ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

УДК 343.137.5
DOI https://doi.org/10.32782/2709-9261-2024-4-12-1

Груздь Олександр Іванович,
кандидат юридичних наук,
старший викладач кафедри кримінального процесу та криміналістики факультету № 1
(Донецький державний університет внутрішніх справ, м. Кропивницький)
ORCID: https://orcid.org/0000-0003-0370-3791

Квашук Олександр Дмитрович,
кандидат юридичних наук,
викладач кафедри кримінального процесу та криміналістики факультету № 1
(Донецький державний університет внутрішніх справ, м. Кропивницький)
ORCID: https://orcid.org/0009-0008-5969-4576

Воробйов Максим Валерійович,
курсант факультету № 1
(Донецький державний університет внутрішніх справ, м. Кропивницький)
ORCID: https://orcid.org/0009-0008-2992-1547

ПРАВОВЕ РЕГУЛЮВАННЯ ТА ЕТИЧНІ АСПЕКТИ ВИКОРИСТАННЯ IMSI-CATCHER

У статті розкрито сутність IMSI-catcher як технічного засобу, здатного ідентифікувати мобільні пристрої та маніпулювати мобільним зв'язком, що становить загрозу конфіденційності користувачів. Досліджено міжнародні та національні підходи до правового регулювання застосування цих пристроїв, зокрема органами Національної поліції України, їхній вплив на права, гарантовані Європейською конвенцією з прав людини. Зроблено висновок про необхідність чіткого правового регулювання та розроблення етичних стандартів для запобігання зловживанням і забезпечення прозорості використання IMSI-catcher.
Ключові слова: *права людини, Європейський суд, Національна безпека, цифровізація, зловживання службовим становищем.*

Постановка проблеми. Несанкціоноване використання IMSI-catcher у репресивних цілях, зокрема під час масових зібрань і протестів, є негативним явищем для суспільства, що порушує права людини. Технологічні аспекти, які уможливлюють зловживання та вплив на право на приватність і свободу зібрань, які будуть застосовані з метою чіткого правового регулювання та розроблення етичних стандартів для запобігання зловживанням і забезпечення прозорості використання IMSI-catcher.

Аналіз останніх досліджень та публікацій. Питання, пов'язані з механізмом використання правоохоронними органами в Україні спеціального технічного засобу, який дозволяє перехоплювати ідентифікаційні номери мобільних пристроїв – IMSI-catcher натепер не було широкомасштабно досліджено вітчизняними вченими, але окремі аспекти захисту мобільних телефонних засобів зв'язку розглядали А. Барсук, А. Берцюк, С. Онищук, Л. Скачек, М. Частокол та інші. Проте значну увагу особливостям використання IMSI-catcher, а також проблемним питанням, пов'язаним із порушеннями прав люди, приділяли науковці країн Європейського Союзу та Сполучених Штатів Америки, як-от П. Алрашед, Р. Бернс, К. Керім, Т. Камер, М. Нартіджарві.

Мета статті. Проведення комплексного аналізу ризиків використання IMSI-catcher для непрозорого стеження, визначення правових і етичних аспектів їх застосування з метою захисту прав людини.

Виклад основного матеріалу. З розвитком мобільних технологій значно зросла потреба в захисті особистих даних користувачів. Однією із сучасних загроз конфіденційності є IMSI-catcher – спеціальний технічний засіб, який дозволяє перехоплювати ідентифікаційні номери мобільних пристроїв (IMSI) та маніпулювати мобільним зв'язком, ставить під загрозу конфіденційність і безпеку мобільних пристроїв і їх користувачів [1]. Винахід і застосування цих пристроїв, спочатку призначених для правоохоронних органів і розвідувальних служб, стали предметом серйозних правових і етичних дискусій у всьому світі.

Зазвичай правоохоронні органи для перехоплення комунікацій покладаються на телекомунікаційних провайдерів, які зобов'язані надавати доступ до своїх мереж відповідно до законодавства. Проте телекомунікаційні компанії менш зацікавлені у співпраці із владою через витрати на адаптацію своїх систем. Законодавство, яке змушує операторів сприяти перехопленню даних, виконує ще одну важливу функцію – законодавчо закріплює втручання у приватне життя. Європейський суд з прав людини (далі – ЄСПЛ) наголошує, що будь-яке втручання у приватність повинно мати чітку правову основу та бути передбачуваним для громадян [2].

Водночас IMSI-catcher здатен працювати автономно, без участі телекомунікаційних операторів, що створює ризики несанкціонованого використання для моніторингу громадян, зокрема під час масових заходів, протестів або поблизу урядових установ. Це викликає занепокоєння щодо потенційного використання IMSI-catcher у репресивних цілях, особливо у країнах з обмеженими демократичними свободами. В Україні й у всьому світі проблема використання IMSI-catcher стає дедалі актуальнішою через стрімкий розвиток технологій і відсутність чіткого правового регулювання, що робить її серйозною правовою дилемою, яка потребує комплексного аналізу.

Як уже зазначалося, IMSI-catcher – це пристрій, призначений для збору даних, зокрема ідентифікаторів абонентів зв'язку (IMSI), що дозволяє взаємодіяти з мобільним зв'язком і маніпулювати ним. IMSI (International Mobile Subscriber Identifier – міжнародний ідентифікатор абонента мобільного зв'язку) – це номер із 14–15 цифр, який ідентифікує абонента мобільного зв'язку за його SIM-карткою. Він складається з кількох частин, включаючи код країни, код мережі й індивідуальний набір цифр, що ідентифікує кожну конкретну SIM-картку в мережі. Цей унікальний номер зберігається на SIM-картці та залишається незмінним навіть у разі перенесення номера на іншу SIM-картку. Це дозволяє мобільним операторам перевіряти IMSI абонента, що допомагає зменшити кількість випадків шахрайства зі зміною SIM-карт [3].

Отже, IMSI – це спеціальний код, який допомагає оператору мобільного зв'язку розпізнати ваш пристрій у мережі. Він зберігається на SIM-картці й використовується щоразу, коли ви телефонуєте, надсилаєте повідомлення або користуєтеся мобільним інтернетом. IMSI є важливим для забезпечення доступу до послуг оператора й ідентифікації користувача в мережі. По суті, це як «паспорт» вашого телефона, який дозволяє мережі знати, що ви – це ви.

IMSI-catcher є потужним інструментом для відстеження та контролю за громадянами під час масових заходів, як-от протести та демонстрації, що показує значну проблематику у сфері забезпечення фундаментальних прав людини, особливо актуально в умовах зростання соціальної напруги. Водночас цей пристрій має значний потенціал для гарантування громадської безпеки та протидії тероризму. У разі відповідного регулювання та прозорого використання технологія перехоплення може сприяти ідентифікації підозрілих осіб і запобіганню загрозам під час масових зібрань, забезпечувати своєчасну реакцію державних органів на потенційні небезпеки для захисту мирних громадян.

IMSI-catcher робить це, «прикидаючись» вишкою мобільного зв'язку –обманом змушує телефон користувача підключитися до IMSI-ловця, а потім розкриває персональні дані користувача телефона без його відома. Це дозволяє владі ідентифікувати учасників зібрань і фіксувати інформацію про їхнє місцезнаходження та пересування, несанкціоновано збирати особисті дані громадян [4].

Одним із негативних прикладів є використання IMSI-catcher для моніторингу протестів і масових зібрань, що зумовлює значне занепокоєння серед громадськості та правозахисних організацій. У багатьох країнах питання прозорості використання цієї технології правоохоронними органами залишається невирішеним. Натепер немає публічної дискусії щодо обсягу та характеру використання урядових уловлювачів IMSI, зокрема й щодо того, наскільки цей метод спостереження втручається у права людини в демократичному суспільстві [4].

Одним із характерних випадків використання технології перехоплення є подія в Чикаго, коли активісти заявили про використання поліцією технології "Stingray" для стеження за протестувальниками. Як повідомляє Майк Краузер із WBBM (WBBM – позивний код радіостанції *Newsradio,* 780 AM & 105.9 FM, у Чикаго), активісти, що брали участь у протестах, надали докази того, що їхні телефонні розмови могли бути перехоплені поліцією. Stingray створює бар'єр між телефоном користувача та мобільною вежею, змушує телефони в зоні дії підключатися не до провайдера, а безпосередньо до пристрою стеження, що дозволяє поліції отримувати

інформацію про місцезнаходження та комунікації користувачів. Активісти опублікували фотографії автомобіля міської ради Чикаго з радаром на даху, який, на їхню думку, використовувався для моніторингу протестувальників. Цей випадок став ще більш очевидним у жовтні, коли департамент поліції Чикаго визнав, що придбав пристрої для перехоплення мобільних телефонів, зокрема й IMSI-ловці, ще у 2008 р., під різними назвами, як-от Stingray [5].

Можемо припускати, що у країнах з обмеженими демократичними свободами IMSI-catcher стане інструментом для контролю за політичною активністю та відстеження учасників мирних зібрань. Залучаючи всі мобільні телефони в межах свого діапазону, цей пристрій заманює їх до підключення та змушує передавати дані IMSI та міжнародний ідентифікатор мобільного обладнання (IMEI). Це дозволяє легко ідентифікувати учасників протестів, що порушує права на свободу вираження й асоціацій, гарантовані міжнародним правом [6].

Протиправне використання IMSI-catcher не лише державою, а й правопорушниками створює значні ризики для безпеки мобільних користувачів, оскільки ці пристрої можуть змусити мобільні телефони підключатися до підроблених базових станцій, що відкриває широкий спектр можливостей для атак.

За словами А. Барсука, такі атаки можуть включати різні види загроз, як-от:

– підміна SMS;
– розкриття розташування абонента;
– порушення доступності абонента;
– перехоплення вхідних SMS-повідомлень;
– прослуховування вихідних дзвінків [6].

Використання IMSI-catcher органами Національної поліції України регламентується чинним законодавством, зокрема законами України «Про Національну поліцію» та «Про оперативно-розшукову діяльність», а також Кримінальним процесуальним кодексом України (далі – КПК). Це обладнання використовується для цілей оперативно-розшукової діяльності або в межах кримінального провадження.

Згідно з національним законодавством України, дії, пов'язані з незаконним використанням IMSI-catcher, можуть бути кваліфіковані за кількома статтями Кримінального кодексу України (далі – КК України).

По-перше, незаконні дії з використанням IMSI-catcher можуть бути кваліфіковані за ст. 361 КК України, за ознаками несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Норми даної статті передбачають відповідальність за будь-які несанкціоновані дії, які призводять до порушення роботи телекомунікаційних систем [7].

По-друге, у ст. 359 КК України передбачено кримінальну відповідальність за незаконне придбання, збут або використання спеціальних технічних засобів негласного отримання інформації [7]. Оскільки IMSI-catcher є технічним засобом для негласного збору даних про абонентів мобільного зв'язку, його незаконне використання або продаж можуть підпадати під ознаки об'єктивної сторони цієї статті.

По-третє, у ст. 182 КК України передбачено відповідальність за порушення недоторканності приватного життя [7]. Збір конфіденційних даних за допомогою IMSI-catcher, як-от відстеження місцезнаходження або перехоплення комунікацій без згоди особи, є серйозним порушенням права на приватність, відповідно до чого підпадає під дію зазначеної статті.

З погляду Конвенції з прав людини і основоположних свобод використання таких пристроїв, як IMSI-catcher, викликає численні питання щодо порушення приватності, законності та прав людини. Варто розглянути нормативні вимоги до їх застосування, особливо в контексті відповідності вимогам міжнародного права.

Використання таких технологій дозволяє органам правопорядку відстежувати мобільні пристрої та збирати метадані, як-от ідентифікатори абонентів. Відповідно до вимог ст. 8 Конвенції з прав людини і основоположних свобод, втручання у приватне життя може бути допустимим лише за умови відповідності законним цілям, якщо воно ґрунтується на національному законодавстві та забезпечує необхідні гарантії проти можливих зловживань [8].

Важливим аспектом у розгляді правового статусу таких технологій є необхідність забезпечення передбачуваності та прозорості законодавства. У 1984 р. ЄСПЛ ухвалив рішення в першій справі, що стосувалася комунікацій.

Так, справа «Малоун проти Сполученого Королівства» стосувалася використання методу під назвою «прослуховування» британською поліцією, коли поліцейські органи отримували від телефонної компанії інформацію про номери, на які телефонував визначений абонент, а також про тривалість дзвінків. ЄСПЛ встановив, що доступ уряду до такого роду інформації про комунікації є обмеженням ст. 8 Конвенції в тому ж сенсі, що й доступ до змісту комунікацій, тому це вимагало законодавчого підґрунтя. Тобто ЄСПЛ підкреслив, що закони, які дозволяють спостереження, повинні бути чіткими і зрозумілими для осіб, яких вони стосуються. Це означає, що законодавство має чітко регулювати, за яких умов і в яких межах може здійснюватися таке втручання, щоб не допустити свавілля з боку державних органів [9].

Однак на практиці законодавчі акти, що стосуються використання таких технологій, часто є не досить деталізованими. Наприклад, у Швеції застосування таких технологій довгий час не було чітко регламентоване законом і спиралося на внутрішні принципи. У зв'язку із цим у шведському законодавстві використовувався принцип «ефір вільний», який стверджував, що радіозв'язок не підлягає особливому захисту конфіденційності. Це ставило Швецію в невигідне становище з погляду відповідності європейським нормам, як-от Директива 2002/58/ЄС Європейського парламенту і Ради ЄС від 12 липня 2002 р. про обробку персональних даних і захист конфіденційності в секторі електронних комунікацій, яка встановлює вимоги до захисту комунікаційних даних [11].

Принцип «ефір вільний» означає, що радіочастоти можуть вільно використовуватися без спеціальних обмежень щодо конфіденційності комунікацій. Це дозволяло державним органам використовувати технології для спостереження без додаткових правових гарантій захисту персональних даних. Такий підхід не враховує сучасних вимог до приватності, адже радіокомунікації, які колись вважалися публічними, тепер часто містять важливу приватну інформацію. Тому застосування цього принципу без належного правового регулювання підриває захист прав на конфіденційність і ставить під сумнів законність таких дій у світлі міжнародних правових стандартів.

У контексті міжнародного права IMSI-ловушки стають предметом серйозного аналізу, оскільки їх ви-

користання може порушувати права, гарантовані не лише національними законами, але й міжнародними угодами. Наприклад, окрім Конвенції про захист прав людини і основоположних свобод, застосування таких технологій повинно відповідати вимогам Міжнародного пакту про громадянські і політичні права, ухваленого 16 грудня 1966 р., який також передбачає захист права на приватне життя та свободу вираження думок. Будь-яке втручання в ці права має бути обґрунтованим, пропорційним і забезпеченим належними процесуальними гарантіями, як зазначено у ст. 17 цього Пакту [11].

Окрім того, варто зазначити, що використання IMSI-catcher у різних юрисдикціях може підпадати під різні правові режими. У державах – членах ЄС дія Директиви 2002/58/ЄС Європарламенту і Ради від 12 липня 2002 р. про обробку персональних даних і захист конфіденційності в секторі електронних комунікацій забезпечує деякий захист даних громадян. Однак в інших регіонах цей захист може бути слабшим або взагалі відсутнім [11]. Це порушує питання про необхідність створення загальносвітових стандартів щодо використання зазначених технологій, які могли б уніфікувати підходи до захисту прав людини в умовах глобальної цифровізації [11].

У висновку ми можемо зазначити, що стрімкий розвиток технологій, як-от IMSI-catcher, ставить перед суспільством серйозні виклики у сфері правового й етичного регулювання приватності. Здатність цих пристроїв автономно працювати поза межами контролю телекомунікаційних операторів загострює питання про можливості несанкціонованого моніторингу громадян, зокрема під час масових зібрань і протестів. У країнах з обмеженими демократичними свободами або неналежною правовою базою IMSI-catcher може стати інструментом репресій, порушувати права на свободу вираження думок і мирних зібрань, що є фундаментальними для демократичного суспільства.

Технологія IMSI-catcher не лише дозволяє перехоплювати ідентифікаційні дані, але й потенційно відкриває шлях для серйозних порушень приватного життя громадян. Втручання в особисте життя, яке не є прозорим і підзвітним, може створити атмосферу страху і невизначеності в суспільстві, ставити під загрозу право громадян на захист їхніх особистих даних. Неврегульоване використання таких засобів може призвести до зловживань, коли приватні дані громадян збираються і використовуються без відповідного обґрунтування та контролю. Отже, правове регулювання використання IMSI-catcher є необхідним для забезпечення законності та прозорості, запобігання порушенням прав людини і зловживанням з боку державних органів.

З огляду на це ми пропонуємо такі рекомендації щодо правового регулювання й етичних стандартів використання IMSI-catcher:

– по-перше, розробити чіткі правові норми та стандарти для обмеження використання IMSI-catcher під час масових заходів і протестів. Пристрій має здатність відстежувати місцезнаходження учасників протестів та ідентифікувати конкретний пристрій, що може використовуватися для впливу на мирні збори та свободу вираження думок. Правові норми та стандарти повинні обмежувати використання цієї технології до виняткових випадків, коли є явна загроза громадському порядку чи безпеці, з обов'язковою умовою використовувати лише за визначених обставин, які будь передбачені у стандартах і нормах. Це забезпечить належний баланс між вимогами безпеки та захистом прав людини, зокрема на свободу висловлювання та зібрань;

– по-друге, установлення етичних стандартів, що забороняють використання IMSI-catcher або подібних пристроїв у політичних цілях або для досягнення власних інтересів, а також унеможливлюють їх застосування проти мирних зібрань. IMSI-catcher не повинен використовуватися для стеження за політичними опонентами чи контролю над учасниками мирних протестів. Етичні стандарти мають передбачати повагу до приватного життя громадян, що унеможливить використання IMSI-catcher для політичного тиску або маніпуляцій.

Заборона застосування цих технологій для політичних цілей стане важливим кроком на шляху до захисту прав людини в умовах розвитку нових технологій.

Висновки. Правове регулювання й етичні стандарти використання технологій на кшталт IMSI-catcher є надзвичайно важливими для захисту прав людини, зокрема права на приватність, свободу зібрань і вираження думок. Створення чітких правових норм і обмежень на використання IMSI-catcher дозволить захистити громадян від потенційних зловживань і незаконного втручання в особисте життя. Важливим аспектом є також дотримання етичних принципів, які унеможливлять використання таких технологій для політичного тиску або контролю над громадянами. Ці заходи допоможуть зберегти демократичні свободи, досягти балансу між вимогами безпеки та правами людини в умовах швидкого розвитку новітніх технологій.

Список використаних джерел

1. Kareem K. M. The impact of IMSI catcher deployments on cellular network security: challenges and countermeasures in 4G and 5G networks. *International journal on recent and innovation trends in computing and communication*. 2023. Т. 11. № 9. https://doi.org/10.7910/DVN/6JPQWO.

2. Міжнародний пакт про громадянські і політичні права : Пакт ООН від 16.12.1966 р., станом на 19.10.1973 р. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text (дата звернення: 17.10.2024).

3. IMSI (international mobile subscriber identifier). *GMS AI-driven communications solutions partner*. URL: https://www.gms.net/glossary/imsi/ (дата звернення: 14.10.2024).

4. Privacy International. IMSI catchers legal analysis. London : Privacy International, 2020. URL: https://privacyinternational.org/report/3965/imsi-catchers-pis-legal-analysis (дата звернення: 06.11.2024).

5. Activists say chicago police used "stingray" eavesdropping technology during protests. *CBS News – Breaking news, 24/7 live streaming news & top stories*. URL: https://www.cbsnews.com/chicago/news/activists-say-chicago-police-used-stingray-eavesdropping-technology-during-protests/ (дата звернення: 08.11.2024).

6. Барсук А. Методи та засоби захисту мобільних телефонних засобів зв'язку. *ElAr.* URL: https://openarchive.nure.ua/entities/publication/86e34618-dc27-4d17-8eb6-b667e0c316c9 (дата звернення: 14.10.2024).

7. Кримінальний кодекс України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 14.10.2024).

8. Конвенція про захист прав людини і основоположних свобод : Конвенція Ради Європи від 04.11.1950 р., станом на 01.08.2021 р. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 15.10.2024).

9. Рішення Європейського суду з прав людини від 02.08.1984 р. у справі № 8691/79. URL: https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-57533%22]} (дата звернення: 16.10.2024).

10. Naarttijärvi M. Swedish police implementation of IMSI-catchers in a European law perspective. *Computer law & security review*. 2016. Т. 32. № 6. https://doi.org/10.1016/j.clsr.2016.07.006.

11. Директива Європейського парламенту і Ради 2009/136/ЄС від 25 листопада 2009 р. про внесення змін до Директиви 2002/22/ЄС про універсальну послугу та права користувачів щодо електронних комунікаційних мереж та послуг, Директиви 2002/58/ЄС про опрацювання персональних даних і захист приватності у сфері електронних комунікацій, Регламенту (ЄС) № 2006/2004 про співпрацю між національними органами : Директива Європ. Союзу від 25.11.2009 р. № 2009/136/ЄС. URL: https://zakon.rada.gov.ua/laws/show/984_013-09#Text (дата звернення: 08.11.2024).

References

1. Kareem, K. M. (2023). The impact of IMSI catcher deployments on cellular network security: challenges and countermeasures in 4G and 5G networks. *International journal on recent and innovation trends in computing and communication.* T.11. № 9. Retrieved from: https://doi.org/10.7910/DVN/6JPQWO [in English].

2. Konventsiia pro zakhyst prav liudyny i osnovopolozhnykh svobod (z protokolamy) [Convention on the Protection of Human Rights and Fundamental Freedoms]. Retrieved from: https://zakon.rada.gov.ua/laws/show/995_004#Text (data zvernenya: 14.10.2024) [in Ukrainian].

3. IMSI (international mobile subscriber identifier). *GMS AI-driven communications solutions partner*. Retrieved from: https://www.gms.net/glossary/imsi/ (data zvernenya: 14.10.2024) [in English].

4. Privacy International. IMSI catchers legal analysis. Privacy International, 2020, London. Retrieved from: https://privacyinternational.org/report/3965/imsi-catchers-pis-legal-analysis (data zvernenya: 06.11.2024) [in English].

5. Activists say Chicago police used stingray eavesdropping technology during protests. *CBS News – Breaking news, 24/7 live streaming news & top stories*. Retrieved from: https://www.cbsnews.com/chicago/news/activists-say-chicago-police-used-stingray-eavesdropping-technology-during-protests/ (data zvernenya: 08.11.2024) [in English].

6. Barsuk, A. T. Metody ta zasoby zakhystu mobilnykh telefonnykh zasobiv zviazku [Methods and means of protection of mobile telephone communications]. *ElAr.* Retrieved from: https://openarchive.nure.ua/entities/publication/86e34618-dc27-4d17-8eb6-b667e0c316c9 (data zvernenya: 14.10.2024) [in Ukrainian].

7. Kryminalnyi kodeks Ukrainy [Criminal Code of Ukraine]: Zakon Ukrainy vid 05.04.2001 r. № 2341–III (2001). Retrieved from: https://zakon.rada.gov.ua/laws/show/2341-14#Text (data zvernenya: 14.10.2024) [in Ukrainian].

8. Rishennia Yevropeiskoho sudu z prav liudyny vid 02.08.1984 u spravi № 8691/79. Retrieved from: https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-57533%22]} (data zvernenya: 15.10.2024) [in Ukrainian].

9. Naarttijärvi, M. (2016). Swedish police implementation of IMSI-catchers in a European law perspective]. *Computer law & security review*. T. 32. № 6. Retrieved from: https://doi.org/10.1016/j.clsr.2016.07.006 [in English].

10. Mizhnarodnyi pakt pro hromadianski i politychni prava [Covenant of the United Nations] vid 16.12.1966: stanom na 19 zhovtnia 1973 r. Retrieved from: https://zakon.rada.gov.ua/laws/show/995_043#Text (data zvernenya: 17.10.2024) [in Ukrainian].

11. Dyrektyva Yevropeiskoho Parlamentu i Rady 2009/136/IeS vid 25 lystopada 2009 roku pro vnesennia zmin do Dyrektyvy 2002/22/IeS pro universalnu posluhu ta prava korystuvachiv shchodo elektronnykh komunikatsiinykh merezh ta posluh, Dyrektyvy 2002/58/IeS pro opratsiuvannia personalnykh danykh i zakhyst pryvatnosti u sferi elektronnykh komunikatsii, Rehlamentu (IeS) № 2006/2004 pro spivpratsiu mizh natsionalnymy orhanamy: Dyrektyva Yevropeiskoho Soiuzu vid 25.11.2009 № 2009/136/IeS. Retrieved from: https://zakon.rada.gov.ua/laws/show/984_013-09#Text (data zvernenya: 08.11.2024) [in Ukrainian].

Hruzd Oleksandr,
PhD in Law,
Senior Lecturer at Department of Criminal Procedure and Criminology Faculty № 1
(Donetsk State University of Internal Affairs, Kropyvnytskyi)
ORCID: https://orcid.org/0000-0003-0370-3791

Kvashuk Oleksandr,
PhD in Law,
Lecturer at the Department of Criminal Procedure and Criminology Faculty № 1
(Donetsk State University of Internal Affairs, Kropyvnytskyi)
ORCID: https://orcid.org/0009-0008-5969-4576

Vorobyov Maksym,
Cadet of Faculty № 1
(Donetsk State University of Internal Affairs, Kropyvnytskyi)
ORCID: https://orcid.org/0009-0008-2992-1547

LEGAL REGULATION AND ETHICAL ASPECTS OF THE USE OF IMSI-CATCHER

The article analyzes the risks associated with the use of IMSI-catchers for opaque surveillance and examines the legal and ethical aspects of their application to safeguard human rights. It explores the nature of IMSI-catchers as technical tools capable of identifying mobile devices and manipulating mobile communications, posing a threat to user confidentiality. International and national approaches to the legal regulation of such devices are reviewed, with a focus on their impact on rights guaranteed by the European Convention on Human Rights.

The problem of ensuring a balance between the effectiveness of law enforcement and the protection of the constitutional rights of citizens is becoming particularly acute. The use of IMSI-catchers should take place within the framework of clearly defined legal procedures, in compliance with the principles of legality, proportionality and judicial control.

An important aspect is also international experience in legal regulation of the use of such technologies. Studying and adapting the best practices of other countries can contribute to the development of an effective national regulatory system.

Research on this topic is of important practical importance for improving legislation, developing control procedures and ensuring proper protection of citizens' rights when using IMSI-catchers by law enforcement agencies.

Examples of unauthorized use of IMSI-catchers for repressive purposes, particularly during mass gatherings and protests, are discussed. Special attention is given to the technological aspects enabling abuses and their implications for privacy and freedom of assembly. The study concludes that clear legal regulations and ethical standards are essential to prevent misuse and ensure transparency in the use of IMSI-catchers.

Recommendations for improving legislation include restricting the use of these devices to exceptional cases under strict oversight. The importance of adhering to ethical principles, which prohibit the use of such technologies for political repression or violations of democratic freedoms, is emphasized.

Key words: *human rights, European Court, National Security, digitalization, abuse of office.*