The Act provides for periodic internal review of surveillance activities by the NSOC. However, it does not expressly provide for a requirement of prior judicial warrants in emergency situations or for an independent judicial review before the information collected is operationally used.

B. Preventive Security Act, 2018

11. The Preventive Security Act, 2018 (PSA) was enacted to enable the State to prevent acts considered prejudicial to national security, public order and the security of critical infrastructure.
12. Section 8 of the PSA authorises preventive detention for a period not exceeding twelve months without a formal criminal charge, where the competent authority is satisfied that such detention is necessary to prevent the detainee from acting in a manner prejudicial to State security.
13. Section 14(2) provides that access to legal counsel may, in specified circumstances, be deferred for a period not exceeding ten days, where an officer of the rank of Joint Secretary or above certifies in writing that immediate access to counsel is likely to compromise an ongoing anti-terrorism, national-security or cyber-security investigation.
14. The Government contends that the PSA is preventive and not punitive in character and that detention under the Act does not amount to a determination of criminal guilt.

II. FACTUAL MATRIX

15. Ms. Ayesha Khan is an investigative journalist, founder of *The Digital Sentinel*, a non-profit digital journalism platform, and an active civil-liberties advocate. Over the preceding three years, *The Digital Sentinel* had published several investigative reports concerning government surveillance, data protection, artificial intelligence and the use of predictive policing technologies.
16. In January 2025, Ms. Khan published a series of reports collectively titled "The Algorithmic State." The reports examined the increasing use of artificial intelligence, predictive analytics, biometric identification and automated decision-making by State agencies in matters concerning national security and public order. In the course of her investigative reporting, Ms. Khan had previously published technical material concerning vulnerabilities in the cybersecurity architecture of the Indraprastha Strategic Energy Grid. The material was based substantially upon publicly available documents, regulatory filings and interviews with independent cybersecurity researchers.
17. The Government subsequently contended that certain portions of the reports disclosed technical information that, although publicly accessible, could potentially assist a technically sophisticated actor in identifying vulnerabilities in the Grid. Ms. Khan

maintained that her reports merely exposed deficiencies in the Government's cybersecurity safeguards and did not contain any information obtained through unauthorised access. The Government publicly rejected the allegations and stated that the NDSP did not classify individuals on the basis of political opinion, religion, profession or protected characteristics.

18. On 12 March 2025, the Indraprastha Strategic Energy Grid, one of Aryavarta's critical infrastructure networks, suffered a sophisticated cyber-attack. The attack caused a regional power outage lasting approximately six hours and disrupted several public and private services.
19. On the same day, an anonymous channel operating on an encrypted messaging platform circulated messages calling upon citizens to participate in a coordinated campaign described as "Digital Satyagraha."
20. The messages encouraged citizens to:
    a. temporarily block or overwhelm selected government web portals;
    b. participate in physical demonstrations;
    c. assemble near certain government installations; and
    d. disseminate information concerning alleged governmental surveillance.
21. The Government subsequently alleged that some of the digital activities associated with the campaign were intended to disrupt critical governmental systems. The organisers of the campaign, however, publicly claimed that it was intended to be a non-violent civil-disobedience movement. The identity of the person or organisation responsible for the cyber-attack on the Indraprastha Strategic Energy Grid remained unknown. During its post-attack analysis, the NDSP's automated threat-analysis system identified several metadata similarities between:
    a. communications associated with the anonymous "Digital Satyagraha" channel;
    b. certain IP subnets associated with communications originating from or interacting with the channel; and
    c. digital communications previously published or shared by Ms. Khan.
22. Based upon these correlations, the NDSP assigned Ms. Khan a "Civil Disturbance Threat Vector Score" of 88/100. The system report identified, among other factors, her professional association with investigative journalism, her previous publications concerning the NDSP, her public communications relating to digital rights, and metadata overlaps between certain online communications. During subsequent forensic analysis, investigators identified a communication originating from an encrypted device associated with Ms. Khan's residence that had, approximately three days before the cyber-attack, connected to an IP address later identified by investigators as having been associated with infrastructure used during the attack on the Indraprastha Strategic Energy Grid.
23. The State asserts that this connection constitutes an additional intelligence indicator linking Ms. Khan or persons operating from her residence to the cyber-attack. The Petitioners dispute the inference and contend that the relevant IP address was part of a shared cloud-based infrastructure and could have been accessed by multiple users. No evidence conclusively establishes that Ms. Khan personally initiated or controlled the communication. The forensic report relied upon by the State records that the IP

connection is a "significant intelligence correlation but not, by itself, conclusive evidence of attribution." The report expressly stated that a threat score constituted an intelligence indicator and did not, by itself, establish criminal involvement. The State subsequently relied upon the said IP connection, together with the NDSP threat score and other classified intelligence, in support of the preventive detention order issued against Ms. Khan.

24. The Government nevertheless contended that the cumulative intelligence indicated that Ms. Khan might possess information concerning persons involved in the cyber-attack and might facilitate further disruption of critical infrastructure.

III. THE SEARCH AND DETENTION

25. On 14 March 2025, a special security unit entered and searched Ms. Khan's residence without obtaining a prior judicial warrant. The officers invoked the emergency powers under Section 12 of the PCIDSA, stating that delay in obtaining judicial authorisation could jeopardise an ongoing national-security investigation. During the search, officers seized several electronic devices belonging to Ms. Khan, including:
    a. two smartphones;
    b. three encrypted laptops;
    c. external hard drives; and
    d. digital storage devices.
26. No conventional seizure memo was prepared at the residence. The State subsequently maintained that an electronic inventory was generated on an internal government system.
27. The Petitioners dispute the existence, authenticity and completeness of the electronic inventory and contend that no contemporaneous chain-of-custody record was provided to Ms. Khan.
28. During the search, the officers sought access to Ms. Khan's primary smartphone. Ms. Khan refused to voluntarily provide the device's passcode. The officers thereafter forcibly held Ms. Khan's face before the smartphone's facial-recognition sensor, thereby unlocking the device through its biometric authentication mechanism. Ms. Khan alleges that the officers thereafter accessed encrypted applications and digital material stored on the device.
29. The device subsequently displayed several categories of information, including encrypted messaging applications, photographs, email accounts and documents protected by separate application-level security measures. It remains disputed whether the biometric authentication merely unlocked the device or also constituted authorisation to access all information contained within it.
30. The State contends that no statement or testimonial communication was compelled from Ms. Khan and that biometric authentication merely constituted the collection of physical identifying characteristics, comparable to fingerprints or photographs.
31. The Petitioners contend that, in the circumstances of the present case, biometric unlocking provided the State with access to the contents of a device containing private, confidential and potentially privileged information and therefore constituted compelled testimonial or communicative assistance.
32. On the same day, Ms. Khan was detained under Section 8 of the PSA.

33. The detention order stated that Ms. Khan had:
    a. incited disruption of critical infrastructure;
    b. maintained communications with unidentified actors associated with the "Digital Satyagraha" campaign;
    c. potentially facilitated hostile cyber activity; and
    d. posed a grave threat to national security.
34. The detention order did not allege that Ms. Khan personally executed the cyber-attack on the Indraprastha Strategic Energy Grid. It relied substantially upon classified intelligence reports and the NDSP threat assessment.

IV. EVENTS DURING CUSTODIAL DETENTION

35. Following her detention, Ms. Khan requested immediate access to legal counsel. The Government invoked Section 14(2) of the PSA and issued a written certification deferring access to counsel for ten days.
36. The certification stated that immediate access to counsel could compromise ongoing covert operations intended to identify and apprehend persons allegedly associated with the cyber-attack. During this period, Ms. Khan was subjected to continuous biometric monitoring within the detention facility. Her custodial interactions were also electronically recorded.
37. The Government maintained that such monitoring was necessary to prevent communication with suspected co-conspirators and to protect the integrity of the investigation.
38. The Petitioners contend that the monitoring extended beyond legitimate security requirements and resulted in continuous surveillance of privileged, personal and legally protected communications.
39. No criminal charge was formally framed against Ms. Khan during the initial period of detention. On 24 March 2025, Ms. Khan was permitted her first substantive meeting with legal counsel.

V. PROCEEDINGS BEFORE THE SUPREME COURT

40. On 25 March 2025, a coalition of civil-rights organisations known as the Union for Digital Freedoms, along with Ms. Khan's brother, instituted proceedings directly before the Supreme Court of Aryavarta under Article 32 of the Constitution.
41. The Petitioners filed:
    a. a Public Interest Litigation challenging the constitutional validity of the NDSP framework and relevant provisions of the PCIDSA and PSA; and
    b. a writ petition in the nature of habeas corpus challenging the legality of Ms. Khan's detention.
42. The Petitioners contend that the surveillance framework, the manner in which the search was conducted, the forced biometric unlocking of Ms. Khan's device, the seizure and retention of digital material, the denial of immediate access to counsel and the continued preventive detention cumulatively violate constitutional guarantees.

43. The Petitioners further rely upon India's constitutional jurisprudence on privacy, proportionality, surveillance, free speech, preventive detention, self-incrimination and procedural fairness, as well as the international obligations of Aryavarta under the ICCPR and principles embodied in the UDHR.
44. The State of Aryavarta contests the maintainability of the proceedings and submits that:
    a. the Petitioners have not exhausted available remedies before the High Courts;
    b. the PIL is being used to challenge matters arising from an ongoing national-security investigation;
    c. the Union for Digital Freedoms has no direct personal injury;
    d. digital intelligence and national-security operations fall substantially within the executive domain;
    e. the surveillance measures are authorised by legislation enacted by Parliament;
    f. emergency surveillance without prior judicial warrants is constitutionally permissible in exceptional circumstances;
    g. predictive algorithms are intelligence tools and do not themselves determine guilt;
    h. biometric authentication does not constitute testimonial compulsion;
    i. preventive detention is constitutionally distinct from criminal prosecution; and
    j. the restrictions imposed upon Ms. Khan were necessary and proportionate in view of the alleged cyber-terror threat.
45. The Petitioners, in response, contend that the existence of a national-security justification cannot place executive action beyond constitutional scrutiny and that technological surveillance capable of creating detailed profiles of individuals requires heightened safeguards against abuse.
46. The Petitioners further submit that executive authorisation, executive review and executive secrecy cannot collectively substitute for independent constitutional oversight, particularly where surveillance affects journalists, political dissenters and civil-society actors.
47. The State maintains that judicial intervention at this stage would compromise sensitive intelligence operations and adversely affect national security.