# MOOT PROPOSITION

1. The Republic of Aryavarta is a constitutional democracy situated in South Asia, governed by a written Constitution adopted in 1952 in the aftermath of a prolonged independence movement. The Constitution enshrines a comprehensive catalogue of fundamental rights, including equality before the law, freedom of speech and expression, freedom of peaceful assembly and association, freedom of movement, and the right to life and personal liberty. Over the decades, the Supreme Court of Aryavarta has developed a robust body of constitutional jurisprudence interpreting the right to life as encompassing not merely physical existence but the right to live with dignity, autonomy, and decisional freedom. In several landmark judgments, the Court has recognised informational self-determination and privacy as intrinsic to personal liberty, while simultaneously holding that no fundamental right is absolute and that reasonable restrictions may be imposed in the interests of public order, national security, and the general welfare of society.

2. In the early 2010s, Aryavarta embarked upon an ambitious programme of digital transformation, aimed at leveraging technology to improve governance efficiency, expand access to public services, and integrate its economy with global digital markets. This programme led to the creation of extensive digital public infrastructure, including nationwide identity databases, interoperable payment systems, and large-scale digitisation of public records. Simultaneously, Aryavarta emerged as a preferred destination for artificial intelligence research, data analytics firms, and cross-border digital service providers, owing to its skilled workforce and rapidly expanding data ecosystem.

3. However, this rapid digitisation also gave rise to growing concerns regarding data misuse, surveillance, and the absence of a comprehensive legal framework governing personal data. Multiple high-profile incidents involving unauthorised data sharing by private entities, as well as allegations of excessive data collection by State agencies, triggered public debate and parliamentary scrutiny. Parliamentary committees noted that while innovation and national security imperatives required flexible data usage, unchecked executive discretion posed risks to individual liberty and democratic accountability.

4. Against this backdrop, Parliament enacted the Aryavarta Digital Personal Data Protection Act, 2023 ("**ADPDP Act**") after extensive debate, expert consultations, and submissions from civil societies, industry associations, and law enforcement agencies. The Statement of Objects and Reasons accompanying the Act declared that its purpose was to "*establish a principled framework for the processing of digital personal data, balancing the rights of individuals with the legitimate needs of the State and the economy, while ensuring that Aryavarta remains competitive in the global digital ecosystem*."

5. The ADPDP Act recognises personal data protection as a statutory right and imposes obligations on entities processing such data. At the same time, the ADPDP Act accords the State significant latitude by authorising the processing of personal data without the consent of the data principal where such processing is considered necessary for the maintenance of public

order, the prevention or investigation of offences, or the security of the State. The Act further empowers the Central Government to exempt specified State instrumentalities from the application of certain provisions of the Act through executive notification, on grounds of sovereignty, integrity, or public interest.

6. Additionally, the ADPDP Act permits the cross-border transfer of personal data to foreign States, territories, or entities as may be notified by the Central Government, subject to such conditions as it may prescribe. During parliamentary debates, the Government justified this provision as essential for international cooperation, global trade in digital services, and the functioning of advanced artificial intelligence systems that rely on transnational data processing. Critics, however, warned that broad executive discretion over exemptions and data transfers could undermine constitutional guarantees of privacy and expose citizens' data to foreign surveillance regimes.

7. Since its enactment, the ADPDP Act has been both lauded as a forward-looking legislative intervention and criticised for allegedly privileging State and corporate interests over individual rights. Several provisions of the Act have already been the subject of constitutional challenge, setting the stage for judicial scrutiny of the balance it strikes between technological governance, individual liberty, and State power.

8. In the latter half of 2023, Aryavarta witnessed a marked escalation in large-scale public demonstrations across several major metropolitan centres, triggered by a combination of economic slowdown, rising unemployment among urban youth, and public unease over the increasing deployment of automated decision-making systems in governance. While the overwhelming majority of these demonstrations were peaceful and constitutionally protected, intelligence and law enforcement agencies reported isolated but recurrent incidents of vandalism, arson, and targeted attacks on transport infrastructure, government buildings, and public utilities. Official estimates suggested that a small fraction of protestors were exploiting the anonymity of large crowds to engage in unlawful activity before dispersing.

9. Multiple parliamentary standing committee reports, tabled during the Winter Session of Parliament in 2023, noted the structural limitations of conventional policing methods in such contexts. The reports highlighted difficulties in identifying individual perpetrators *post facto*, reliance on inconsistent eyewitness testimony, and the growing use of masks, crowd density, and rapid movement to evade identification. At the same time, the committees cautioned against the unregulated adoption of surveillance technologies and stressed the need for legal safeguards, transparency, and accountability mechanisms.

10. Against this backdrop, the Ministry of Home Stability ("**MHS**"), invoking its statutory mandate to preserve public order and prevent threats to internal security, approved the initiation of Project OMNISIGHT, an artificial intelligence–enabled Facial Recognition Technology (FRT) system intended to operate as a decision-support tool for law enforcement agencies. Internal government communications described the project as a "*measured technological intervention*" aimed at enhancing investigative efficiency rather than replacing human judgment. The stated objectives of Project OMNISIGHT included the identification of

individuals suspected of involvement in violent incidents, deterrence of repeat offenders through enhanced detection capabilities, and improvement of response times during rapidly evolving public disturbances.

11. Project OMNISIGHT was conceived as a pilot programme, initially deployed in select urban zones with high-density CCTV coverage. The Ministry publicly stated that the system would operate primarily in public spaces, would not involve continuous tracking of individuals, and would be subject to periodic review by an inter-departmental oversight committee comprising representatives from the Ministries of Home Stability, Law and Justice, and Electronics and Information Technology.

12. The technological backbone of Project OMNISIGHT was developed through a publicprivate partnership with NeuroVision Inc., a multinational artificial intelligence and data analytics company incorporated and headquartered in Nordland, a technologically advanced State with which Aryavarta maintained longstanding diplomatic and commercial relations. NeuroVision was selected following a competitive global tender process that evaluated bidders on criteria including technical expertise, prior deployment experience, compliance with international data protection standards, and cost efficiency. The tender evaluation committee noted NeuroVision's prior involvement in urban security projects in several foreign jurisdictions, where its systems had reportedly contributed to reductions in unresolved violent crime.

13. Under the contractual framework, NeuroVision was tasked with providing the core algorithmic architecture, periodic software updates, and technical support for Project OMNISIGHT. The datasets used for training and deployment were sourced exclusively from government databases lawfully maintained by Aryavarta, including passport and immigration records, voter identification databases, driving licence repositories, and criminal records maintained by law enforcement agencies. The Government of Aryavarta expressly retained ownership and control over all personal data utilised under the project.

14. However, the agreement permitted NeuroVision limited and conditional access to certain datasets for purposes of system optimisation, debugging, and accuracy enhancement. Such access was subject to confidentiality obligations and oversight protocols, though the precise contours of these safeguards were not disclosed publicly. Government officials maintained that all data sharing was conducted in accordance with the ADPDP Act and that personal data was anonymised wherever feasible.

15. Notwithstanding these assurances, internal notes from the tender evaluation phase (later disclosed through parliamentary questions) revealed that certain officials had raised concerns regarding the long-term implications of algorithmic dependence, potential bias in training datasets, and the risks associated with cross-border technical collaboration. These concerns were ultimately overridden on the ground that delaying deployment would leave law enforcement ill-equipped to address emergent public order challenges.

16. On 18 March 2024, a large student-led protest was convened at Loktantra Square, the administrative and symbolic heart of Aryavarta's capital city, Cyberabad. The demonstration

was organised by a coalition of university unions and civil society groups to oppose recently introduced labour reforms and to express apprehension over the expanding deployment of algorithmic surveillance tools by State agencies. The organisers obtained prior permission from the local authorities, complied with prescribed conditions regarding crowd size and duration, and publicly reiterated their commitment to peaceful assembly.

17. From early afternoon until sunset, the protest remained largely non-violent, featuring speeches, placards, and sit-ins. According to official crowd estimates, more than 20,000 participants were present at various points during the day. As dusk approached, however, a small and unidentified segment of the gathering began engaging in confrontations with law enforcement personnel stationed at the periphery of the square. These confrontations escalated into stone-pelting, damage to barricades, and arson of two parked police vehicles. Several police officers sustained injuries, and public property was damaged.

18. Law enforcement agencies later characterised the outbreak of violence as "*coordinated and targeted*," suggesting the involvement of trained agitators embedded within the larger protest. No organisation formally claimed responsibility, and no contemporaneous arrests were made at the site, owing, according to the police, to concerns about escalating panic and stampede risks.

19. In the immediate aftermath, the MHS authorised the retrospective analysis of CCTV footage captured across Loktantra Square and its adjoining corridors. The footage was processed through Project OMNISIGHT, which had recently been integrated with the city's live surveillance network. Using a combination of facial recognition, movement trajectory mapping, and behavioural pattern analysis, the system generated a list of individuals categorised as "*high-confidence matches*" allegedly present during the violent phase of the protest.

20. Among those identified was Mr. Aarav Sen, a 26-year-old postgraduate student at the National University of Aryavarta, specialising in public policy. Mr. Sen was also a known participant in online digital rights advocacy forums and had previously attended lawful demonstrations relating to privacy and technology governance. There was no prior criminal record against him.

21. On the morning of 19 March 2024, Mr. Sen was arrested from his residence under provisions of the Public Order Preservation Act, 1987. The arrest memo cited "*algorithmically verified presence at the site of violence, supported by movement analytics generated through Project OMNISIGHT*" as the primary ground for arrest. No eyewitness testimony or physical evidence directly linking Mr. Sen to acts of violence was cited at the time of arrest.

22. From the outset, Mr. Sen denied any involvement in violent activity, maintaining that he had left Loktantra Square well before the onset of clashes. In support of his claim, he produced metadata from his personal mobile device, including location history, digital transit records, and timestamped messages, indicating his presence at a café approximately six kilometres

away during the relevant time window. He also furnished affidavits from two acquaintances who claimed to have met him at that location.

23. During custodial interrogation, Mr. Sen was informed that his identification was based on a "*confidence score exceeding 92%*" generated by Project OMNISIGHT. However, upon seeking disclosure of the underlying methodology, he was informed that the precise algorithmic parameters constituted proprietary information of NeuroVision Inc. and could not be fully disclosed.

24. Independent digital forensics experts engaged by Mr. Sen's legal counsel later examined publicly available technical documentation related to Project OMNISIGHT and highlighted that the system's own internal validation studies acknowledged a non-negligible false positive rate, particularly in environments characterised by dense crowds, partial facial occlusion, and low-light conditions – factors all present during the protest. Experts further noted that the system's accuracy varied significantly across demographic groups.

25. The prosecution countered these assertions by contending that Project OMNISIGHT's output was not relied upon in isolation. It argued that the algorithmic match was corroborated by secondary indicators, including gait analysis, historical patterns of Mr. Sen's participation in prior protests, and inferred movement trajectories derived from aggregated CCTV feeds. The prosecution emphasised that algorithmic tools function as probabilistic aids, not infallible determiners, and must be assessed cumulatively alongside other circumstantial material.

26. At the bail hearing, the Trial Court admitted the OMNISIGHT-generated evidence, observing that the exclusion of technologically obtained evidence at a preliminary stage would "*unduly handicap legitimate law enforcement efforts in an evolving threat landscape marked by sophisticated methods of anonymity*." The Court further noted that challenges relating to accuracy, bias, and transparency of the technology could be addressed at the stage of trial.

27. Mr. Sen's application for bail was rejected, with the Court citing the seriousness of the alleged offences, the potential for influencing witnesses, and the need to deter further public disorder. The Court also observed that the statutory presumption under the Public Order Preservation Act warranted a cautious approach in cases involving alleged coordinated violence.

28. In May 2024, a series of investigative reports published by leading national and international media outlets revealed that facial images, biometric templates, metadata, and behavioural datasets processed under Project OMNISIGHT were being routinely transferred to NeuroVision Inc.'s cloud servers located in Nordland. According to documents cited in the reports, these transfers occurred at regular intervals and were undertaken to facilitate machine learning–based optimisation, including recalibration of facial recognition accuracy, bias reduction models, and system performance audits.

29. The reports further alleged that while certain identifiers were masked, a significant portion of the transferred data remained re-identifiable when combined with auxiliary datasets, particularly movement trajectories and timestamped location metadata. Internal

correspondence quoted in the media suggested that NeuroVision's overseas engineering teams played an active role in refining the core algorithm, requiring access to real-world deployment data from Aryavarta.

30. These disclosures triggered widespread public debate. Several civil society organisations, digital rights collectives, and former members of statutory oversight bodies raised concerns that Nordland's domestic legal framework permits intelligence and law enforcement agencies to compel private companies to provide access to data stored within its jurisdiction. They warned that the cross-border transfer of sensitive personal data could expose Aryavartan citizens to foreign surveillance beyond the reach of domestic constitutional protections, thereby undermining informational self-determination.

31. In response, the Union Government of Aryavarta issued a public clarification stating that all data transfers were lawful, purpose-limited, and undertaken strictly within the framework of the ADPDP Act. The Government asserted that data was anonymised or pseudonymised "*to the maximum extent feasible*," that contractual safeguards prohibited misuse, and that no evidence existed of unauthorised access by foreign State agencies. Officials further emphasised that cross-border data flows were essential for maintaining cutting-edge AI systems and fulfilling Aryavarta's aspirations as a global digital economy.

32. Amid intensifying political scrutiny and parliamentary questions, the MHS, in coordination with the Ministry of Electronics and Information Technology, issued an executive order suspending NeuroVision's operational licence pending an inter-ministerial review. The suspension halted all data transfers and restricted NeuroVision's access to existing datasets, citing the need to reassess compliance with domestic law, national security considerations, and public confidence.

33. NeuroVision publicly expressed "*deep disappointment*," asserting that it had acted at all times with the knowledge and approval of Aryavartan authorities and in accordance with contractual and statutory obligations. The company warned that the suspension would severely disrupt ongoing system maintenance and compromise public safety objectives.

34. Within days, the Government of Nordland issued a formal diplomatic protest, alleging that Aryavarta's actions constituted a breach of the Bilateral Investment Treaty between Aryavarta and Nordland, 2011 ("**the Treaty**"). The protest note asserted that the abrupt suspension of operations without prior notice or opportunity to be heard violated obligations of fair and equitable treatment, protection against arbitrary and discriminatory measures, and legitimate expectations arising from regulatory assurances. Nordland further reserved its right to pursue remedies under the dispute resolution mechanism provided in the Treaty.

35. The Ministry of External Affairs of Aryavarta responded that while it remained committed to its international obligations, the measures in question fell squarely within sovereign regulatory powers exercised in the interest of public order, national security, and data sovereignty. It contended that the Treaty expressly recognises security and public interest exceptions and that no foreign investor could claim immunity from domestic law.

36. In September 2024, the Union Government of Aryavarta constituted a high-level InterMinisterial Review Committee (“**the Committee**”) to assess the legal, technical, and security implications of the project’s operational framework. The Committee comprised senior officials from the MHS, the Ministry of External Affairs, and the Ministry of Electronics and Information Technology, and was mandated to examine whether the continued engagement with NeuroVision Inc. posed risks to national security, data sovereignty, and constitutional rights. The Committee was also tasked with evaluating Aryavarta’s exposure to international legal obligations arising from its data governance policies.

37. While the Committee’s deliberations were ongoing and no final report had been submitted, the Ministry of Home Stability issued an executive notification suspending all data-sharing arrangements with NeuroVision Inc. with immediate effect. The notification cited “*emergent security considerations*” and directed all government departments and law enforcement agencies to cease the transfer of personal data to servers located in Nordland. It further mandated that all datasets previously transferred or mirrored overseas be localised within Aryavarta within a period of thirty days. The notification did not provide detailed reasons, nor did it specify whether the suspension was temporary or permanent in nature.

38. NeuroVision Inc. publicly protested the decision, asserting that the suspension had been imposed without prior notice, opportunity of hearing, or disclosure of reasons, despite the company having made substantial financial investments and deployed proprietary technology in Aryavarta over several years. The company contended that its operations were undertaken pursuant to express regulatory approvals and contractual arrangements entered into with the Government of Aryavarta, and that its investment was protected under the Treaty. NeuroVision further claimed that the abrupt suspension rendered its investment commercially unviable, disrupted ongoing system maintenance, and caused significant reputational harm in international markets.

39. Following the suspension, the Government of Nordland issued a formal diplomatic communication to Aryavarta expressing what it described as “*grave concern*” over the treatment accorded to an investor operating under the protection of the Treaty. The communication alleged that the measures adopted by Aryavarta were arbitrary, disproportionate, and inconsistent with regulatory assurances previously extended to NeuroVision Inc. It asserted that the transfer of data had been undertaken with the knowledge, consent, and active participation of Aryavartan authorities under the framework of the ADPDP Act and related executive approvals.

40. The diplomatic note further contended that the sudden reversal of policy, without procedural safeguards, constituted a breach of the Treaty’s obligation to provide fair and equitable treatment, and that the mandatory localisation directive effectively deprived NeuroVision of the economic value of its investment, amounting to indirect expropriation. Nordland warned that unless the dispute was resolved through amicable consultations, it reserved the right to initiate international arbitration in accordance with the dispute resolution provisions of the Treaty.

41. In response, the Ministry of External Affairs of Aryavarta acknowledged the existence of the Treaty but maintained that the impugned measures were justified by essential security interests and public order considerations. The Government asserted that the Treaty could not be interpreted to constrain Aryavarta's sovereign authority to regulate data flows within its territory, particularly where national security, constitutional rights, and public confidence in governance were implicated.

42. Against this evolving backdrop, Mr. Aarav Sen approached the Supreme Court of Aryavarta under Article 32 of the Constitution, challenging multiple facets of the State's actions. He assailed the legality of his arrest and continued detention, the admissibility of evidence generated through facial recognition technology, and the constitutional validity of the ADPDP Act itself. Mr. Sen argued that the Act confers excessively broad and unguided discretion upon the executive, dilutes the right to informational privacy recognised by constitutional jurisprudence, and enables mass surveillance without meaningful judicial or independent oversight.

43. The Union of Aryavarta defended the ADPDP Act as a carefully calibrated legislative instrument crafted after extensive deliberation. It is submitted that the ADPDP Act balances individual rights with collective security needs and incorporates sufficient safeguards through purpose limitation, executive accountability, and *post-facto* review mechanisms. The Government cautioned that judicial invalidation of core provisions would paralyse the State's ability to respond to complex and evolving security threats.

44. As diplomatic tensions escalated, a consortium of Aryavartan technology associations, industry bodies, and public interest litigants sought intervention in Mr. Aarav Sen's pending writ petition before the Supreme Court. These intervenors argued that the executive suspension of data transfers and operational licences, if upheld without judicial scrutiny, would have a chilling effect on foreign investment in Aryavarta's digital economy and undermine the predictability of its regulatory environment.

45. The intervenors further contended that the ADPDP Act and the executive actions taken under it exposed Aryavarta to international legal liability, thereby implicating Article 253 of the Constitution, which empowers Parliament to implement international treaties. They argued that arbitrary executive action in violation of treaty obligations could not be insulated from judicial review merely because it touched upon matters of foreign relations.

46. The Union of Aryavarta raised a preliminary objection to the maintainability of the issues pertaining to the Treaty before the Supreme Court. It argued that disputes arising under bilateral investment treaties are matters for international arbitration, not constitutional adjudication, and that domestic courts lack jurisdiction to pronounce upon alleged treaty breaches unless the treaty has been expressly incorporated into domestic law by legislation.

47. The Government further contended that judicial examination of the compliance with bilateral investment treaties would impermissibly entangle the Court in matters of foreign policy and

diplomatic relations, domains traditionally reserved to the executive. At the same time, however, the Union relied upon the security and public interest exceptions contained in the Treaty to justify its actions, submitting that the Court would necessarily have to interpret the scope of those exceptions in order to assess the legality and reasonableness of the executive measures under challenge.

48. In view of the overlapping constitutional, technological, and international law questions raised in the proceedings, the Supreme Court observed that the case involved novel and substantial issues of constitutional importance, including the domestic effect of international economic obligations, the extent to which executive action taken pursuant to a statute may expose the State to international liability, and whether constitutional courts may examine compliance with treaty obligations incidentally while adjudicating fundamental rights claims.

49. Accordingly, the Chief Justice of Aryavarta constituted a five-judge Constitution Bench and clarified that the issues relating to the Bilateral Investment Treaty would be heard and adjudicated to the extent they bear upon the constitutionality, legality, and arbitrariness of State action under the Constitution of Aryavarta.

The framed issues before the court are as follows:

I. Whether evidence collected through facial recognition technology deployed by the Government is admissible in law.

II. Whether the ADPDP Act is ultra vires the Constitution of Aryavarta.

III. Whether the deployment of Project OMNISIGHT and the arrest of Mr. Aarav Sen are violative of fundamental rights guaranteed under the Constitution.

IV. Whether the executive suspension of data transfers and operational licenses to NeuroVision is consistent with Aryavarta's obligations under the Treaty.

## PROCEDURAL ORDER BY THE SUPREME COURT OF ARYAVARTA

1. The Hon'ble Supreme Court of Aryavarta clarifies that it has jurisdiction under Article 32 of the Constitution to entertain the present writ petition, insofar as it raises substantial questions concerning the alleged violation of fundamental rights guaranteed under Part III of the Constitution.

2. The Court further clarifies that the challenge to executive action affecting cross-border data transfers, though implicating obligations arising under the Bilateral Investment Treaty between Aryavarta and Nordland, 2011, is maintainable before this Court to the limited extent that such obligations bear upon the constitutional validity of statutory provisions, the legality, proportionality, and non-arbitrariness of executive action, and the reasonableness of State conduct under Articles 14 and 21 of the Constitution.

3. The Court expressly notes that it is not exercising jurisdiction as an international arbitral tribunal, nor is it called upon to grant reliefs available under the Bilateral Investment Treaty. However, the Court may incidentally interpret treaty provisions where such interpretation is necessary to assess the constitutionality or legality of State action under domestic law.

4. The objection raised by the Union of Aryavarta regarding the exclusive jurisdiction of international arbitration is kept open for adjudication on merits, and shall be addressed by this Court while determining the scope and limits of judicial review in matters involving foreign relations, at a later stage.

### NOTE FOR THE COUNSELS

1. All issues framed by the Court, including Issue IV concerning the Bilateral Investment Treaty, shall be heard together and decided in accordance with the law. No party shall raise objections as to maintainability at the stage of final arguments beyond those already recorded.

2. The counsel appearing for all parties are directed to confine their submissions strictly to the issues framed. No additional facts shall be assumed, and no new grounds of challenge shall be introduced at the stage of oral arguments.

## ANNEXURE A

**Extract from "The Aryavarta Chronicle" dated 19 March 2024**

(***Independent National Daily***)

### STUDENT PROTEST AT LOKTANTRA SQUARE TURNS VIOLENT; POLICE ARREST SEVERAL USING AI SURVEILLANCE

What began as a peaceful student demonstration against recent labour reforms escalated into brief but intense clashes on Monday evening at Loktantra Square, leaving at least twelve police personnel injured and several public installations damaged.

The protest, organised by a coalition of student groups and civil society organisations, drew thousands of participants from across the city. Protestors carried placards criticising rising unemployment, data-driven governance, and what they described as the "normalisation of algorithmic surveillance."

Eyewitnesses stated that tensions rose shortly after sunset when a small group attempted to breach a police barricade near the northern entrance of the square. Police responded with controlled force, including batons and water cannons. By 9:30 PM, the area was cleared.

Senior police officials later confirmed that Project OMNISIGHT, the government's newly deployed facial recognition system, was used in real time to identify individuals suspected of instigating violence. "This is the future of policing," said a senior official on condition of anonymity. "We are no longer dependent solely on unreliable eyewitness accounts."

Among those arrested was Aarav Sen, a postgraduate student known for his involvement in digital rights advocacy. Mr. Sen's family and supporters maintain that he left the protest well before the clashes began.

Civil liberties groups have criticised the arrests, warning that reliance on facial recognition technology without transparency or independent oversight risks criminalising dissent. The Ministry of Home Stability has denied these allegations, stating that "technology merely assists human decision-making and does not replace it."

## ANNEXURE B

### Extract from "*OMNISIGHT: A Scalable AI-Driven Facial Recognition System for Urban Security" (Technical White Paper submitted by NeuroVision Inc. to the Ministry of Home* Stability)

Abstract

OMNISIGHT is an artificial intelligence–based facial recognition and behavioural analytics platform designed to assist law enforcement agencies in large-scale urban environments. The system integrates live video feeds with legacy identity databases to generate probabilistic identity matches.

System Architecture

OMNISIGHT employs a convolutional neural network trained on over 200 million facial images sourced from government-authorised datasets. The system uses a multi-factor recognition model incorporating facial geometry, gait analysis, and contextual behavioural markers.

Accuracy Metrics

Internal validation tests indicate an average accuracy rate of 92–94% under optimal lighting and camera resolution conditions. Accuracy declines in high-density crowd scenarios, adverse lighting, or partial occlusion.

False positive rates may increase under these conditions, particularly when matching against legacy databases with outdated or low-resolution images.

Human Oversight

OMNISIGHT does not autonomously trigger arrests. All match outputs are flagged as "assistive intelligence" and are subject to review by trained law enforcement officers prior to operational action.

Limitations

The system is not designed to determine criminal intent. It merely identifies facial similarity and movement correlation across multiple frames. OMNISIGHT explicitly disclaims responsibility for final enforcement decisions.

Data Processing and Optimisation

To improve system performance, anonymised datasets may be processed on secure cloud servers operated by NeuroVision Inc. outside Aryavarta. Such processing is undertaken strictly for algorithmic optimisation and quality assurance.

## ANNEXURE C

### *Relevant Provisions of the Aryavarta Digital Personal Data Protection Act, 2023*[1]

### *Section 16 – Cross-Border Transfer of Personal Data*

(1) The Central Government may notify such countries or territories to which a Data Fiduciary may transfer personal data, subject to such terms and conditions as may be specified.

(2) Nothing contained in this section shall restrict the applicability of any law for the time being in force in India that provides for a higher degree of protection for or restriction on transfer of personal data by a Data Fiduciary outside India in relation to any personal data or Data Fiduciary or class thereof.

### *Section 17 – Exemptions*

The Central Government may, by notification, exempt any instrumentality of the State from the application of this Act or any provision thereof, in the interest of the sovereignty and integrity of Aryavarta, the security of the State, or public order.

[1] ***Note***: The remaining provisions of the ADPDP are pari materia to Chapters I - IV of the Digital Personal Data Protection Act, 2023 of the Republic of India.