УДК 343.132(477):342.7
DOI https://doi.org/10.32782/2709-9261-2026-1-17-10

Романов Віталій Олександрович,
кандидат юридичних наук
(Сумська філія Харківського національного університету внутрішніх справ, м. Суми)
ORCID: https://orcid.org/0000-0002-8569-5723

ПОНЯТТЯ ТА МЕЖІ «ПРИВАТНОГО СПІЛКУВАННЯ» У КРИМІНАЛЬНОМУ ПРОЦЕСІ УКРАЇНИ: ПРОБЛЕМИ ТЛУМАЧЕННЯ СТ. 258 КПК

У статті уточнено зміст і межі поняття «приватне спілкування» у кримінальному процесі України крізь призму ст. 258 КПК. Показано, що приватність визначається не самим каналом зв'язку, а «умовами» передання й зберігання інформації та обґрунтованими очікуваннями конфіденційності учасників. Розглянуто співвідношення цієї норми з конституційними гарантіями та ст. 8 Конвенції про захист прав людини і основоположних свобод. На матеріалі практики ЄСПЛ і підходів Верховного Суду обґрунтовано, що ухвала слідчого судді не забезпечує законності автоматично: значення мають чіткі межі дозволу, доведення субсидіарності та належна фіксація результатів негласних слідчих (розшукових) дій.

Ключові слова: *приватне спілкування, втручання, НСРД, електронні комунікації, судовий контроль, допустимість доказів.*

Постановка проблеми. Втручання у приватне спілкування є одним із найбільш чутливих інститутів кримінального процесу, бо саме тут найчастіше стикаються інтереси розслідування і гарантії прав людини. Стаття 258 КПК закріплює судовий порядок такого втручання та окреслює базові межі понять «спілкування», «приватне спілкування» і «втручання» [1]. Проблема, однак, у тому, що поняття приватності закон формулює через оцінні конструкції – «умови» та «можуть розраховувати». Через це однакові комунікації в різних ситуаціях отримують різну правову оцінку, а межа між «приватним» і «неприватним» виявляється нестабільною [1].

Ця нестабільність особливо помітна в цифровому середовищі. Повідомлення й дзвінки часто зберігаються у третіх осіб – сервісів або провайдерів, супроводжуються метаданими, а доступ до інформації здобувають і негласними заходами, і процесуальними діями щодо пристроїв. У зв'язку з чим часто виникають спори про те, де закінчується судовий дозвіл, чи справді НСРД застосовувалися як виняток, і чи можна вважати отримані відомості допустимими доказами. Саме в таких ситуаціях оціночні категорії ст. 258 КПК застосовуються по-різному – залежно від контексту й аргументації сторін.

Важливо й те, що цифрова комунікація майже завжди має кілька рівнів. Зміст повідомлень поєднується з метаданими (час, ідентифікатори, тривалість), а також із даними, що фізично або логічно розміщені на різних носіях – у пристрої, в обліковому записі, у хмарному середовищі. Це ускладнює просте питання: що саме підпадає під режим «втручання у приватне спілкування» і коли потрібна ухвала слідчого судді [1]. Якщо ці межі не визначити переконливо, судовий контроль може стати формальністю, а не на дієву гарантію.

Аналіз останніх досліджень і публікацій. В українській науці питання приватного спілкування та процесуальних гарантій уже істотно напрацьоване, однак кілька практично значущих вузлів досі залишаються «на межі» теорії та правозастосування. Зокрема: Камінська Н. В. аналізує реалізацію конституційного права на таємницю телефонних розмов і типові труднощі його забезпечення. При цьому межі «цифрових» комунікацій у логіці ст. 258 КПК окреслені не повністю, що залишає простір для різночитань у нових ситуаціях [2, с. 107]. Кухта М., Кушпіт В. описують загальні засади втручання у приватне життя в кримінальному процесі, але саме критерії «приватності» комунікації і вимоги до змісту судового дозволу в цифрових кейсах потребують більшої визначеності [3, с. 216–218]. Паршутін А. Б. пропонує теоретико-правове розуміння втручання у приватне спілкування, однак питання практичного застосування критерію «можуть розраховувати» як інструмента судового контролю залишається відкритим і суперечливим [4, с. 232]. Стельмах А. П. розкриває сутність приватного спілкування у кримінальному процесі, натомість практичні орієнтири для кваліфікації сучасних цифрових каналів (месенджери, хмарні сервіси, службові системи) потребують подальшої конкретизації [5, с. 358–360].

Для порівняльного контексту доречно звертатися й до підходів іноземних авторів, які підсилюють методологічну частину проблеми: де Герт П., Гутвірт С. пропонують розмежування приватності як «інструмента непрозорості людини» і захисту даних як «інструмента

прозорості влади». Це допомагає точніше подивитися на державний доступ до комунікацій крізь призму гарантій і контролю, хоча такі ідеї потребують узгодження з процесуальними механізмами КПК – насамперед із вимогами до ухвали та меж втручання [6, с. 61–64]. Керр О. С. підкреслює, що в технологічно нових ситуаціях традиційні доктрини приватності часто дають нестійкі результати; тому потрібні обережні й чіткі критерії, які зменшують довільність оцінок [7, с. 805]. Солов Д. Дж. звертає увагу на «профілювання» особи через цифрові практики збору й обробки даних, а також на те, що ризик для приватності не завжди зводиться до змісту повідомлень. Ця теза підтримує аргументи на користь значущості метаданих і потреби пропорційності [8, с. 8].

Отже, попередні дослідження дають концептуальну основу, але три питання залишаються не закритими повністю: як уніфікувати застосування критеріїв «умов» та «можуть розраховувати» у цифрових комунікаціях; які стандарти мають визначати межі судового дозволу; і як процесуально відмежовувати доступ до змісту, доступ до носіїв і збір метаданих.

Мета статті полягає в уточненні змісту та меж поняття «приватного спілкування» у контексті ст. 258 КПК з урахуванням конституційних гарантій і стандартів ст. 8 Конвенції про захист прав людини і основоположних свобод, а також у виробленні практичних орієнтирів для правозастосування щодо:

– критеріїв приватності комунікації;

– меж судового дозволу та вимог субсидіарності/пропорційності;

– ризиків недопустимості доказів у разі виходу за межі ухвали або формального судового контролю.

Виклад основного матеріалу. Конституція України гарантує таємницю листування, телефонних розмов та іншої кореспонденції. Винятки допускаються лише на підставі судового рішення, у передбачених законом випадках, і за умови, що інформацію неможливо отримати іншим шляхом [9]. Під субсидіарністю слід розуміти вимогу «останньої необхідності»: у клопотанні має бути показано, чому інші слідчі дії або доступ до інформації іншими законними способами не дають результату або є непридатними, і лише після цього обґрунтовується звернення до НСРД. Паралельно Конституція містить ширшу рамку захисту приватності (ст. 32): ідеться про заборону втручання в особисте й сімейне життя та про режим конфіденційної інформації [9]. Для кримінального процесу це важливо не лише як декларація права, а як критерій оцінки «меж допустимого», коли вирішується питання про втручання в комунікації.

Міжнародний стандарт задає ст. 8 Конвенції про захист прав людини і основоположних свобод: втручання можливе тільки «згідно із законом» і лише за умови необхідності в демократичному суспільстві для легітимних цілей [10]. На практиці це означає, що наявності норми і навіть наявності судового дозволу недостатньо, якщо немає передбачуваних меж і запобіжників. Саме на цьому наголошують матеріали ЄСПЛ, де систематизовано орієнтири щодо «якості закону», передбачуваності та гарантій від зловживань [11]. Для українського процесу це прямо пов'язано з тим, як заповнюється змістом судовий контроль: чи він реально обмежує втручання, чи лише створює зовнішню видимість законності.

Стаття 258 КПК подає «спілкування» максимально широко – як передання інформації в будь-якій формі від однієї особи до іншої, безпосередньо або із застосуванням засобів зв'язку [1]. Ця технологічна нейтральність є сильною стороною норми: під її охорону підпадають і цифрові канали – від електронної пошти до месенджерів та відеозв'язку.

Натомість «приватне спілкування» закон пов'язує не з конкретним видом каналу, а з умовами передання або зберігання інформації: такими, за яких учасники можуть розраховувати на захист від втручання інших осіб [1]. Звідси випливає двокомпонентна природа приватності: з одного боку, мають існувати об'єктивні бар'єри доступу, а з іншого – очікування конфіденційності мають бути обґрунтованими. Саме ця друга частина – «можуть розраховувати» – найчастіше і створює складність. Вона вимагає не механічного застосування, а аргументованої оцінки конкретних умов комунікації.

Фізичні умови приватності зазвичай зводяться до фактичного контролю доступу. Є різниця між ситуацією, коли зміст стає доступним стороннім без додаткових дій, і випадком, коли потрібно застосовувати спеціальні заходи або технічні засоби. Юридичні умови, своєю чергою, задаються нормами Конституції, КПК та іншими режимами охорони інформації [1; 9]. У цифрових комунікаціях цей поділ не зникає, але ускладнюється: дані можуть бути водночас «поруч» (в пристрої) і «далеко» (в сервісі), а доступ до них може відбуватися різними процесуальними шляхами.

Варто підкреслити: сам факт зберігання даних у сервісів третіх осіб не робить їх «відкритими». Вирішальними стають налаштування доступу, авторизація, попередження про контроль, а також наявність законної процедури державного доступу [10; 11]. Якщо ці фактори ігноруються, приватність починають підміняти назвами сервісів або побутовими уявленнями, і тоді судовий контроль втрачає точність.

Щоб уникати різночитань, доцільно спиратися на підхід, який тримається на чітких і перевірюваних ознаках приватності. Тоді приватність визначається не тим, через що саме спілкувалися (телефон, месенджер чи інший сервіс), а тими фактичними й юридичними умовами, які справді формують очікування конфіденційності. Це узгоджується з доктринальними міркуваннями про те, що в технологічно мінливих ситуаціях правові висновки без ясних орієнтирів легко стають непослідовними, і водночас зменшує ризик надмірного втручання [7, с. 801, 805, 861, 875–876; 8, с. 8]. Зазвичай увага зосереджується на таких моментах:

- кому адресована комунікація і хто є її учасниками;
- який режим доступу встановлено та які налаштування конфіденційності діють;
- як поводяться сторони і які заходи вони вживають, щоб зберегти зміст закритим;
- чи є повідомлення про можливий контроль у службових системах;
- у якому контексті відбувається спілкування;
- наскільки чутливим є зміст.

У такий спосіб оціночні формулювання закону отримують практичний зміст, який можна аргументувати й перевірити.

У ст. 258 КПК втручання пов'язується насамперед із доступом до змісту приватного спілкування і допускається лише на підставі ухвали слідчого судді [1]. Для практики принципово важливо не змішувати різні типи дій:

- заходи, спрямовані на зміст комунікації (перехоплення);
- дії щодо носіїв (вилучення пристрою, огляд, копіювання);
- збір метаданих (час, тривалість, ідентифікатори тощо).

Метадані також здатні істотно впливати на приватність, адже на їх основі відтворюються зв'язки, повсякденні практики та загальна «картина» соціальної взаємодії [11; 8, с. 8]. Через це оцінка пропорційності не має обмежуватися аналізом змісту повідомлень: у певних випадках ступінь втручання в приватне спілкування визначається саме метаданими. Контроль пропорційності в такій ситуації зводиться до перевірки, чи не є обсяг і деталізація зібраних даних надмірними щодо процесуальної мети, і чи обмежено втручання конкретними параметрами (строком, ідентифікаторами, видами даних).

Окремо слід ураховувати абсолютні заборони втручання у спілкування захисника або священнослужителя з підозрюваним, обвинуваченим чи засудженим [1]. У таких ситуаціях питання меж не зводиться до доцільності – воно вирішене законом наперед і має спрацьовувати як «жорсткий запобіжник».

ЄСПЛ визнає можливість негласних заходів, але висуває вимогу, яку важко обійти: контроль має бути реальним, а гарантії – достатніми для стримування зловживань. У справі Klass and Others v. Germany наголошено, що негласний нагляд допускається лише за наявності відповідних запобіжників [12]. У рішенні Weber and Saravia v. Germany сформульовано мінімальні вимоги до режимів перехоплення – насамперед щодо визначеності підстав, меж, строків і нагляду [13]. Подібний підхід щодо критерію «передбачено законом» і неприпустимості надмірно широких правил простежується також у справах Liberty and Others v. the United Kingdom [14], Szabó and Vissy v. Hungary [15], Big Brother Watch and Others v. the United Kingdom [16].

З огляду на ці орієнтири формальної наявності ухвали в українському процесі недостатньо. Ухвала має реально обмежувати втручання, дозволяти перевірити субсидіарність і пропорційність, а також не створювати підстав для «надмірного збору» інформації [11; 12–16]. Інакше кажучи, судовий дозвіл повинен працювати не як формальний допуск до НСРД, а як інструмент встановлення рамок, які потім можна зіставити з фактичними діями.

Інструкція про організацію проведення НСРД встановлює стандарти організації та фіксації результатів негласних заходів [17]. Саме на цьому рівні часто «ламається» перевірюваність втручання: проблеми з допустимістю зазвичай виникають тоді, коли неможливо встановити джерело даних, протоколювання є формальним, порушується «ланцюг збереження» матеріалів або фактичний обсяг втручання виходить за межі судового дозволу [17].

Узагальнення Верховного Суду показують підхід, за якого оцінюється не сам факт порушення, а його характер і вплив на права учасників та надійність доказів [18]. Для втручання у приватне спілкування це має доволі конкретний наслідок: втручання без ухвали або з виходом за її межі зазвичай зачіпає ядро судового контролю (у зв'язку зі ст. 31 Конституції) і створює істотні ризики недопустимості [1; 9; 18]. Саме тому питання меж – не технічна деталь, а центральний елемент легітимності втручання.

Висновки: Стаття 258 КПК формує процесуальну основу захисту приватного спілкування та встановлює, що втручання можливе лише за судовим дозволом. При цьому приватність комунікації не зводиться до назви сервісу або каналу зв'язку: вона визначається сукупністю фізичних і юридичних умов та тим, наскільки обґрунтованими є очікування сторін щодо конфіденційності. Практика ЄСПЛ додатково акцентує, що потрібні реальні запобіжники, чітко окреслені межі дозволу й реальний контроль пропорційності. Отже, ухвала слідчого судді має бути не формальністю, а механізмом, який задає рамки втручання і дозволяє перевірити субсидіарність.

Перспективним напрямом видається вироблення практичних орієнтирів для підготовки клопотань і ухвал слідчого судді: чітко визначати ідентифікатори, часові межі, види даних та правила мінімізації зібраної інформації. Окремої уваги потребує й процесуальне осмислення збору метаданих як чинника, що впливає на приватність.

Список використаних джерел

1. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/4651-17 (дата звернення: 05.02.2026).

2. Камінська Н., Джуська А., Шемчук В. Реалізація конституційного права людини на таємницю телефонних розмов в Україні. Науковий вісник Національної академії внутрішніх справ. 2020. Т. 114, № 1. С. 100–109. DOI: https://doi.org/10.33270/01201141.100.

3. Кухта М., Кушпіт В. Правові положення щодо втручання у приватне життя в кримінальному процесуальному праві. Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки. 2022. № 4 (36). С. 216–222. DOI: https://doi.org/10.23939/law2022.36.216.

4. Паршутін А. Б. Поняття втручання у приватне спілкування: теоретико-правова природа. Право і суспільство. 2018. № 5, ч. 2. С. 227–232. URL: https://pravoisuspilstvo.org.ua/archive/2018/5_2018/part_2/40.pdf (дата звернення: 05.02.2026).

5. Стельмах А. П. Сутність приватного спілкування у кримінальному процесі: окремі теоретико-правові та прикладні аспекти. Аналітично-порівняльне правознавство. 2022. № 4. С. 358–363. DOI: https://doi.org/10.24144/2788-6018.2022.04.65.

6. De Hert P., Gutwirth S. Privacy, data protection and law enforcement: Opacity of the individual and transparency of power. Privacy and the Criminal Law / ed. by E. Claes, A. Duff, S. Gutwirth. Antwerp ; Oxford : Intersentia, 2006. P. 61–104.

7. Kerr O. S. The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution. Michigan Law Review. 2004. Vol. 102, No. 5. P. 801–888. DOI: https://doi.org/10.2307/4141982.

8. Solove D. J. The Digital Person: Technology and Privacy in the Information Age. New York : New York University Press, 2004. 283 p.

9. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 05.02.2026).

10. Конвенція про захист прав людини і основоположних свобод : Конвенція від 04.11.1950. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/995_004 (дата звернення: 05.02.2026).

11. ЄСПЛ-KS. Стаття 8 – Право на повагу до приватного і сімейного життя : довідковий ресурс / Council of Europe. URL: https://ks.echr.coe.int/uk/web/echr-ks/article-8 (дата звернення: 05.02.2026).

12. Klass and Others v. Germany : judgment of 06 September 1978, application no. 5029/71. HUDOC (European Court of Human Rights). URL: https://hudoc.echr.coe.int/eng?i=001-57510 (дата звернення: 05.02.2026).

13. Weber and Saravia v. Germany : decision of 29 June 2006, application no. 54934/00. HUDOC (European Court of Human Rights). URL: https://hudoc.echr.coe.int/eng?i=001-76586 (дата звернення: 05.02.2026).

14. Liberty and Others v. the United Kingdom : judgment of 01 July 2008, application no. 58243/00. HUDOC (European Court of Human Rights). URL: https://hudoc.echr.coe.int/eng?i=001-87207 (дата звернення: 05.02.2026).

15. Szabó and Vissy v. Hungary : judgment of 12 January 2016, application no. 37138/14. HUDOC (European Court of Human Rights). URL: https://hudoc.echr.coe.int/fre?i=001-160020 (дата звернення: 05.02.2026).

16. Big Brother Watch and Others v. the United Kingdom [GC] : judgment of 25 May 2021, application nos. 58170/13, 62322/14, 24960/15. HUDOC (European Court of Human Rights). URL: https://hudoc.echr.coe.int/fre?i=001-210077 (дата звернення: 05.02.2026).

17. Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : наказ від 16.11.2012 № 114/1042/516/1199/936/1687/5. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/v0114900-12 (дата звернення: 05.02.2026).

18. Огляд судової практики Касаційного кримінального суду у складі Верховного Суду (2022 рік) : аналітичний матеріал / Верховний Суд. URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/ogliady/Oglyad_KKS_2022.pdf (дата звернення: 05.02.2026).

References

1. Verkhovna Rada Ukrainy. (2012, April 13). Kryminalnyi protsesualnyi kodeks Ukrainy: Zakon Ukrainy No. 4651-6 [Criminal Procedure Code of Ukraine: Law of Ukraine No. 4651-6]. Baza danykh “Zakonodavstvo Ukrainy” [Legislation of Ukraine database]. https://zakon.rada.gov.ua/go/4651-17 [in Ukrainian].

2. Kaminska, N., Dzhuska, A., & Shemchuk, V. (2020). Realizatsiia konstytutsiinoho prava liudyny na taiemnytsiu telefonnykh rozmov v Ukraini [Implementation of the constitutional human right to the secrecy of telephone conversations in Ukraine]. Naukovyi visnyk Natsionalnoi akademii vnutrishnikh sprav [Scientific Bulletin of the National Academy of Internal Affairs], 114, 100–109. https://doi.org/10.33270/01201141.100 [in Ukrainian].

3. Kukhta, M., & Kushpit, V. (2022). Pravovi polozhennia shchodo vtruchannia u pryvatne zhyttia v kryminalnomu protsesualnomu pravi [Legal provisions on interference with private life in criminal procedural law]. Visnyk Natsionalnoho universytetu “Lvivska politekhnika”. Seriia: Yurydychni nauky [Bulletin of Lviv Polytechnic National University. Series: Legal Sciences], 4(36), 216–222. https://doi.org/10.23939/law2022.36.216 [in Ukrainian].

4. Parshutin, A. B. (2018). Poniattia vtruchannia u pryvatne spilkuvannia: teoretyko-pravova pryroda [The concept of interference with private communication: Theoretical and legal nature]. Pravo i suspilstvo [Law and Society], 5(2), 227–232. https://pravoisuspilstvo.org.ua/archive/2018/5_2018/part_2/40.pdf [in Ukrainian].

5. Stelmakh, A. P. (2022). Sutnist pryvatnoho spilkuvannia u kryminalnomu protsesi: okremi teoretyko-pravovi ta prykladni aspekty [The essence of private communication in criminal procedure: Certain theoretical, legal, and applied aspects]. Analitychno-porivnialne pravoznavstvo [Analytical and Comparative Jurisprudence], 4, 358–363. https://doi.org/10.24144/2788-6018.2022.04.65 [in Ukrainian].

6. de Hert, P., & Gutwirth, S. (2006). Privacy, data protection and law enforcement: Opacity of the individual and transparency of power. In E. Claes, A. Duff, & S. Gutwirth (Eds.), Privacy and the criminal law (pp. 61–104). Intersentia. [in English].

7. Kerr, O. S. (2004). The Fourth Amendment and new technologies: Constitutional myths and the case for caution. Michigan Law Review, 102(5), 801–888. https://doi.org/10.2307/4141982 [in English].

8. Solove, D. J. (2004). The digital person: Technology and privacy in the information age. New York University Press. [in English].

9. Verkhovna Rada Ukrainy. (1996, June 28). Konstytutsiia Ukrainy: Zakon Ukrainy No. 254k-96-VR [Constitution of Ukraine: Law of Ukraine No. 254k-96-VR]. Baza danykh “Zakonodavstvo Ukrainy” [Legislation of Ukraine database]. https://zakon.rada.gov.ua/go/254%D0%BA/96-%D0%B2%D1%80 [in Ukrainian].

10. Verkhovna Rada Ukrainy. (1950, November 4). Konventsiia pro zakhyst prav liudyny i osnovopolozhnykh svobod [Convention for the Protection of Human Rights and Fundamental Freedoms]. Baza danykh “Zakonodavstvo Ukrainy” [Legislation of Ukraine database]. https://zakon.rada.gov.ua/go/995_004 [in Ukrainian].

11. Council of Europe. (n.d.). YeSPL-KS. Stattia 8 – Pravo na povahu do pryvatnoho i simeinoho zhyttia [ECHR KS. Article 8 – Right to respect for private and family life]. https://ks.echr.coe.int/uk/web/echr-ks/article-8 [in Ukrainian].

12. Klass and Others v. Germany, Application No. 5029-71, European Court of Human Rights (1978, September 6). https://hudoc.echr.coe.int/eng?i=001-57510 [in English].

13. Weber and Saravia v. Germany, Application No. 54934-00, European Court of Human Rights (2006, June 29). https://hudoc.echr.coe.int/eng?i=001-76586 [in English].

14. Liberty and Others v. the United Kingdom, Application No. 58243-00, European Court of Human Rights (2008, July 1). https://hudoc.echr.coe.int/eng?i=001-87207 [in English].

15. Szabó and Vissy v. Hungary, Application No. 37138-14, European Court of Human Rights (2016, January 12). https://hudoc.echr.coe.int/fre?i=001-160020 [in English].

16. Big Brother Watch and Others v. the United Kingdom [GC], Application Nos. 58170-13, 62322-14, 24960-15, European Court of Human Rights (2021, May 25). https://hudoc.echr.coe.int/fre?i=001-210077 [in English].

17. Verkhovna Rada Ukrainy. (2012, November 16). Pro zatverdzhennia Instruktsii pro orhanizatsiiu provedennia nehlasnykh slidchykh (rozshukovykh) dii ta vykorystannia yikh rezultativ u kryminalnomu provadzhenni: Nakaz No. 114-1042-516-1199-936-1687-5 [On approval of the Instruction on organizing covert investigative (search) actions and using their results in criminal proceedings: Order No. 114-1042-516-1199-936-1687-5]. Baza danykh “Zakonodavstvo Ukrainy” [Legislation of Ukraine database]. https://zakon.rada.gov.ua/go/v0114900-12 [in Ukrainian].

18. Verkhovnyi Sud. (2022). Ohliad sudovoi praktyky Kasatsiinoho kryminalnoho sudu u skladi Verkhovnoho Sudu (2022 rik): analitychnyi material [Review of the case law of the Criminal Cassation Court within the Supreme Court (2022): Analytical material]. https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/ogliady/Oglyad_KKS_2022.pdf [in Ukrainian].

Romanov Vitalii,
Candidate of Law
(Sumy Branch of Kharkiv National University of Internal Affairs, Sumy)
ORCID: https://orcid.org/0000-0002-8569-5723

DEFINITION AND BOUNDARIES OF 'PRIVATE COMMUNICATION' IN UKRAINIAN CRIMINAL PROCEDURE: CHALLENGES IN INTERPRETING ARTICLE 258 OF THE CRIMINAL PROCEDURE CODE

This article examines the content and limits of the notion of "private communication" in Ukrainian criminal procedure through the prism of Article 258 of the Criminal Procedure Code of Ukraine. The key point is that this provision establishes not only a procedural ban on interference without an investigating judge's warrant, but also a minimum concept of privacy linked to the "conditions" under which participants may reasonably expect protection of information from third-party access. Because the statute relies on evaluative wording ("conditions", "may expect"), the same type of communication may be classified differently depending on context. Accordingly, privacy is not determined by the channel itself (telephone, messenger, letter), but by a combination of factual and legal features: the circle of recipients, access settings, consent to disclosure, the context of professional communications, and the parties' expectations of confidentiality. The article also addresses the relationship between Article 258 Criminal Procedure Code of Ukraine and constitutional guarantees, as well as the standards under Article 8 of the European Convention on Human Rights, including legality, necessity, proportionality, and the need for effective safeguards against abuse. Relying on ECtHR case-law and the approaches reflected in the practice of the Supreme Court, the paper argues that the mere existence of a warrant is insufficient: decisive are the clarity of the authorization's limits (scope, time frame, identifiers, categories of data), genuine subsidiarity in using covert investigative measures, and proper documentation of results. A multifactor "reasonable expectation of privacy" test is proposed as a practical tool for qualifying communications as private and for improving the quality of motions and judicial warrants. The practical value of the study lies in promoting a more consistent interpretation of Article 258 Criminal Procedure Code of Ukraine and strengthening judicial oversight of interferences with private communications in a digital environment.

Key words: *private communication, interference, covert investigative measures (CIM), electronic communications, judicial oversight, admissibility of evidence.*

Дата першого надходження статті до видання: 17.02.2026
Дата прийняття статті до друку після рецензування: 25.03.2026
Дата публікації (оприлюднення) статті: 11.05.2026