Погорецький Микола Миколайович
начальник наукової лабораторії
науково-організаційного центру
Національної академії Служби безпеки
України, кандидат юридичних наук,
старший дослідник

ТАЄМНЕ СПОСТЕРЕЖЕННЯ В ДЕМОКРАТИЧНОМУ СУСПІЛЬСТВІ: БАЛАНС МІЖ БЕЗПЕКОЮ І ПРАВАМИ ЛЮДИНИ

Негласні розслідування є важливим інструментом забезпечення безпеки, проте їх застосування в Україні супроводжується серйозними проблемами. Серед основних – формальний характер судового контролю, слабкий прокурорський нагляд, відсутність незалежного моніторингу та чітких стандартів щодо новітніх технологій (штучного інтелекту, біометрії тощо). Це створює ризики зловживань і порушень прав людини, зокрема права на приватність. На відміну від багатьох країн Європи, в Україні також відсутній механізм компенсації за незаконне застосування негласних заходів. Ситуація потребує негайного вдосконалення законодавства, посилення контролю та запровадження незалежного нагляду відповідно до міжнародних стандартів.

Термін «негласне розслідування» злочинів є поширеним серед зарубіжних та вітчизняних фахівців. В кожній із країн, у тому числі й в Україні, цей термін має свою історію становлення та розвитку і як наслідок – свій зміст. Нерідко поряд з терміном «негласне розслідування» зарубіжними фахівцями вживаються як синоніми також і такі терміни як «конфіденційне розслідування», «таємне розслідування», «розслідування під прикриттям» тощо.

Розвиток інформаційних технологій сприяв значному розширенню можливостей негласного розслідування. У 1978 році в США було прийнято Закон про зовнішню розвідку (FISA) [1], який встановив правові рамки для перехоплення електронних комунікацій у розвідувальних цілях. У Великобританії у 2000 році набув чинності Закон про регулювання слідчих повноважень (RIPA) [2], який визначив

порядок використання негласного спостереження правоохоронними органами. Наприкінці XX – на початку XXI століття цифрові технології відкрили нові можливості для негласних розслідувань, включаючи кіберспостереження, аналіз великих даних та використання штучного інтелекту.

У правоохоронній сфері негласне розслідування включає приховане спостереження та використання агентів під прикриттям для збору доказів про злочинну діяльність. Згідно з документом «Практичні кодекси таємного спостереження та таємних джерел розвідувальної інформації» («Covert Surveillance and Covert Human Intelligence Sources Codes of Practice») [3], такі методи є важливими для захисту громадськості від тероризму та злочинності, але потребують ретельного нагляду та регулярної переоцінки, щоб забезпечити їх обґрунтованість та законність.

Негласне розслідування – це приховане збирання інформації правоохоронними органами про осіб чи події, що мають значення для кримінального провадження або національної безпеки. Воно здійснюється без відома об'єкта, з використанням спеціальних методів, технічних засобів і оперативно-розшукових заходів. Наприклад, це може бути робота таємного агента або встановлення прихованого аудіо- та відеоспостереження. Через втручання в приватне життя, таке розслідування проводиться лише за наявності законних підстав і з дозволу уповноважених органів, що забезпечує захист прав людини.

Ці методи тісно пов'язані з розвідувальною діяльністю, оскільки обидві форми роботи спрямовані на отримання прихованої інформації. Методи розвідки включають технічну розвідку (супутниковий моніторинг, кіберрозвідка), сигнальну розвідку (SIGINT), що охоплює перехоплення електронних комунікацій, гуманітарну розвідку (HUMINT) – вербування агентів, а також кіберрозвідку (CYBINT), яка виявляє кіберзагрози та атакує системи супротивника. Наприклад, застосування дронів для виявлення терористичних баз у зонах бойових дій поєднує елементи як технічної розвідки, так і негласного спостереження, ілюструючи ефективність комплексного підходу до забезпечення національної безпеки [4].

Застосування негласних методів розслідування породжує серйозні етичні та правові виклики, пов'язані з втручанням у приватне життя. У західних країнах такі заходи суворо регламентовані законом. Наприклад, у Німеччині заборонено вилучати документи, що стосуються правової чи медичної допомоги, крім випадків їх використання для вчинення злочину. У Швейцарії особиста кореспонденція підозрюваного може бути недоторканною, якщо інтереси захисту переважають інтереси слідства. Використання таких матеріалів у суді можливе лише за умови їх законного отримання. Водночас навіть у таких системах трапляються зловживання, що свідчить про важливість ефективного контролю за застосуванням негласних методів.

Програма PRISM, розкрита Едвардом Сноуденом у 2013 році, показала, що Агентство національної безпеки (АНБ) США масово збирало дані громадян без їхнього відома. Це включало доступ до серверів таких технологічних гігантів, як Google, Apple та Facebook, що дозволяло АНБ відстежувати електронні листи, чати та інші комунікації користувачів. Ці дії викликали значний суспільний резонанс та дискусії щодо приватності та державного нагляду [5].

У січні 2025 року News Group Newspapers, видавець The Sun, визнав незаконні дії та приніс «повне та беззастережне вибачення» принцу Гаррі за серйозне втручання в його приватне життя в період з 1996 по 2011 роки. Це стало результатом п'ятирічної судової боротьби, під час якої принц Гаррі наполягав на відповідальності за незаконне збирання інформації. Вибачення також стосувалося втручання в приватне життя його покійної матері, принцеси Діани. Цей випадок став важливим прецедентом у боротьбі за відповідальність медіа за незаконні методи збору інформації [6].

Ці події підкреслюють серйозність проблеми незаконного використання негласного спостереження та необхідність суворого контролю за діяльністю медіа та правоохоронних органів у цій сфері.

У сучасній Європі питання правового контролю за негласними розслідуваннями набуває особливої актуальності. Це пов'язано з необхідністю забезпечення балансу між

ефективністю правоохоронної діяльності та захистом фундаментальних прав людини, зокрема права на приватність.

Європейські стандарти у цій сфері акцентують увагу на процесуальних гарантіях під час проведення негласних спостережень та захисту даних. Технологічний прогрес останніх років ставить нові виклики у забезпеченні права на повагу до приватного життя та вимагає, щоб будь-яка обробка персональних даних відповідала встановленим стандартам. Зокрема, Рада Європи наголошує на необхідності чіткого регулювання негласного спостереження, забезпечення прозорості процедур та наявності ефективних механізмів контролю за такими діями [7].

ЄСПЛ послідовно наголошує, що втручання у приватне життя під час негласного розслідування має бути законним, обґрунтованим і пропорційним. Європейські стандарти вимагають судового контролю за такими діями та регулярного моніторингу їх застосування для запобігання зловживанням і порушенням прав людини [8].

Отже, негласні розслідування є важливим інструментом забезпечення національної безпеки, боротьби з тероризмом, корупцією та злочинністю. Водночас їх застосування без належного контролю може призвести до порушень прав людини, зловживань владою та послаблення демократичних інститутів. Ефективність негласних розслідувань залежить від дотримання принципів законності, необхідності, пропорційності та контролю.

Законодавство демократичних держав передбачає механізми нагляду, проте навіть у США, Великобританії та ЄС зберігаються ризики зловживань, що підтверджують міжнародні скандали, пов’язані з масовим стеженням.

Забезпечення демократичного контролю, вдосконалення правового регулювання та впровадження міжнародних стандартів, зокрема практики ЄСПЛ та Ради Європи, сприятимуть зміцненню правової держави, підвищенню довіри громадян та мінімізації ризиків зловживань.

Список використаних джерел

1. Foreign Intelligence Surveillance Act 1978 (FISA) // U.S. Congress. Washington, D.C.: U.S. Government, 1978. Available at: https://uscode.house.gov/view.xhtml?path=/prelim@title50/chapter36.

2. Regulation of Investigatory Powers Act 2000 (RIPA) // UK Legislation. London: HM Government, 2000. Available at: https://www.legislation.gov.uk/ukpga/2000/23/contents.

3. Covert Human Intelligence Sources Code of Practice 2022. GOV.UK, 13 Dec. 2022, https://www.gov.uk/government/publications/covert-human-intelligence-sources-code-of-practice-2022.

4. National Security Agency. Signals Intelligence (SIGINT) Overview. Fort Meade: NSA, 2021. Available at: https://www.nsa.gov/Signals-Intelligence/Overview/.

5. MacAskill, Ewen; Poitras, Laura; Greenwald, Glenn. NSA Prism program taps in to user data of Apple, Google and others. The Guardian. 7 червня 2013. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

6. Prince Harry says Sun publisher made ‘historic admission’ as he settles case. The Guardian. 22 January 2025. https://www.theguardian.com/uk-news/2025/jan/22/prince-harry-says-sun-publisher-made-historic-admission-as-he-settles-case.

7. Council of Europe Data Protection website. Council of Europe. https://www.coe.int/en/web/data-protection.

8. Князєв С. М. Судовий контроль за здійсненням негласної діяльності: міжнародний досвід. Юридичний журнал Національної академії внутрішніх справ. 2019. № 1 (17). С. 90–97. URL: https://lawjournal.com.ua/uk/article/read/sudovy-kontrol-za-zdiysnennyam-neglasnoyi-diyalnosti-mizhnarodny-dosvid.