

Дмитро КАЛЮЖНИЙ,
здобувач вищої освіти третього (наукового) рівня
кафедри права гуманітарно-правового факультету
Національного аерокосмічного університету
«Харківський авіаційний інститут», Харків, Україна
ORCID: <https://orcid.org/0009-0006-1709-8405>
e-mail: dmitrijkoluznyj555@gmail.com

DOI: <https://doi.org/10.32620/pls.2025.67.16>

ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ ВИКОРИСТАННЯ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ ПРАВООХОРОННИМИ ОРГАНАМИ

Анотація: Відеоспостереження завжди було критично важливим компонентом забезпечення правопорядку та громадської безпеки в роботі правоохоронців. Зображення та аудіо з записів відеоспостереження відіграють важливу роль у виявленні злочинів, ідентифікації потенційних свідків, ідентифікації та/або усуненні підозрюваних, а також у визначенні потенційних можливостей для розслідування, таких як хронологія подій та додаткові джерела даних відеоспостереження. Станом на сьогодні існують проблеми правового регулювання щодо встановлення систем відеоспостереження як з боку місцевої влади, так і для правоохоронців. Закони України «Про місцеве самоврядування в Україні» та «Про Національну поліцію» як і інші профільні нормативні акти не передбачають прямих повноважень щодо встановлення технологій стеження за населенням. Таким чином, впровадження і застосування систем відеоспостереження в правоохоронній сфері потребує спеціального нормативного врегулювання і конкретизації.

Ключові слова: системи відеоспостереження, правоохоронна діяльність, інформаційна безпека, персональні данні, технологія розпізнавання обличчя.

В сучасному цифровому світі інформаційні дані стають все більш важливим джерелом і інструментом для правоохоронних органів в забезпеченні громадської безпеки. Для виконання покладених на них завдань, органи Національної поліції користуються повноваженнями у сфері інформаційно-аналітичного забезпечення відповідно до ст. 25-27 Закону України «Про Національну поліцію» [1], згідно з якими в рамках своєї діяльності вони можуть: формувати реєстри та бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України; користуватися реєстрами та базами (банкками) даних Міністерства внутрішніх справ України та інших органів державної влади; здійснювати інформаційно-пошукову та інформаційно-аналітичну роботу та інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями. Насьогодні, реалізація зазначених повноважень здійснюється за допомогою використання ІКТ та алгоритмів штучного інтелекту, не останнє місце серед яких посідають системи відеоспостереження з можливостями ШІ-аналітики. Наприклад, в поліцейських центрах, що працюють в режимі реального часу, ШІ може значно підвищити ефективність і дієвість поліцейських,

автоматизувавши аналіз великих обсягів даних, надаючи інформацію в реальному часі та прогнозуючи злочинну діяльність. Системи ШІ можуть відстежувати записи з камер спостереження, виявляти підозрілу поведінку та сповіщати правоохоронців про потенційні загрози, дозволяючи їм швидше й точніше реагувати на інциденти. Відеоаналітика автоматично генерує описи того, що відбувається у відео із камер спостереження, які можна використовувати для відстеження людей (FRT), автомобілів та інших об'єктів, виявлених у відеопотоці, а також їх зовнішнього вигляду та рухів. Потім цю інформацію можна використовувати як основу для повідомлення центру оперативного реагування правоохоронних органів. Так, у м. Харків було запущено програмно-апаратний комплекс аналітичного супроводу оперативно-розшукової діяльності та підтримки прийняття рішень (Ricas), який було розроблено співробітниками Управління інформаційного забезпечення ГУ НПУ в Харківській області спільно з місцевими ІТ-компаніями. Система є надбудовою над існуючими інформаційними системами НП України. Головною особливістю системи є візуалізація на географічній карті інформації НП України з її подальшим аналізом. Фактично це геоінформаційна аналітична система НП України. Інструментарій системи

«RICAS» базується на математичних моделях і методах інтелектуального семантичного аналізу, візуального темпорального аналізу, аналізу поведінкового профілю, аналізу прихованих закономірностей. RICAS дозволяє виконувати наступні види аналізу:

- аналіз кримінальної обстановки;
- аналіз конкретного розслідування;
- порівняльний аналіз;
- аналіз групової злочинності;
- аналіз розслідувань.[2].

Подібні системи були впроваджені і ефективно працювали і в інших регіонах країни. Визнаючи позитивний вплив відеоспостереження на результати роботи правоохоронців і сфері забезпечення громадського порядку і безпеки, необхідно звернути увагу і на ризики, які воно породжує. В першу чергу це стосується правових підстав впровадження і використання масового відеоспостереження, а також юридичного статусу матеріалів, які отримані в його результаті. Також, загально визнаним є факт, що масове відеоспостереження призводить до обмеження цілого ряду громадянських прав і свобод, таких як право на приватність, конфіденційність персональних даних тощо. Отже, при запровадженні відеоспостереження, зокрема з технологією розпізнавання обличчя (FRT), в громадських місцях для підтримання правопорядку, пошуку злочинців і для інших цілей, правоохоронні органи зобов'язані посилатися на конкретний нормативний акт. Українське законодавство прямо не відносить зображення обличчя до персональних даних, які є захищеними на законодавчому рівні. Тому, на відміну від адміністрування паспортних даних, адміністратори систем відеоспостереження не мають значного інтересу у захисті такої інформації. До того ж, Державна служба спецв'язку та захисту інформації зазначає, що відсутність статусу персональних даних призводить до ситуації, коли вимога атестації систем незастосовна, якщо вона збирає зображення обличчя особи чи номеру її транспортного засобу. Тому вважаємо необхідним звернутися до стандартів ЄС, які визначають критерії пропорційності і необхідності використання цієї технології в діяльності поліції [3], [4]. Зокрема вони розрізняють терміни: «необхідна обробка», «суворо необхідність», «вкрай необхідна» тощо. Так, стаття 10(1) Директиви «Про захист персональних даних» встановлює, що використання FRT повинно бути «суворо необхідним». Згідно зі статтею 29, це означає «передбачити точні та особливо вагомні обґрунтування для обробки таких даних» (Article 29 Data Protection Working Party, 2017, с. 8). Завдяки масовому невибіркового нагляду за допомогою відеоспостереження в громадських місцях немає анонімності. Кожна людина може стати підозрюваною і навіть випадкова поведінка (наприклад, носіння великих сонцезахисних окулярів) може вважатися підозрою. З цього приводу Європейська організація, спрямована на захист прав і свобод в Інтернеті (EDRI) висловила наступним чином: «Захід, який передбачає постійне спостереження в режимі реального часу, особливо

пов'язане з обробкою конфіденційних даних спеціальної категорії, таких як біометричні дані обличчя ... сам по собі порушує суть основних прав... і, таким чином, буде несумісним із законодавством ЄС (...) Масове стеження за своєю природою є фундаментальним порушенням основних прав: це зазіхає на саму суть конфіденційності, захисту даних та інших прав» [5] З цих причин втручання в конфіденційність, які впроваджують (або можуть перерости в) масове стеження, неодноразово відхилялися в ЄС.

Сьогодні в Європі є вже десятки документів, направлених на регулювання питань, пов'язаних зі штучним інтелектом і окремими його технологіями, такими як відеоспостереження і FRT. В Україні, на жаль, діє тільки один спеціальний нормативний акт в цій сфері – «Концепція розвитку штучного інтелекту в Україні» [6], що є недостатнім для правомірного впровадження та застосування технологій ШІ у правоохоронній діяльності тому що встановлює лише загальні засади та принципи розвитку ШІ в нашій країні. Проблема правомірності встановлення і застосування апаратних комплексів систем відеоспостереження ще й в тому, що в країні немає жодного нормативного акту, який передбачає право якогось державного органу влади або місцевого самоврядування використовувати технології для масового нагляду за життям громадян. Як показує практика, переважна більшість таких систем перебуває на балансі органів місцевого самоврядування або комунальних підприємств. Але проблема полягає у тому, що на сьогодні у місцевої влади немає правових підстав встановлювати технічні засоби відеонагляду, не кажучи вже про доступ до баз даних інших органів, наприклад, для впровадження функції розпізнавання обличчя. У кожному регіоні місцева влада самостійно ухвалює рішення щодо обробки відеопотоків, використовуючи пристрої з різним програмним забезпеченням та технічними характеристиками. Таке різноманіття в обладнанні суттєво ускладнює спроби інтегрувати муніципальні відеосистеми в мережу інформаційних систем, які використовує Національна поліція. По-друге, доступ правоохоронців до обробки відеозаписів, у більшості випадків, не можливий без попереднього отримання дозволу від власника систем – органів місцевого самоврядування, які не мають єдиного підходу щодо надання правоохоронцям можливості користуватися масивом інформації. У деяких громадах порядок доступу поліцейських до відеоданих встановлюється актами органів місцевого самоврядування, в інших – взагалі не регламентується й залежить від усталеної практики взаємин місцевих чиновників з правоохоронцями [7,с.17].

В свою чергу, правоохоронні органи мають право вести відеоспостереження лише за окремими громадянами на підставах і в порядку, визначених в Законі України «Про оперативно-розшукову діяльність». Таким чином, законодавча неузгодженість в регулюванні цього питання призводить до «конфлікту інтересів» і зниження рівня громадської безпеки.

На наш погляд, встановлення і використання систем відеоспостереження в громадських місцях, на дорогах, в громадському транспорті має бути у підпорядкуванні правоохоронних органів. Чинне законодавство потребує прийняття спеціального нормативного акту щодо підстав, принципів і процедур впровадження і застосування ІКТ в діяльності правоохоронних органів, окремим розділом якого має стати використання відеоспостереження в громадських місцях, в тому числі і технології FRT.

Бібліографічні посилання

1. Про Національну поліцію: Закон України // Відомості Верховної Ради (ВВР), 2015, № 40-41, ст.379. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text> (дата звернення: 08.05.25). (дата звернення: 15.04.25).
2. Інформційний ресурс. <https://ricas.org/uk/>
3. Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. URL: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en.
4. EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data. URL: https://www.edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf
5. EDRI (2020). Заборона біометричного масового спостереження (набір вимог до Європейської комісії та держав-членів ЄС щодо основних прав), 13 травня 2020 р. URL: <https://edri.org/our-work/blog-ban-biometric-mass-surveillance/>.
6. Розпорядження Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. «Про схвалення Концепції розвитку штучного інтелекту в Україні». URL: <https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text>
7. Відеоспостереження у публічних місцях: основи захисту персональних даних (посібник для органів місцевого самоврядування) / В.К. Батчаєв, У.С. Шадська. – К.: Компринт, 2021. – 98 с. URL: https://umdp.info/wp-content/uploads/2021/09/POSIBNYK_videosposterezhennya_u_publichnyh_miscyax.pdf

D. Koluznyj

Problems of legal regulation of the use of video surveillance systems by law enforcement authorities.

Abstract: Video surveillance has always been a critical component of law enforcement and public safety in the work of law enforcement agencies. Images and audio from video surveillance recordings play an important role in detecting crimes, identifying potential witnesses, identifying and/or eliminating suspects, and identifying potential investigative opportunities, such as the timeline of events and additional sources of video surveillance data. As of today, there are problems with the legal regulation of the installation of video surveillance systems both on the part of local authorities and law enforcement agencies. The Laws of Ukraine 'On Local Self-Government in Ukraine' and 'On the National Police', as well as other relevant regulations, do not provide for direct powers to install surveillance technologies. Thus, the introduction and use of video surveillance systems in law enforcement requires special regulatory regulation and specification.

Keywords: video surveillance systems, law enforcement, information security, personal data, face recognition technology.

Зразок для цитування:

Калужний Д. Проблеми правового регулювання використання систем відеоспостереження правоохоронними органами. Пропілії права та безпеки, 2025. №6-7. С. 65-67. DOI: <https://doi.org/10.32620/pls.2025.67.16>.