INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

DIGITAL DISSENT UNDER SURVEILLANCE: AN ANALYSIS

AUTHORED BY - APOORWA PANDEY[1]& DR. R. P. CHOUDHARY[2]

ABSTRACT

Artificial intelligence-enabled surveillance technologies deployed at public protests, including live facial recognition systems, predictive policing algorithms, and automated social media monitoring tools, generate a chilling effect upon the right to peaceful assembly that existing legal doctrine has failed to adequately address. This paper advances a specific doctrinal argument: that such surveillance constitutes not merely a negative interference with Article 21 of the International Covenant on Civil and Political Rights and Article 11 of the European Convention on Human Rights, but a breach of the positive obligation to facilitate peaceful assembly confirmed in *Kudrevičius and Others v Lithuania*. Existing proportionality and necessity doctrines are architecturally incapable of capturing this harm, algorithmic opacity forecloses meaningful proportionality review, and those most deterred by AI surveillance generate no enforcement record and bring no legal claim, rendering them structurally invisible to doctrine organised around discrete acts of interference. Comparative documentary analysis of the European Union and India confirms that no jurisdiction has enacted regulatory frameworks adequate to discharge this positive obligation.

Keywords: Freedom of assembly, AI surveillance, Chilling effect, Positive obligation.

1. INTRODUCTION

The right to freedom of peaceful assembly is not merely a formal legal entitlement it is the structural precondition upon which organised democratic dissent depends. Over the past decade, however, the spaces in which that right is exercised have been progressively colonised by artificial intelligence-enabled surveillance infrastructure. Facial recognition systems capable of identifying individuals in real time, predictive crowd-management algorithms, unmanned aerial vehicles, and automated social media monitoring tools now constitute a

[1] Author: Research Scholar, Dr. C.V. Raman University, Kota, Bilaspur, Chhattisgarh, India. Email: apoorwapandeyphd@gmail.com, Contact Number: 8982092688
[2] Co-Author: Dean of the Faculty of Law, Associate Professor, Dr. C.V. Raman University, Kota, Bilaspur (C.G.)

ISSN: 2582-6433

routine feature of law enforcement responses to public protest across a significant and growing number of jurisdictions. The legal frameworks governing these technologies have not kept pace with their operational deployment.

This paper investigates a specific and underexamined tension: the relationship between AI-enabled policing tools and the right to freedom of peaceful assembly as protected under international human rights law and domestic constitutional instruments. Existing scholarship has examined AI surveillance through the lens of privacy rights, data protection, and proportionality doctrine.[3] What no existing work has done is systematically argue that AI surveillance at protests breaches the positive obligation to facilitate peaceful assembly as distinct from the negative obligation to refrain from unjustified interference confirmed in *Kudrevičius and Others v Lithuania*.[4]

This paper advances that argument. AI surveillance generates a chilling effect that deters individuals from attending protests before any enforcement action occurs. Algorithmic opacity forecloses the transparency that meaningful proportionality review requires.[5] A multi-jurisdictional analysis reveals systemic regulatory failures in addressing these technological harms. Purpose-specific legislation is not a counsel of perfection; it is the minimum that obligation requires.

1.1.Existing Scholarship and The Research Gap

The intersection of AI surveillance and human rights has attracted considerable scholarly attention, though existing literature has developed along three largely separate tracks that together leave a critical doctrinal gap which this paper addresses.

The first track comprises technical and empirical assessments of AI surveillance accuracy and demographic impact. Fussey and Murray's independent evaluation of the Metropolitan Police's facial recognition trials established the empirical foundation for accuracy and rights concerns in the United Kingdom context, documenting the absence of meaningful legal oversight and the disproportionate impact upon marginalised communities.[6] The National Institute of

[3] Fussey and Murray, Independent Report on the MPS Trial of Live Facial Recognition Technology, 1–8, https://repository.essex.ac.uk/24946/1/Houston-We-Have-a-Problem.pdf; Murray, "Human Rights Implications of Algorithm-Based Decision-Making," 147–168, https://doi.org/10.1080/13600869.2019.1575385; Edwards and Veale, "Slave to the Algorithm?," 18–84, https://doi.org/10.2139/ssrn.2972855.

[4] Kudrevičius and Others v Lithuania, App No 37553/05, ECHR 2015 (Grand Chamber, 15 October 2015), [149]–[165], https://hudoc.echr.coe.int/eng?i=001-158910.

[5] Pasquale, Black Box Society, 1–18; Wachter, Mittelstadt, and Floridi, "Why a Right to Explanation Does Not Exist," 76–99, https://doi.org/10.1093/idpl/ipx005.

[6] Fussey and Murray, Independent Report on the MPS Trial of Live Facial Recognition Technology, 1–8, https://repository.essex.ac.uk/24946/1/Houston-We-Have-a-Problem.pdf.

ISSN: 2582-6433

Standards and Technology's Face Recognition Vendor Testing programme has since provided the most systematic global evidence of demographic accuracy differentials across facial recognition algorithms.[7] These contributions are empirically indispensable but do not advance doctrinal arguments about the legal consequences of the harms they document, and neither addresses the assembly rights dimension of AI surveillance.

The second track comprises legal scholarship on algorithmic accountability and transparency obligations under data protection and administrative law frameworks. Edwards and Veale have examined whether EU law imposes meaningful explanation requirements upon automated decision-making systems, concluding that existing frameworks fall significantly short of what accountability requires.[8] Wachter, Mittelstadt, and Floridi have similarly demonstrated that the right to explanation under the General Data Protection Regulation is narrower than commonly assumed, leaving significant accountability gaps in algorithmic decision-making.[9] Murray has examined the broader human rights implications of algorithm-based decision-making, identifying structural tensions between automated systems and established rights frameworks.[10] This track has established that algorithmic opacity poses fundamental challenges to legal accountability but engages primarily with data protection and administrative law rather than assembly rights, and does not address the chilling effect that surveillance generates upon collective action.

The gap these two tracks collectively share is the one this paper addresses. No existing scholarship has systematically argued that AI surveillance at protests breaches the positive obligation to facilitate peaceful assembly under Article 11 ECHR and Article 21 ICCPR; as distinct from the more commonly examined negative obligation to refrain from unjustified interference.

1.2.Contribution

This article establishes that AI surveillance at protests breaches the positive obligation to facilitate peaceful assembly under Article 11 ECHR and Article 21 ICCPR, that existing proportionality doctrine is architecturally incapable of capturing this breach.

[7] Grother, Ngan, and Hanaoka, Face Recognition Vendor Testing (FRVT) Part 3, 1–3, https://doi.org/10.6028/NIST.IR.8280.
[8] Edwards and Veale, "Slave to the Algorithm?," 18–84, https://doi.org/10.2139/ssrn.2972855.
[9] Wachter, Mittelstadt, and Floridi, "Why a Right to Explanation Does Not Exist," 76–99, https://doi.org/10.1093/idpl/ipx005.
[10] Murray, "Human Rights Implications of Algorithm-Based Decision-Making," 147–168, https://doi.org/10.1080/13600869.2019.1575385.

ISSN: 2582-6433

2. Conceptual and Theoretical Framework

2.1. AI Policing as a Modality of Power

AI-enabled policing is not an incremental development in surveillance technology; it represents a qualitatively distinct threat to collective action.[11] Contemporary AI surveillance systems operationalise this panoptic logic at scale, removing the resource constraints that historically limited its reach. Critically, they do more than record conduct: predictive algorithms profile individuals and allocate enforcement resources in advance of any act, meaning that persons may be targeted not for what they have done but for what a risk model projects they might do.

2.2. The Accountability Gap

The diffusion of decision-making authority across automated systems generates a structural accountability deficit that existing legal frameworks are not designed to address. Where a human officer stops, photographs, or detains a protestor, a legal subject is identifiable and accountability mechanisms can engage. Where the same decision is produced by an algorithm, responsibility is dispersed across system designers, procuring agencies, supervising officers, and political authorities a condition Nissenbaum has characterised as the 'problem of many hands.[12] This diffusion is compounded by what Pasquale terms the 'black box' problem: the opacity of automated decision-making systems forecloses the reasoned, reviewable justification that legal accountability requires.[13] A court cannot determine whether surveillance constitutes the least restrictive means available if the mechanism identifying its targets remains inaccessible to scrutiny.

2.3.The Chilling Effect and Categorical Targeting

The relationship between surveillance and the suppression of collective action has been examined empirically across several scholarly traditions. Ferguson demonstrated that predictive surveillance constitutes the populations it targets rather than neutrally detecting risk.[14] Penney provided quantitative evidence that awareness of state monitoring measurably reduces political engagement.[15] Zuboff identified the knowledge asymmetry between

[11] Foucault, Discipline and Punish, 195–228.
[12] Nissenbaum, "Accountability in a Computerised Society," 25–42, https://doi.org/10.1007/BF02639315.
[13] Pasquale, Black Box Society, 1–18.
[14] Ferguson, The Rise of Big Data Policing, 15–40. https://nyupress.org/9781479829859
[15] Penney, "Chilling Effects: Online Surveillance and Wikipedia Use," 117. https://btlj.org/data/articles2016/vol31/31_1/0117_0182_Penney_ChillingEffects_WEB.pdf

ISSN: 2582-6433

surveilling institutions and surveilled individuals as the foundational condition rendering meaningful resistance structurally unavailable.[16]

The chilling effect doctrine holds that surveillance can constitute a rights violation through its deterrent impact upon protected conduct independently of any enforcement action a proposition originating in *Laird v Tatum* and received into European human rights law through *Gillan and Quinton v United Kingdom* and *R (Bridges) v Chief Constable of South Wales Police*.[17] AI surveillance produces chilling effects structurally more severe than conventional policing for three reasons: its scalar reach deters all present rather than those individually observed; its data retention capacity makes deterrence temporally unbounded; and its categorical targeting logic operates on algorithmic profile rather than individual conduct.[18] This categorical logic is incompatible with the individualised assessment that Articles 21 ICCPR and 11 ECHR presuppose.[19] Those most deterred individuals who choose not to attend protests at all; generate no enforcement record and bring no claim, remaining structurally invisible to existing doctrine. This invisibility is the precise mechanism through which AI surveillance engages not merely the negative obligation to refrain from unjustified interference but the positive obligation confirmed in *Kudrevičius and Others v Lithuania* to take reasonable and appropriate measures to enable peaceful assembly to take place.[20]

4. AI Policing Technologies in Protest Contexts

4.1.Facial Recognition Systems

Live facial recognition (LFR) captures facial images via CCTV or dedicated cameras, creating biometric templates to match against watchlists in real time. Its use in protests is notable for identifying individuals without suspicion or consent, often based on broadly defined watchlists. The UK, especially the Metropolitan Police, has been actively deploying LFR since 2020, potentially scanning about one million faces annually. Legal challenges, like R (Bridges) v

[16] Zuboff, The Age of Surveillance Capitalism, 63–97. https://www.publicaffairsbooks.com/titles/shoshana-zuboff/the-age-of-surveillance-capitalism/9781610395694

[17] Laird v Tatum 408 US 1 (1972), 11–13; Gillan and Quinton v United Kingdom, App No 4158/05, (2010) 50 EHRR 45, [64]–[65], https://hudoc.echr.coe.int/eng?i=001-96585; R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058, [88]–[89], https://www.bailii.org/ew/cases/EWCA/Civ/2020/1058.html.

[18] Zuboff, Age of Surveillance Capitalism, 233–235; Pasquale, Black Box Society, 14–17; UN Human Rights Committee, General Comment No 37, CCPR/C/GC/37, [23], https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsldCrOlUTvLRFDzh6%2Fx1pWAuHDAfhBIFE3c%2BKJFwEjLFcbFPNPQZ5nWCnwvPEBSBPMcuL8IStSRENLtJzXJLgc4ZWJmxkTXiByFkpMSR6sT.

[19] UN Human Rights Committee, General Comment No 37, CCPR/C/GC/37, [23]; R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058, [88].

[20] Kudrevičius and Others v Lithuania, App No 37553/05, ECHR 2015 (Grand Chamber, 15 October 2015), https://hudoc.echr.coe.int/eng?i=001-158910.

ISSN: 2582-6433

Chief Constable of South Wales Police, highlight its vulnerabilities in absence of specific legal frameworks.[21]

4.2.Predictive Policing Algorithms

Predictive policing tools, using statistical and machine-learning models, analyse historical crime data, demographics, and geography to generate risk scores for individuals and locations. These tools have been used to identify potential disorder participants at protests, facilitating pre-emptive intelligence and resource allocation.[22][23]

4.3.Drone and Aerial Surveillance

Unmanned aerial vehicles equipped with high-resolution imaging, thermal sensors, and in some jurisdictions facial recognition payloads have been increasingly deployed at protest events. Their operational advantages persistent coverage, geographic flexibility, and visual access to large outdoor gatherings render them particularly effective for monitoring demonstrations that cannot be comprehensively observed from fixed ground infrastructure.

4.4.Automated Social Media Monitoring

Automated social media monitoring presents a specific and underappreciated threat to the organisational dimension of assembly rights. If the right to freedom of peaceful assembly is to be practically effective rather than formally recognised it must encompass protection for the communicative processes through which assemblies are planned and coordinated. Surveillance of those processes by law enforcement, prior to any assembly taking place, may chill not merely attendance at protests but the organisational capacity that makes collective action possible. This is a harm that existing assembly rights doctrine focused as it predominantly is upon the physical act of gathering is not presently structured to address.

[21] R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058, [85]– [90], https://www.bailii.org/ew/cases/EWCA/Civ/2020/1058.html.

[22] Bhuiyan, Johana. "LAPD Ended Predictive Policing Programs Amid Public Outcry: A New Effort Shares Many of Their Flaws." Guardian. 8 November 2021. https://www.theguardian.com/us-news/2021/nov/07/lapd-predictive-policing-surveillance-reform.
National Institute of Justice. "Predictive Policing Model in Los Angeles, Calif." CrimeSolutions. Posted 28 November 2022. https://crimesolutions.ojp.gov/ratedprograms/predictive-policing-model-los-angeles-calif.

[23] Oswald, "Algorithmic Risk Assessment Policing Models," 223–250, https://doi.org/10.1080/13600834.2018.1458455.

ISSN: 2582-6433

5. Comparative Analysis

5.1.The European Union

The European Union represents the most developed regulatory framework for AI policing globally, and the only jurisdiction to have enacted comprehensive, binding AI-specific legislation with direct application to facial recognition in law enforcement contexts. The EU AI Act Regulation (EU) 2024/1689 prohibits real-time remote biometric identification by law enforcement in publicly accessible spaces from 2 February 2025, subject to narrow carve-outs for terrorism, missing persons, and serious crime investigations.[24] Predictive policing based solely on profiling is classified as an "unacceptable risk" practice, prohibited from the same date.[25] Retrospective facial recognition the analysis of previously recorded footage, including footage of protest events is classified as high-risk rather than prohibited, with compliance obligations deferred to 2 December 2027 under the provisionally agreed AI Omnibus.[26]

The implementation gap is compounded by the divergence between regulatory text and operational reality. A 2024 survey identified at least eleven EU member states already operating police facial recognition systems prior to the prohibited-practices provisions becoming enforceable, and as of mid-2025 only three member states had designated the national competent authorities required under the Act. Sweden introduced legislation in March 2026, Proposition 2025/26:150, proposing to authorise police use of AI systems for real-time facial recognition for serious crimes, with the proposed law entering into force on 1 July 2026, directly exercising the member-state exception clause a development civil liberties organisations have identified as a structural vulnerability in the Act's prohibition architecture.[27]

The processing of personal data by police for law enforcement is governed by Directive (EU) 2016/680, known as the Law Enforcement Directive (LED), rather than the General Data Protection Regulation. The LED mandates obligations such as purpose limitation, data minimisation, and enhanced protections for special data categories, particularly biometric data. Specifically, storage limitations apply to biometric records from protest surveillance, and processing biometric data must meet a 'strictly necessary' standard. Compliance is overseen

[24] Regulation (EU) 2024/1689 (Artificial Intelligence Act), OJ L 1689/1, arts 5(1)(d), 5(1)(h), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.
[25]Regulation (EU) 2024/1689 (Artificial Intelligence Act), OJ L 1689/1, art 5(1)(d), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.
[26] Regulation (EU) 2024/1689 (Artificial Intelligence Act), OJ L 1689/1, Annex III, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.
[27] Swedish Government, Polisens användning av AI för ansiktsigenkänning i realtid, Proposition 2025/26:150 (3 March 2026), https://www.riksdagen.se/sv/dokument-och-lagar/dokument/proposition/polisens-anvandning-av-ai-for-ansiktsigenkanning-i_hd03150/html/.

ISSN: 2582-6433

by national data protection authorities, with additional guidance confirming that real-time facial recognition in public areas also falls under LED obligations alongside the AI Act.[28]

The EU AI Act therefore does not discharge the positive obligation confirmed in *Kudrevičius*: its prohibition on real-time biometric identification addresses only the most overt modality of AI surveillance, retrospective protest surveillance remains classified as high-risk rather than prohibited with compliance obligations deferred until December 2027, and a state cannot be said to have taken reasonable and appropriate measures to facilitate peaceful assembly when the primary regulatory framework governing the tools most likely to chill that assembly will not be fully operative for years after those tools have been deployed.

5.2.India

India presents a distinct regulatory profile: constitutional provisions with considerable latent protective capacity, operating alongside a formally approved and expanding AI surveillance infrastructure in the near-total absence of purpose-specific legislative governance. Article 19(1)(b) of the Constitution of India guarantees the right to assemble peaceably and without arms, and Article 21's protection of personal liberty has, following the Supreme Court's landmark judgment in *K.S. Puttaswamy (Retd.) v Union of India* (2017), been authoritatively interpreted to encompass a fundamental right to privacy.[29]

The Digital Personal Data Protection Act 2023 Act No. 22 of 2023, which received Presidential assent on 11 August 2023 establishes India's primary data protection framework.[30] However, the Act's protective scope is significantly curtailed in law enforcement contexts by two categories of exemption. First, the rights of data principals and obligations of data fiduciaries do not apply to processing by government entities in the interest of the security of the state and public order.[31] Second, exemptions apply to the prevention and investigation of offences.[32] As the PRS India legislative analysis confirms, these exemptions are framed with sufficient breadth to exclude the majority of police AI surveillance activity from the Act's

[28] Directive (EU) 2016/680, OJ L 119/89, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0680; European Data Protection Board, "Guidelines 05/2022 on Facial Recognition in Law Enforcement," https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition-technology_en.

[29] K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1 (Supreme Court of India), https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf.

[30] Digital Personal Data Protection Act 2023, Act No 22 of 2023 (India), https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.

[31] PRS Legislative Research, "Digital Personal Data Protection Bill, 2023," https://prsindia.org/billtrack/the-digital-personal-data-protection-bill-2023.

[32] PRS Legislative Research, "Digital Personal Data Protection Bill, 2023," https://prsindia.org/billtrack/the-digital-personal-data-protection-bill-2023.

ISSN: 2582-6433

operative requirements a structural limitation that renders the DPDP Act largely ineffective as a constraint upon AI policing at protest events.[33]

The existence of a national Automated Facial Recognition System (AFRS) administered by the National Crime Records Bureau (NCRB) is confirmed by official government sources. A Ministry of Home Affairs parliamentary statement of 4 March 2020 confirmed that approval had been accorded for implementation of the AFRS by the NCRB, stating that it would use police records and be accessible only to law enforcement agencies.[34] No purpose-specific legislative authorisation for the AFRS and no independent judicial oversight mechanism governing its use at protest events has been established. The constitutional framework established by *Puttaswamy* furnishes the doctrinal foundation for such a challenge, but no definitive judicial determination of the AFRS's compatibility with fundamental rights had been reported at the time of writing.

India's constitutional framework, as developed in *Puttaswamy*, furnishes the doctrinal foundation upon which a positive obligation to facilitate peaceful assembly free from AI surveillance could be constructed, but the operational deployment of the Automated Facial Recognition System without purpose-specific legislative authorisation, without independent judicial oversight, and with broad exemptions effectively excluding law enforcement processing from the Digital Personal Data Protection Act 2023's operative requirements, confirms that that foundation has not yet been built upon — and that the positive obligation, if it is to have practical content, demands legislative action that has not been taken.

6. Findings and Suggestions

The following recommendations represent not preferable improvements upon existing frameworks but the minimum legislative threshold required to discharge the positive obligation to facilitate peaceful assembly confirmed in Kudrevičius and Others v Lithuania an obligation that, as the doctrinal and comparative analysis above demonstrates, no jurisdiction examined has yet satisfied.

First, legislatures should enact purpose-specific statutes expressly governing AI surveillance at protests, specifying authorisation conditions, permissible data categories, maximum retention periods, and designated supervisory authorities following the legislative architecture established by Article 5 of the EU AI Act, which prohibits real-time biometric identification in

[33] PRS Legislative Research, "Digital Personal Data Protection Bill, 2023," https://prsindia.org/billtrack/the-digital-personal-data-protection-bill-2023.
[34] Ministry of Home Affairs, "Automated Facial Recognition System," https://mha.gov.in.

ISSN: 2582-6433

publicly accessible spaces.

Second, governments should mandate human rights impact assessments prior to any AI surveillance deployment at protests, expressly requiring evaluation of chilling effects upon assembly rights; adopting the compatibility assessment mechanism under the New Zealand Bill of Rights Act 1990 as the operative model for rights-proofing at the point of legislative design.

Third, independent regulatory authorities should require mandatory demographic bias auditing of all AI surveillance systems before protest deployment, with results publicly disclosed modelled on the bias audit obligations under the Illinois Artificial Intelligence Video Interview Act 2019, extended to law enforcement contexts with commensurate public reporting requirements.

Fourth, states should prohibit retention of biometric records generated at protest events in searchable databases absent individualised suspicion of a specific criminal offence, consistent with the storage limitation obligation under Article 4(1)(e) of the Law Enforcement Directive and General Comment No 37's prohibition on unjustified monitoring of assembly participants.

Fifth, legislatures should establish a binding statutory corroboration requirement prohibiting any arrest, detention, or search based solely on an AI surveillance result elevating the Williams v City of Detroit settlement standard into a universally applicable legislative obligation.

7. Conclusion

The positive obligation argument advanced in this paper can be stated precisely. AI surveillance tools deployed at protest events breach that obligation not through any single act of enforcement, but through the cumulative, pre-emptive, and structurally invisible deterrence they generate. And judicial remedies, however rigorously applied, are confined by definition to those who have already been subjected to the power from which the law should have protected them. What follows from this is not merely that better regulation is desirable. It is that purpose-specific legislation; incorporating mandatory human rights impact assessments, independent demographic auditing, enforceable retention limits, and a statutory corroboration requirement; is the minimum the positive obligation legally demands, and that states which deploy AI surveillance at protests without enacting it are not navigating a regulatory grey area: they are in breach of a binding international human rights obligation.

Bibliography

ACLU of New Jersey. "ACLU-NJ and ACLU National File Amicus in Challenge to Wrongful Arrest Due to Face Recognition." Accessed May 18, 2026. https://www.aclu-nj.org/press-

ISSN: 2582-6433

releases/aclu-nj-and-aclu-national-file-amicus-challenge-wrongful-arrest-due-face-recognition.

American Civil Liberties Union. "Civil Rights Advocates Achieve the Nation's Strongest Police Department Policy on Facial Recognition Technology." Accessed May 18, 2026. https://www.aclu.org/press-releases/civil-rights-advocates-achieve-the-nations-strongest-police-department-policy-on-facial-recognition-technology.

American Civil Liberties Union. "More Than a Dozen Wrongful Arrests Due to Police Reliance on Facial Recognition Technology." Accessed May 18, 2026. https://www.aclu.org/news/privacy-technology/more-than-a-dozen-wrongful-arrests-due-to-police-reliance-on-facial-recognition-technology.

American Civil Liberties Union. "Parks v McCormac." Accessed May 18, 2026. https://www.aclu.org/cases/parks-v-mccormac.

American Civil Liberties Union. "Williams v City of Detroit." Accessed May 18, 2026. https://www.aclu.org/cases/williams-v-city-of-detroit-face-recognition-false-arrest.

Artificial Intelligence Video Interview Act 2019 (Illinois), 820 ILCS 42/1. https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=4212.

Bhuiyan, Johana. "LAPD Ended Predictive Policing Programs Amid Public Outcry: A New Effort Shares Many of Their Flaws." *The Guardian,* November 8, 2021. https://www.theguardian.com/us-news/2021/nov/07/lapd-predictive-policing-surveillance-reform.

Biometric Information Privacy Act (Illinois, 2008), 740 ILCS 14/1. https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

Cagle, Matt. "Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color." *ACLU of Northern California,* October 11, 2016. https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target.

Chen, Stephen. "Surveillance on the Moon? China to Take Its Mass Camera Network to Outer Space." *South China Morning Post,* March 4, 2024. https://www.scmp.com/news/china/science/article/3254054/skynet-20-china-plans-bring-largest-surveillance-camera-network-earth-moon-protect-lunar-assets.

Convention for the Protection of Human Rights and Fundamental Freedoms, opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953). https://www.echr.coe.int/documents/d/echr/convention_ENG.

Data Protection Act 2018 (UK). https://www.legislation.gov.uk/ukpga/2018/12/contents.

ISSN: 2582-6433

Digital Personal Data Protection Act 2023 (India). https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.

Director of Public Prosecutions v Ziegler and Others UKSC 23, AC 408. https://www.bailii.org/uk/cases/UKSC/2021/23.html.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119/89. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0680.

Edwards, Lilian, and Michael Veale. "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For." *Duke Law & Technology Review* 16 (2017): 18–84. https://doi.org/10.2139/ssrn.2972855.

European Data Protection Board. "Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement." Accessed May 18, 2026. https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition-technology_en.

Executive Order No. 14179, 90 Fed Reg 8741 (January 20, 2025). https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/.

Executive Order No. 14319, 90 Fed Reg 35389 (July 23, 2025). https://www.whitehouse.gov/fact-sheets/2025/07/fact-sheet-president-donald-j-trump-prevents-woke-ai-in-the-federal-government/.

Executive Order No. 14365, 90 Fed Reg 58499 (December 11, 2025). https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/.

Ferguson, Andrew Guthrie. *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York: NYU Press, 2017. https://nyupress.org/9781479829859.

Foucault, Michel. *Discipline and Punish: The Birth of the Prison*. Translated by Alan Sheridan. New York: Vintage Books, 1977.

Fussey, Pete, and Daragh Murray. *Independent Report on the MPS Trial of Live Facial Recognition Technology*. Human Rights Centre, University of Essex, 2019. https://repository.essex.ac.uk/24946/1/Houston-We-Have-a-Problem.pdf.

ISSN: 2582-6433

Gillan and Quinton v United Kingdom (European Court of Human Rights, Chamber, App No 4158/05, 12 January 2010). https://hudoc.echr.coe.int/eng?i=001-96585.

Grother, Patrick, Mei Ngan, and Kayee Hanaoka. *Face Recognition Vendor Testing (FRVT) Part 3: Demographic Effects*. NISTIR 8280. National Institute of Standards and Technology, 2019. https://doi.org/10.6028/NIST.IR.8280.

Home Office (UK). "Police Use of Facial Recognition." Accessed May 18, 2026. https://www.gov.uk/government/publications/police-use-of-facial-recognition.

Human Rights Act 1998 (UK). https://www.legislation.gov.uk/ukpga/1998/42/contents.

International Covenant on Civil and Political Rights, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976). https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

IPVM Team. "China Public Video Surveillance Guide: From Skynet to Sharp Eyes." *IPVM*, June 14, 2018. https://ipvm.com/reports/sharpeyes.

K.S. Puttaswamy (Retd.) v Union of India, (2017) 10 SCC 1. https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf.

Koebler, Jason. "Customs and Border Protection Predator Drone Over Minneapolis." *Vice*, May 29, 2020. https://www.vice.com/en/article/customs-and-border-protection-predator-drone-minneapolis-george-floyd.

Kudrevičius and Others v Lithuania (European Court of Human Rights, Grand Chamber, App No 37553/05, 15 October 2015). https://hudoc.echr.coe.int/eng?i=001-158910.

Laird v Tatum, 408 US 1 (1972).

Metropolitan Police Service. "Live Facial Recognition." Accessed May 18, 2026. https://www.met.police.uk/police-forces/metropolitan-police/areas/about-us/about-the-met/facial-recognition-technology.

Ministry of Home Affairs (India). "Automated Facial Recognition System." Accessed May 18, 2026. https://mha.gov.in.

Murray, Daragh. "Human Rights Implications of Algorithm-Based Decision-Making." *Information & Communications Technology Law* 28, no. 3 (2019): 147–168. https://doi.org/10.1080/13600869.2019.1575385.

National Institute of Justice. "Predictive Policing Model in Los Angeles, Calif." *CrimeSolutions*, November 28, 2022. https://crimesolutions.ojp.gov/ratedprograms/predictive-policing-model-los-angeles-calif.

National Institute of Standards and Technology. "Demographic Effects in Face Recognition." Accessed May 18, 2026. https://pages.nist.gov/frvt/html/frvt_demographics.html.

ISSN: 2582-6433

New Zealand Bill of Rights Act 1990 (NZ). https://www.legislation.govt.nz/act/public/1990/0109/latest/whole.html.

New Zealand Human Rights Act 1993 (NZ). https://www.legislation.govt.nz/act/public/1993/0082/latest/whole.html.

Nissenbaum, Helen. "Accountability in a Computerized Society." *Science and Engineering Ethics* 2, no. 1 (1996): 25–42. https://doi.org/10.1007/BF02639315.

Oswald, Marion, Jamie Grace, Sheena Urwin, and Geoffrey C. Barnes. "Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and 'Experimental' Proportionality." *Information & Communications Technology Law* 27, no. 2 (2018): 223–250. https://doi.org/10.1080/13600834.2018.1458455.

Pasquale, Frank. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press, 2015.

Penney, Jonathon W. "Chilling Effects: Online Surveillance and Wikipedia Use." *Berkeley Technology Law Journal* 31, no. 1 (2016): 117–182. https://btlj.org/data/articles2016/vol31/31_1/0117_0182_Penney_ChillingEffects_WEB.pdf.

PRS Legislative Research. "Digital Personal Data Protection Bill, 2023." Accessed May 18, 2026. https://prsindia.org/billtrack/the-digital-personal-data-protection-bill-2023.

Public Order Act 2023 (UK). https://www.legislation.gov.uk/ukpga/2023/15/contents.

R (Bridges) v Chief Constable of South Wales Police EWCA Civ 1058. https://www.bailii.org/ew/cases/EWCA/Civ/2020/1058.html.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L 1689/1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.

Swedish Government. *Polisens användning av AI för ansiktsigenkänning i realtid*, Proposition 2025/26:150 (March 3, 2026). https://www.riksdagen.se/sv/dokument-och-lagar/dokument/proposition/polisens-anvandning-av-ai-for-ansiktsigenkanning-

ISSN: 2582-6433

i_hd03150/html/.

UN Human Rights Committee. *General Comment No. 37 (2020) on the right of peaceful assembly (article 21)*, 129th sess, UN Doc CCPR/C/GC/37 (17 September 2020). https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsldCrOlUTvLRFDzh6%2Fx1pWAuHDAfhBIFE3c%2BKJFwEjLFcbFPNPQZ5nWCnwvPEBSBPMcuL8IStSRENLtJzXJLgc4ZWJmxkTXiByFkpMSR6sT.

Wachter, Sandra, Brent Mittelstadt, and Luciano Floridi. "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation." *International Data Privacy Law* 7, no. 2 (2017): 76–99. https://doi.org/10.1093/idpl/ipx005.

White House. "President Donald J. Trump Unveils National AI Legislative Framework." March 20, 2026. https://www.whitehouse.gov/releases/2026/03/president-donald-j-trump-unveils-national-ai-legislative-framework/.

Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019. https://www.publicaffairsbooks.com/titles/shoshana-zuboff/the-age-of-surveillance-capitalism/9781610395694.