

класифікаційних категорій персоналу у сфері культури відповідно по яким буде формуватись сітка оплати праці (адже сьогодні спостерігається значний перекош в оплаті праці деяких закладів культури, які фінансуються з державного бюджету та тих, які стоять на балансі ОМС ; 5) сприяння розвитку приватних закладів культури (музеїв, галерей, експозиційних центрів, театрів, хореографічних та музичних студій та отриманню ними субвенції в частині надання ними культурних послуг вузького спрямування; 6) сприяння отриманню фінансової автономії закладів культури комунальної власності; 7) запровадження дієвого механізму фінансування порядку підвищення кваліфікації працівників закладів культури.

1. Про охорону культурної спадщини: Закон від 8 червня 2000 року № 1805-III. *Відомості Верховної Ради України*. 2000. № 39. Ст.333.

2. Про Національну поліцію України : Закон України від 02.07.2015. URL: <https://zakon.rada.gov.ua/laws/show/58019#Text>.

3. Про затвердження категорій об'єктів державної форми власності та сфер державного регулювання, які підлягають охороні органами поліції охорони на договірних засадах : постанова Кабінету Міністрів України від 21 листопада 2018 р. № 975. URL: <https://zakon.rada.gov.ua/laws/show/975-2018-%D0%BF#Text>.

4. Про організацію службової діяльності поліції охорони з питань забезпечення фізичної охорони об'єктів: Наказ МВС України від 07.07.2017 № 577. URL: <https://zakon.rada.gov.ua/laws/show/z0989-17#Text>.



Ростислав МОЛЧАНОВ

доцент кафедри
адміністративного права і процесу
Дніпровського державного
університету внутрішніх справ
(м. Дніпро, Україна),
кандидат юридичних наук, доцент

ІНТЕГРАЦІЯ ТЕХНОЛОГІЙ РОЗПІЗНАВАННЯ ОБЛИЧ (FRT) У СИСТЕМІ МІСЬКОГО ВІДЕОСПОСТЕРЕЖЕННЯ: ПРАВОВІ ВИКЛИКИ ТА МІЖНАРОДНИЙ ДОСВІД

Інтеграція технології розпізнавання облич (Facial Recognition Technology – FRT) у системи міського відеоспостереження фундаментально змінює характер взаємодії держави та особи. Технічна сутність FRT перетворює традиційний розшук підозрюваних на інструмент масового стеження (mass surveillance): задля ідентифікації одного правопорушника система обробляє біометричні дані тисяч законослухняних громадян. Це створює прецедент «віртуального шиккування» (perpetual line-up), де кожен перехожий де-факто стає об'єктом підозри. Мета доповіді – проаналізувати правові механізми США, ЄС та Великої Британії щодо захисту права на анонімність осіб, які не є фігурантами кримінальних проваджень.

«Теорія мозаїки» та ерозія приватності (досвід США).

Традиційну доктрину про відсутність «очікування приватності» у публічних місцях американські правники переглядають крізь призму «теорії мозаїки» (Mosaic Theory), розвинутої у рішеннях Верховного Суду США (справи *United States v. Jones*, *Carpenter v. United States*). Суть теорії полягає в тому, що хоча поодинокі фіксації особи не є порушенням, сукупність (мозаїка) даних про її пересування створює якісно нову інформацію. Це дозволяє ретроспективно відтворити приватне життя особи: від політичних поглядів і віросповідання до кола спілкування [1; 12].

FRT руйнує концепцію «публічної анонімності» (obscurity), перетворюючи адміністративний моніторинг на несанкціонований обшук без ордеру, що суперечить Четвертій поправці до Конституції США. Законодавство окремих штатів, зокрема Закон Меріленду 2024 року (Facial Recognition for Law Enforcement Act), уже забороняє використовувати FRT для моніторингу осіб під час реалізації ними конституційних прав (наприклад, на мітингах) і вимагає негайного видалення даних, що не збіглися зі списками розшуку.

«Охолоджуючий ефект» та демократія (європейський підхід).

Європейські інституції вбачають у FRT загрозу демократичним свободам через

поширення «охолоджуючого ефекту» (chilling effect) – самоцензури громадян внаслідок страху бути ідентифікованими [7; 11].

У рішенні у справі *Glukhin v. Russia* (2023) Європейський суд з прав людини визнав використання FRT щодо учасника мирного пікету порушенням статей 8 та 10 Конвенції. Суд наголосив: технологія є настільки інтрузивною (втручальною), що її застосування до осіб, які не становлять суспільної небезпеки, є непропорційним. Держава не має права використовувати біометрію для контролю за політичною активністю під приводом охорони порядку. Цей підхід кодифіковано в Регламенті ЄС про штучний інтелект (EU AI Act 2024). Стаття 5 Регламенту відносить дистанційну ідентифікацію в реальному часі у публічних місцях до «заборонених практик», оскільки ризики для прав мільйонів громадян переважають потенційну безпекову користь [9; 10].

Технічні ризики та прецедент *Bridges* (Велика Британія).

Окрім правових аспектів, існує критична проблема технічної похибки. Звіти NIST (2024–2025) підтверджують, що ризик «хибнопозитивних результатів» (False Positives) залишається високим, особливо в умовах вуличної зйомки [5; 6]. Для середнього громадянина це створює реальну загрозу безпідставного затримання.

Апеляційний суд Англії у справі *Bridges v South Wales Police* (2020) встановив засадничий принцип: сам факт автоматизованого порівняння обличчя особи зі списком розшуку (processing) уже є втручанням у приватність, незалежно від того, чи будуть ці дані зберігатися далі. Суд також вказав на порушення обов'язку щодо рівності (PSED), оскільки поліція не перевірила алгоритм на наявність демографічної упередженості, що створює ризик дискримінації жінок та етнічних меншин [2; 8].

Висновки:

Враховуючи викладене, встановлення та забезпечення відповідного балансу між безпекою та правами людини потребує дотримання наступних норм:

Заборона масового сканування. Законодавчо заборонити невибіркове використання FRT. Ідентифікація має бути виключно цільовою (targeted) та здійснюватися за санкцією суду.

Правовий статус результатів. Закріпити норму, згідно з якою автоматичне спрацювання системи (match) є лише підставою для перевірки, а не доказом вини чи приводом для затримання без додаткової верифікації людиною.

Захист даних осіб, що не перебувають у розшуку. Впровадити імперативну вимогу щодо миттєвого та незворотного знищення біометричних шаблонів осіб, які не збіглися зі списком розшуку.

Прозорість моніторингу. Забезпечити чітке маркування зон біометричного контролю, аби громадяни могли свідомо обирати – перебувати в зоні моніторингу чи ні.

1. Alvarado A. The Mosaic Theory in Fourth Amendment Jurisprudence: The Last Bastion of Privacy in a Camera-Surveilled World. *St. Mary's Law Journal*. 2024. Vol. 55, no. 3. P. 849–885.

2. Biometrics and Surveillance Camera Commissioner. Annual Report 2023–2024. London : UK Home Office, 2024. 34 p.

3. Facial Recognition for Law Enforcement Act of 2024 (Senate Bill 192). General Assembly of Maryland. 2024. Chapter 123.

4. *Glukhin v. Russia* : judgment of the European Court of Human Rights dated 4 July 2023 (Application no. 11519/20). Strasbourg : *ECHR*, 2023.

5. Grother P., Ngan M., Hanaoka K. Face Recognition Technology Evaluation (FRTE) Part 1: Verification : NIST Interagency Report 8525. Gaithersburg : NIST, 2024.

6. Knott A. et al. A Rapid Test for Accuracy and Bias of Face Recognition. WACV 2025 Proceedings. 2025.

7. Penney J. W. Understanding Chilling Effects. *Minnesota Law Review*. 2022. Vol. 106. P. 1451–1518.

8. *R (Bridges) v Chief Constable of South Wales Police* : judgment of the Court of Appeal (Civil Division) dated 11 Aug. 2020. EWCA Civ 1058. London, 2020.

9. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*. 2024. L series.

10. Remote Biometric Identification: A Technical & Legal Guide. European Digital Rights (EDRI). 2025. URL : <https://edri.org/our-work/remote-biometric-identification-a-technical-legal-guide/>.

11. Stop Facial Recognition campaign. Big Brother Watch. URL : <https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/>.

12. Vidyarthi A. The Public Square Has Eyes (or Cameras): Anonymous Speech Under the First and Fourth Amendments in the Age of Facial Recognition. *Fordham Intellectual Property, Media and Entertainment Law Journal*. 2022. Vol. 32, no. 3. P. 630–674.