MOOT PROPOSITION

BEFORE THE

HON'BLE HIGH COURT OF AURELIA

(Special Original Jurisdiction)

W.P. No. 1 of 2026

IN THE MATTER OF:

Arjun Mehra & Anr. … Petitioners

Versus

Union of Aurelia & Ors. … Respondents

STATEMENT OF JURISDICTION

The Petitioners invoke the extraordinary writ jurisdiction of this Hon'ble High Court under Articles 226 and 227 of the Constitution of Aurelia *(pari materia with Articles 226 & 227 of the Constitution of India)*, seeking appropriate writs, orders, and directions for enforcement of fundamental rights guaranteed under Part III of the Constitution, and for judicial review of actions taken by investigative authorities under cyber-criminal statutes.

STATEMENT OF FACTS

I. The Parties

1. The Republic of Aurelia is a sovereign democratic nation governed by a written Constitution, whose provisions relating to fundamental rights, criminal law, and digital regulation are pari materia with those of the Republic of Bharat.
2. Petitioner No. 1, *Arjun Mehra*, aged 34 years, is a software architect and co-founder of NeuroLink Dynamics Pvt. Ltd., a technology company engaged in developing AI-driven data analytics solutions for financial institutions.

3. Petitioner No. 2, *NeuroLink Dynamics Pvt. Ltd.*, is a company incorporated under the Companies Act of Aurelia, having its registered office in Helios City, Aurelia. The company acts as a *data processor* and, in limited circumstances, as a *data fiduciary* under the Digital Personal Data Protection Act, 2023 (Aurelia).
4. Respondent No. 1 is the Union of Aurelia, through the Ministry of Home Affairs.
5. Respondent No. 2 is the Cyber Crime Investigation Division (CCID), Helios City.
6. Respondent No. 3 is the Officer-in-Charge, Cyber Police Station, Helios City.

II. Background of the Dispute

1. NeuroLink Dynamics Pvt. Ltd. is engaged in the design and deployment of machine-learning models intended to identify anomalous transaction patterns in high-volume banking systems. The company markets its software as a "non-intrusive, metadata-driven analytical layer", claiming that it does not directly process personally identifiable financial information.
2. In January 2023, NeuroLink entered into a Data Processing and Technology Services Agreement with Aurelia First Bank, a scheduled commercial bank regulated by the Central Bank of Aurelia. Under the agreement, NeuroLink was required to analyse transaction datasets provided by the bank through a secure API environment hosted on third-party cloud infrastructure.
3. The agreement expressly stated that:
    - NeuroLink would not retain raw transaction data beyond processing cycles;
    - all datasets supplied would be pseudonymised by the bank prior to access;
    - NeuroLink would function strictly as a *data processor*, acting on documented instructions of the bank.
4. Over the course of 2023–24, NeuroLink's software was integrated across multiple regional branches of Aurelia First Bank and was credited internally with improving fraud-flagging efficiency.
5. In July 2024, Aurelia First Bank detected a series of unauthorised electronic fund transfers executed over a compressed time window, involving dormant and low-activity customer accounts. Preliminary internal estimates placed the total loss at approximately ₹120 crores, impacting customers across at least five states.

6. On 2 August 2024, the bank lodged a complaint with the Cyber Crime Investigation Division (CCID), alleging that the fraud appeared to involve system-level manipulation rather than isolated credential theft.
7. Based on the complaint, Respondent No. 3 registered an FIR against unknown persons, invoking offences under the Bharatiya Nyaya Sanhita, 2023, the Information Technology Act, 2000, and other allied cyber-crime provisions.
8. At the initial stage, neither NeuroLink nor its directors were named as accused. However, internal CCID notes subsequently recorded that "third-party algorithmic systems used by the bank may have been exploited or compromised".
9. No technical audit report, third-party security assessment, or judicially sanctioned expert review was obtained prior to this inference.

III. Actions of the Investigating Agency

1. On 14 September 2024, a team of officers from the CCID arrived at the registered office of NeuroLink Dynamics Pvt. Ltd. at approximately 9:30 a.m., during regular business hours.
2. The officers informed the staff that they were conducting a "technical inspection" in connection with an ongoing cyber-crime investigation. No written notice, search warrant, or prior intimation was furnished to the company or its directors at that time.
3. Over the course of the day, the investigating officers:
   - directed the shutdown of internal servers;
   - restricted access to employee workstations;
   - prohibited the use of personal electronic devices within the premises.
4. The officers proceeded to seize and image multiple digital assets, including but not limited to:
   - laptops assigned to software engineers,
   - external storage devices,
   - on-premises servers used for testing and deployment,
   - credentials enabling access to cloud-hosted repositories.
5. The imaging process was conducted using forensic tools claimed to be compliant with standard cyber-forensic protocols. However, the Petitioners allege that:
   - no independent witnesses were present during imaging;
   - no contemporaneous hash values were generated or shared;

- employees were not permitted to observe or document the process.

6. During the course of the operation, Petitioner No. 1 was required to remain present at the premises for several hours and was directed to disclose:
   - encryption passphrases,
   - administrator-level system credentials,
   - access tokens for cloud-based development environments.
7. The Petitioners contend that such disclosure was compelled under threat of immediate detention, though no formal arrest was effected on that date.
8. A handwritten inventory of seized items was prepared internally by the officers; however, no signed seizure memo was handed over to the Petitioners at the conclusion of the operation.
9. On 17 September 2024, three days after the search, the Petitioners received an email from CCID attaching:
   - a typed seizure list,
   - a brief intimation that forensic analysis was underway,
   - a direction restraining the Petitioners from accessing or modifying any mirrored systems.
10. In October 2024, the Petitioners were orally informed that forensic examination had revealed "incriminating log patterns" indicating possible data exfiltration linked to NeuroLink's software architecture.
11. Upon repeated requests, the Petitioners were eventually supplied a hash certificate, purporting to reflect SHA-256 values of certain cloned images.
12. The Petitioners thereafter engaged an independent cyber-forensic expert, who, upon limited inspection of the materials provided, opined that:
    - certain hash values did not correspond with system-generated records;
    - metadata timestamps reflected activity subsequent to the date of seizure;
    - documentation evidencing an unbroken chain of custody was absent.
13. Despite these objections being formally communicated to CCID, the investigating agency continued to issue summonses to Petitioner No. 1 under threat of coercive action, while publicly maintaining that the investigation was "at a critical stage".
14. The Petitioners assert that the continuing restraint on access to their systems has paralysed business operations, jeopardised contractual obligations, and exposed them to potential liability under data-protection laws.

IV. Writ Proceedings Before the High Court

1. Aggrieved by:
   - Alleged illegal search and seizure
   - Compelled disclosure of digital credentials
   - Violation of data privacy obligations
   - Threat of coercive criminal action

   the Petitioners approached this Hon'ble High Court by filing the present Criminal Writ Petition.
2. The Respondents justify their actions on grounds of:
   - National economic security
   - Urgency of cyber-crime investigation
   - Statutory powers under IT Act and criminal procedure law
3. The matter is now listed for final adjudication before this Hon'ble High Court.

ISSUES FOR CONSIDERATION

1. Whether the warrantless search, seizure, forensic cloning, and prolonged retention of digital devices and cloud-based repositories of the Petitioners complies with the requirements of "procedure established by law" under Articles 14 and 21 of the Constitution of Aurelia, read with the statutory safeguards governing interception, access, and handling of electronic data under the Information Technology Act, 2000?
2. Whether the failure to adhere to procedural safeguards such as contemporaneous seizure documentation, transparency of grounds, and post-search accountability renders the impugned digital search and seizure arbitrary and unconstitutional, in light of the principles governing misuse of police power as judicially recognized.
3. Whether the compelled disclosure of encryption keys, administrator credentials, and access tokens by Petitioner No. 1 constitutes testimonial compulsion prohibited under Article 20(3), or whether such disclosure is statutorily permissible under the Information Technology Act, 2000 when balanced against constitutional guarantees against self-incrimination?

4. Whether the seizure and mirroring of entire digital ecosystems, including third-party and customer data, without prior judicial authorisation or narrowly tailored scope, violates the doctrine of proportionality and least-intrusive means implicit in Articles 14 and 21 of the Constitution of Aurelia?
5. Whether discrepancies in hash values, metadata timestamps, and gaps in chain of custody vitiate the integrity of electronic evidence under the Information Technology Act, 2000 and established principles of digital forensics, or whether such infirmities merely affect evidentiary weight to be tested at trial?
6. Whether the continued restraint on the Petitioners' access to mirrored systems, in the absence of formal accusation, disproportionately interferes with their fundamental right to carry on trade and business under Article 19(1)(g), particularly when such restraint exposes the Petitioners to statutory liability as data processors under the Digital Personal Data Protection Act, 2023?
7. Whether investigative actions that result in uncontrolled access to personal data of third parties, without demonstrable necessity or safeguards, are violative of the Petitioners' obligations and the data principals' rights under the Digital Personal Data Protection Act, 2023, and if so, whether such statutory non-compliance attracts constitutional scrutiny?
8. Whether the initiation and continuation of coercive criminal process against the Petitioners, solely on the basis of inferred "algorithmic vulnerability" or speculative system-level compromise, satisfies the statutory threshold of "reasonable suspicion" under cyber-crime laws and the constitutional mandate of non-arbitrariness under Article 14?
9. Whether considerations of national economic security and urgency in cyber-crime investigation constitute a valid statutory exception under the IT Act and the Digital Personal Data Protection Act, 2023 to dilute procedural safeguards, or whether such considerations must remain subject to constitutional limitations and judicial oversight?
10. Whether this Hon'ble High Court, while exercising writ jurisdiction under Articles 226 and 227, is duty-bound to intervene where statutory and constitutional safeguards governing digital investigation are demonstrably diluted, or whether judicial restraint must prevail to avoid trenching upon investigative autonomy?

NOTE TO PARTICIPANTS

1. The laws of the Republic of Aurelia are pari materia with the laws of the Republic of India.
2. The problem is fictional and intended solely for academic purposes.
3. Parties may frame additional sub-issues consistent with the facts.
4. All annexures form an integral part of the record.