

ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ І. І. МЕЧНИКОВА

Економіко-правовий факультет

Кафедра кримінального права, кримінального процесу та криміналістики

Кваліфікаційна робота

на здобуття ступеня вищої освіти «магістр»

«Тємниця спілкування, як засада кримінального провадження»

«The secrecy of communication as basis for criminal proceedings»

Виконала: здобувачка очної форми навчання

спеціальності 081 Право

Освітня програма «Право»

Метакса Дар'я Олександрівна

Керівник: д.ю.н., проф. Миколенко О. М. _____

Рецензент: д.ю.н., проф. Чуваков О. А.

Рекомендовано до захисту:
протокол засідання кафедри
№ ____ від ____ . ____ . 2025 р.

Захищено на засіданні ЕК № 6:
протокол № ____ від ____ . ____ . 2025 р.
Оцінка _____ / _____ / _____
(за національною шкалою / шкалою ECTS / бали)

Завідувач кафедри

(підпис) Олег ЧУВАКОВ
(прізвище, ім'я)

Голова ЕК

(підпис) Олена МИКОЛЕНКО
(прізвище, ім'я)

Одеса 2025

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	3
ВСТУП	4
РОЗДІЛ I. ПОНЯТТЯ ТА ЗМІСТ ТАЄМНИЦІ СПІЛКУВАННЯ, ЯК ЗАСАДИ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ	9
1.1 Доктринальне та законодавче розуміння таємниці спілкування, як засади кримінального провадження.....	9
1.2 Міжнародні стандарти у сфері забезпечення права на таємницю спілкування.....	19
1.3 Учасники кримінального провадження та таємниця спілкування.....	29
Висновки до розділу I.....	35
РОЗДІЛ II. ПРОЦЕСУАЛЬНІ ДІЇ, ЩО ОБМЕЖУЮТЬ ТАЄМНИЦЮ СПІЛКУВАННЯ	38
2.1. Підстави та процесуальний порядок обмеження таємниці спілкування..	38
2.2 Обмеження таємниці спілкування в ході проведення аудіо-, відеоконтролю особи та місця.....	45
2.3. Обмеження таємниці спілкування в ході проведення тимчасового доступу до речей та документів.....	50
2.4 Обмеження таємниці спілкування в ході проведення огляду і виїмки кореспонденції.....	58
2.5 Обмеження таємниці спілкування в ході проведення зняття інформації з електронних комунікаційних мереж та зняття інформації з електронних інформаційних систем.....	63
Висновки до розділу II.....	70
РОЗДІЛ III. ОСКАРЖЕННЯ РІШЕНЬ ПРО ДОЗВІЛ НА ВТРУЧАННЯ У ПРИВАТНЕ СПІЛКУВАННЯ	73

Висновки до розділу III.....	80
ВИСНОВКИ.....	82
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	87

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

КПК	Кримінальний процесуальний кодекс України
СРД	Слідчі (розшукові) дії
НСРД	Негласні слідчі (розшукові) дії
ВСУ	Верховний суд України
ККС	Касаційний кримінальний суд
ЄСПЛ, Суд	Європейський суд з прав людини
Інструкція	Інструкція про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні
ЗУ	Закон України
ч.	Частина
п.	Пункт

ВСТУП

Актуальність дослідження. Важливість засад кримінального провадження важко переоцінити, у нинішніх умовах розвитку кримінальної процесуальної науки їм приділяється особлива увага, адже вони формують та визначають спрямованість діяльності всіх учасників кримінальних процесуальних правовідносин, забезпечують дотримання прав людини, правопорядку та юридичної рівності. Засади знаходяться в тісному взаємозв'язку та утворюють єдину систему, нерозривним та важливим елементом цієї системи є таємниця спілкування. Вона бере свій початок від конституційного права на таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції, а тому вимагає найвищого рівня охорони та гарантій. Хоча Україна вже зробила багато кроків у цьому напрямку, проте сьогодні доводиться констатувати, що подальша розробка і впровадження цієї засади залишається актуальним викликом для законодавця та науковців.

В контексті технологічного прогресу та розвитку соціальних мереж на долю яких припадає більшість комунікацій громадян, досі на законодавчому рівні залишається проблематичним визначення обсягу таємниці спілкування, в тому числі чи підпадають під її охорону новітні засоби зв'язку. Складнощі полягають і в тому, що на практиці не завжди досягається справедливий баланс між інтересами слідства та правами особи через обмеженість механізмів контролю, невмотивованість рішень про втручання у приватне спілкування та низький рівень оцінки ризиків такого втручання з боку працівників правоохоронних органів і суду.

За таких обставин потребує ґрунтовного та послідовного аналізу доктринальне та законодавче розуміння таємниці спілкування, також важливо дослідити наскільки національне законодавство узгоджується з міжнародними стандартами, які недоліки існують в правозастосуванні та як можна їх вирішити. Крім того, слід узгодити як таємниця спілкування взаємодіє з учасниками кримінального провадження, якими специфічним правами,

обов'язками та гарантіями вони наділені з метою її дотримання, наскільки якісно врегульовано процес проведення СРД та НСРД, які передбачають втручання у приватне спілкування та як процесуальне законодавство забезпечує оскарження рішень про втручання у приватне спілкування.

Дослідження вчених в даному напрямку здебільшого не зосереджувалися на встановленні того яким чином сучасні технології вплинули на розвиток таємниці спілкування, як засади з якою пов'язано низку процесуальних гарантій. Слід системно дослідити наскільки трансформувалось її бачення та як в еру сучасних технологій забезпечити всебічний захист права особи на таємницю спілкування, коли ризики неправомірного втручання неухильно зростають.

Науково-теоретичним підґрунтям дослідження стали праці вітчизняних фахівців з кримінального процесуального права, зокрема, В. І. Галагана, А. С. Гуменюк, Л. В. Ємчук, А. А. Коваля, В. В. Луцика, В. В. Назарова, С. І. Перепелиці, І. І. Савляк, А. Б. Ткачика, Ж. В. Удовенко, М. О. Черевко, В. В. Шум і ін.

Таким чином, актуальність магістерського дослідження зумовлена необхідністю переосмислення класичного розуміння засади, її значенням в системі процесуальних гарантій та впливом на розвиток кримінальної процесуальної науки.

Мета і задачі дослідження. Метою магістерської роботи є комплексне теоретико-правове дослідження сутності, обсягу і особливостей притаманних таємниці спілкування, як засаді кримінального провадження, виявлення прогалин і суперечностей у правовому регулюванні з метою формування обґрунтованих пропозицій щодо вдосконалення чинного кримінального процесуального законодавства України.

Для досягнення зазначеної мети слід виконати наступні **завдання**:

- дослідити особливості доктринального та законодавчого розуміння таємниці спілкування, як засади кримінального провадження;

- розкрити міжнародні стандарти у сфері забезпечення права на таємницю спілкування;
- дослідити взаємодію таємниці спілкування та учасників кримінального провадження;
- охарактеризувати підстави та порядок обмеження таємниці спілкування;
- визначити суть та специфіку обмеження таємниці спілкування в ході проведення аудіо-, відеоконтролю особи та місця;
- охарактеризувати особливості обмеження таємниці спілкування в ході проведення тимчасового доступу до речей та документів;
- розкрити характер обмеження таємниці спілкування в ході проведення огляду і виїмки кореспонденції;
- окреслити проблеми співвідношення обмеження таємниці спілкування в ході проведення зняття інформації з електронних комунікаційних мереж та зняття інформації з електронних інформаційних систем;
- дослідити ефективність та варіативність способів оскарження рішень про дозвіл на втручання у приватне спілкування.

Об'єктом дослідження є суспільні відносини, що виникають у зв'язку з реалізацією та забезпеченням таємниці спілкування у кримінальному провадженні.

Предметом дослідження є таємниця спілкування, як засада кримінального провадження;

Методи дослідження. Під час написання роботи були використані загальнонаукові і спеціально-юридичні методи правових досліджень. *Антропологічний метод* був застосований для з'ясування сутності таємниці спілкування з точки зору основоположного права особи (підрозділ 1.1). *Системно-структурний метод* дозволив розглянути таємницю спілкування не тільки як засаду кримінального провадження, а й як конституційне право особи (підрозділ 1.1). *Метод порівняльного правознавства* використовувався з метою порівняння законодавчого регулювання таємниці спілкування у

різних національних та міжнародних актах, а також зіставлення з правом на повагу до приватного життя (підрозділи 1.1, 1.2). Застосування методу аналізу дозволило виокремити права, обов'язки та гарантії учасників кримінального провадження, які впливають з засади таємниці спілкування (підрозділ 1.3). Діалектичний метод був застосований з метою виявлення взаємозв'язків, протиріч та відмінностей між НСРД, які мають подібну правову природу (підрозділи 2.2, 2.3, 2.4, 2.5). Застосування формально-юридичного методу дозволило надати оцінку процесуальним положенням, які регламентують порядок оскарження рішень про дозвіл на втручання у приватне спілкування (Розділ 3).

Наукова новизна отриманих результатів полягає в тому, що магістерська робота є комплексним теоретико-правовим дослідженням сутності та змісту таємниці спілкування як засади кримінального провадження. В результаті аналізу було сформульовано низку наукових висновків та пропозицій, зокрема таких:

Уперше:

- запропоновано доповнити п. 3 ч. 2 ст. 248 КПК вимогою про зазначення в клопотанні слідчого, прокурора не тільки правової кваліфікації діяння, а й обґрунтування, що вчинене особою правопорушення відповідає і на момент внесення відомостей до ЄРДР, і на час звернення з клопотанням необхідному ступеню тяжкості. Дана пропозиція зможе запобігти випадкам, коли слідчі, прокурори вдаються до «штучного» створення більш тяжких правових кваліфікацій, аби створити формальні правові підстави для втручання, а слідчі судді при постановленні рішень зможуть завіритися в обґрунтованості попередньої кваліфікації;

- обґрунтовано необхідність впровадження обов'язкової реєстрації користувачів послуг мобільного зв'язку за паспортними даними в момент укладення договору з постачальником комунікаційних послуг з метою сприянні якості проведення НСРД та дотримання права осіб на таємницю спілкування. По-перше, це дозволить точно встановлювати ідентифікаційні

ознаки особи, як об'єкта спостереження з метою проведення зняття інформації з електронних комунікаційних мереж. По-друге, відпаде необхідність проведення додаткових слідчо-оперативних заходів для їх з'ясування, що значно відобразиться на процесуальній економії. По-третє, суттєво зменшиться ризик випадкового неправомірного втручання у приватне спілкування сторонніх осіб, оскільки існуватиме документальне підтвердження прив'язки абонентської картки до конкретної особи;

дістали подальшого розвитку:

- положення про розуміння об'єктів захисту таємницею спілкування;
- дослідження щодо правового удосконалення порядку та підстав проведення НСРД, пов'язаних з втручанням у приватне спілкування;

Апробація результатів дослідження. Деякі з результатів дослідження були оприлюднені на Міжнародній науково-практичній конференції "Міждисциплінарні підходи до вирішення актуальних проблем економіки, обліку, менеджменту та права в умовах світових трансформацій" (м. Кременчук, 18 жовтня 2025 року)

Структура роботи. Магістерська робота складається зі вступу, трьох розділів, восьми підрозділів, висновків, списку використаних джерел.

РОЗДІЛ І. ПОНЯТТЯ ТА ЗМІСТ ТАЄМНИЦІ СПІЛКУВАННЯ, ЯК ЗАСАДИ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ

1.1 Доктринальне та законодавче розуміння таємниці спілкування, як засади кримінального провадження.

Таємниця спілкування, перш за все, є конституційним принципом, що свідчить про особливий підхід законодавця до її охорони, фундаментальний характер та невід'ємність. Згідно зі ст. 31 Конституції України (далі - КУ) «Кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції. Винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинів чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо» [1, ст. 31]. З цього нормативного положення випливає, що дане право не є абсолютним, його обмеження допускається в визначених законодавством випадках та лише за умови дотримання чіткої процедури такого обмеження. Крім того, ст. 31 КУ має універсальний спектр дії, у зв'язку з цим, сфера її поширення не обмежується виключно громадянами України, однаковим чином захищаються права іноземців та осіб без громадянства. Згідно з ЗУ від 13 квітня 2012 «Про правовий статус іноземців та осіб без громадянства»: «Іноземці та особи без громадянства, які перебувають в Україні на законних підставах, користуються тими самими правами і свободами, а також несуть такі самі обов'язки, як і громадяни України, за винятками, встановленими Конституцією, законами чи міжнародними договорами України» [3].

Наразі таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції прийнято розглядати як невід'ємну складову права особи на приватне життя. З цього приводу С. І Перепелиця відзначає: «Зазначені поняття слід співвідносити як ціле та частину, адже поняття "приватне життя" є значно ширшим і включає в себе весь спектр приватноправових інтересів

осіб, до яких відносяться способи комунікації та засоби її здійснення» [2, с. 70-79], в даному контексті ми розділяємо думку науковця та вважаємо, що особисте спілкування особи являє собою один з проявів права особи на приватність, недоторканності правового статусу людини, її ролі в соціальному житті, проте акцентуємо що дія даного права рівною мірою поширюється і на сферу публічних і ділових інтересів. Також, розділяємо думку А.Є. Стрекалова, науковець стверджує: «засада таємниці спілкування проголошує невід'ємне право кожного громадянина, без відповідного захисту якого неможливе повноцінне життя в суспільстві, а тому зазначену засаду, а також жорсткі та чітко визначені нормативно-правовими актами умови втручання в реалізацію цієї засади та кримінально-правову заборону порушення цієї засади слід розглядати як одну з найголовніших гарантій забезпечення охорони таємниці приватного життя від неправомірного втручання та порушення» [16, с. 7].

Цікавим в даному контексті є дослідження С. В. Шевчука: «на підставі аналізу практики Європейського суду з прав людини, однією з основних складових права на повагу до приватного життя науковець виокремив його комунікативний елемент (безпека та приватність листування, електронної пошти, телефонних розмов та інших видів приватних комунікацій)» [11, с. 362]. Автор таким чином підкреслює, що в контексті стрімкого розвитку інформаційних технологій в умовах, коли обсяг комунікацій через цифрові засоби зв'язку невинно зростає, а ризики втручання у таке спілкування через стеження, збирання метаданих або злам цифрових засобів зв'язку набувають системного характеру потрібно розширювати розуміння терміну «таємниця спілкування» та не обмежувати його класичними видами комунікацій.

Для детальнішого аналізу поняття «таємниця спілкування» вважаємо за необхідне звернутися і до інших нормативних актів, які так чи інакше регулюють питання реалізації чи захисту цього конституційного принципу:

Звернемо увагу на Главу 22 Цивільного кодексу України (далі - ЦКУ), яка присвячена регулюванню особистих немайнових прав, що забезпечують

соціальне буття фізичної особи, а саме ст. 306 ЦКУ передбачає: «фізична особа має право на таємницю листування, телеграм, телефонних розмов, телеграфних повідомлень та інших видів кореспонденції. Листи, телеграми та інші види кореспонденції можуть використовуватися, зокрема шляхом опублікування, лише за згодою особи, яка направила їх, та адресата. Якщо кореспонденція стосується особистого життя іншої фізичної особи, для її використання, зокрема шляхом опублікування, потрібна згода цієї особи» [4, ст. 306].

У галузі поштового зв'язку діє спеціальний закон, в якому теж згадується про таємницю листування, згідно ст. 6 ЗУ «Про поштовий зв'язок»: «таємниця поштових відправлень, у тому числі листування та іншої письмової кореспонденції, гарантується Конституцією України. Оператори поштового зв'язку вживають організаційно-технічних заходів для захисту інформації згідно із законодавством. Виймка та огляд поштових відправлень, одержання будь-яких довідок щодо них забороняються, крім випадків, визначених законом» [5, ст. 6].

Виходячи з того, що метою магістерської роботи є дослідження таємниці спілкування саме як засади кримінального провадження, то центральним нормативним актом, що відображає логічний розвиток конституційних положень в сфері кримінального процесу є КПК. Отже, ст. 14 КПК встановлює, що «під час кримінального провадження кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції, інших форм спілкування. Втручання у таємницю спілкування можливе лише на підставі судового рішення у випадках, передбачених цим Кодексом, з метою виявлення та запобігання тяжкому чи особливо тяжкому злочину, встановлення його обставин, особи, яка вчинила злочин, якщо в інший спосіб неможливо досягти цієї мети» [7, ст. 14]. Дана норма є однією з ключових для нашого дослідження, адже вона акцентує на тому, що «вручанням у приватне спілкування є доступ до змісту спілкування за умов, якщо учасники спілкування мають достатні підстави вважати, що спілкування

є приватним» [7, ст. 14]. Вказана засаднича норма прямо забороняє використання отриманої в результаті легітимного втручання у таємницю спілкування інформації з метою не пов'язаною із завданнями кримінального провадження. При цьому звертає на себе увагу й те, що приписи ч. 3 ст. 14 КПК не обмежують коло зобов'язаних суб'єктів, яких стосується ця заборона.

З метою детальнішого аналізу необхідно встановити, що розуміється під поняттями: *«листування»*, *«телефонні розмови»*, *«телеграфна кореспонденція»*, *«кореспонденція» та інші форми спілкування»*. Також слід дослідити як дані поняття співвідносяться та взаємодіють, наскільки актуальними є їх використання на сьогодні та чи однакові підходи до визначення їх змісту. Отже, звернемо увагу на наступні моменти:

1. Термін «кореспонденція» не має нормативного визначення в українському законодавстві, а у науковій літературі трактується по-різному. При цьому ЗУ «Про поштовий зв'язок» від 03.11.2022 надає досить обмежене визначення письмової кореспонденції, як: «листи, поштові картки, дрібні пакети, мішки "М", адресна поштова розсилка та відправлення для сліпих» [5, ст. 1], не відповідаючи на питання, що входить до інших видів кореспонденції і чи позначає це поняття телефонні розмови, повідомлення, що передаються засобами електронного зв'язку.

На противагу цьому, поняття «кореспонденція» в науковій літературі дедалі частіше розглядається як узагальнююче поняття для всіх перелічених у ст. 31 КУ способів передачі інформації. Наприклад, Л.В. Ємчук інтерпретує термін «кореспонденція» розширено, наголошуючи на тому, що «право на таємницю кореспонденції можна визначити як гарантовану державою автономну можливість суб'єкта вільно та негласно обмінюватися інформацією, зокрема особистого характеру, у вигляді поштово-телеграфних відправлень (листів, телеграм, бандеролей, посилок, переказів та ін.), телефонних переговорів, електронного обміну повідомленнями тощо» [27, с. 56-57].

Надаючи визначення поняттю «кореспонденція», необхідно враховувати й динамічний розвиток інформаційно-телекомунікаційної складової життя суспільства. Здійснюючи його тлумачення, вітчизняні науковці, поряд з листуванням, телефонними розмовами та телеграфною кореспонденцією, зазначають про: «повідомлення, зроблені по телетайпу, телефаксу, за допомогою пейджингового зв'язку, електронної пошти (електронні листи та інші повідомлення, які передаються через комп'ютер)» [26, с. 75]. З цього приводу ЄСПЛ у своїх рішеннях доволі часто відзначає: «нові технології також підпадають під поняття кореспонденції, зокрема електронні повідомлення, використання Інтернету, і дані, які зберігаються на комп'ютерних серверах, жорстких і гнучких дисках, та давніші види електронних комунікацій, такі, як телекси, повідомлення на пейджері, і приватна радіотрансляція, окрім трансляції на публічних хвилях, що є доступними для інших» [25, с. 80].

2. Що стосується «*листування*», чинний КПК теж тільки оперує таким поняттям, не даючи його легального визначення. Науковці це поняття розкривають через призму форми спілкування: «написаний чи надрукований на папері або електронний текст, що звернений до деякої фізичної або юридичної особи (осіб)» [10, с. 85-88]. При цьому в ході такого спілкування, особи, які беруть в ньому участь можуть очікувати на належний захист інформації, що є змістом листування від сторонніх осіб. Наприклад, І.І. Савляк дотримується думки, що дане поняття слід розуміти ширше: «Під листуванням слід розуміти обмін поштовими відправленнями, які передаються поштовим зв'язком» [12, с. 26]. Такої ж позиції дотримується А.Б. Ткачик: «вважаємо що таємниця спілкування охоплює не тільки таємницю листування (поштового чи електронного), а також таємницю поштових відправлень» [14, с. 37].

У зв'язку з тим, що ЗУ «Про поштовий зв'язок» від 03.11.2022 окреслює, що «таємниця поштових відправлень, у тому числі листування та іншої письмової кореспонденції, гарантується Конституцією України» [5, ст. 6], то відповідно законодавчою нормою охоплюються не всі типи письмових

відправлень в значенні «листування». «Листування» розглядається, як самостійний елемент в складі письмової кореспонденції і є процесом комунікації через рукописний чи друкований текст відображений на аркушах паперу. Схожої думки, про самостійність поняття «листування» дотримується і М.Є. Шумило та В.С. Рудей: «написання одне одному листів та обмін ними» [13, с. 19], що саме по собі відображає також класичний підхід науковців до дефініції. До прикладу, несанкціонованим втручанням в таємницю листування вважатиметься розкриття працівником пошти сторонній особі факту обміну листами між адресатами, ознайомлення з їхнім змістом інакше, ніж з метою виконання рішення слідчого судді та передача для прочитання іншим особам. Також, у зв'язку з тим, що в згаданому Законі України «Про поштовий зв'язок» письмова кореспонденція визначається, як «листи, поштові картки, дрібні пакети, мішки "М", адресна поштова розсилка та відправлення для сліпих» [5], то в науковій літературі також побутує думка, що листування є «різновидом кореспонденції, а розгляд таємниці листування здійснюється в межах таємниці кореспонденції» [15, с. 90].

Вважаємо за необхідне зосередитися на тому, що нерегульованим на законодавчому рівні залишається питання чи входять до поняття «листування» повідомлення надіслані з застосуванням мережі Інтернет. Нам імпонує думка С. І. Перепелиці, яка зазначає: «Обмін інформацією, який відбувається за допомогою телекомунікаційних мереж Skype, IMessage, WhatsApp, Viber, Telegram, Signal є особистим листуванням в розумінні чинного законодавства України та є об'єктом захисту, адже інформація, яка передається за допомогою згаданих вище додатків, захищена наскрізним шифруванням» [2, с. 70-79]. Про це, наприклад, свідчить й Положення політики конфіденційності додатку «Telegram», де зазначається: «Ми вживаємо всіх відповідних технічних та організаційних заходів (включно з шифруванням ваших персональних даних) для забезпечення належного рівня безпеки даних відповідно до можливих ризиків» [19]. Щодо можливості передання інформації із месенджерів іншим

особам, то Політика конфіденційності «Viber», наприклад, передбачає таку можливість лише у трьох випадках:

«1) згідно із нормами закону або у разі здійснення судового процесу проти компанії;

2) під час виконання підписаних угод (з метою захисту своєї власності та дотримання своїх прав);

3) наявність крайньої потреби, з метою забезпечення безпеки користувачів, громадськості чи служби месенджера» [18, с. 25].

Вищенаведене дає нам змогу розуміти обмін інформацією в таких додатках, як різновид *особистого листування*, доступ до якого за загальним правилом можуть мати лише особи, які беруть в ньому участь, а несанкціонований доступ інших осіб до змісту таких повідомлень забороняється, так як месенджери захищено наскрізним шифруванням, а тому мають місце умови за яких учасники такого спілкування можуть розраховувати на конфіденційність інформації, яка передається.

Показовим стосовно цього питання є вирок Рівненського міського суду Рівненської області від 13.09.2019 у справі № 569/12334/19: «Обвинувачений користуючись персональним комп'ютером, який мав доступ до мережі Інтернет, знаючи авторизаційні дані, а саме логін та пароль доступу до електронної поштової скриньки з обліковим записом, що належить потерпілій, які він отримав шляхом несанкціонованого втручання в роботу електронного поштового серверу, та маючи доступ до листування потерпілої, без згоди власника, не маючи законних підстав, зібрав з електронної поштової скриньки конфіденційну інформацію про особу, яка також є інформацією з обмеженим доступом, а саме скановані копії документів потерпілої. У подальшому, вищевказану конфіденційну інформацію про особу, яка також є інформацією з обмеженим доступом, Обвинувачений, зберіг на жорсткий диск свого персонального комп'ютера» [17]. Таким чином, шляхом несанкціонованого доступу до електронного листування потерпілої обвинувачений фактично

порушив її право та таємницю спілкування, адже втрутився в її особисте електронне листування.

Порівнявши різні підходи, на нашу думку, під «листуванням» слід розуміти процес передачі та обміну інформацією, що закріплена в поштових листах чи електронному листуванні, тобто розглядати поняття «листування» слід в вужчому його розумінні, враховуючи при цьому і передання повідомлень за допомогою використання новітніх технологій. Зміст листування при цьому може мати особистий чи офіційний характер та виконувати комунікативну, інформативні, правові та інші функції

3. В науковій літературі під телефонними розмовами розуміють «обмін інформацією голосом у реальному часі з використанням телекомунікаційних мереж» [20, с. 75]. Телефонний зв'язок в свою чергу є видом електрозв'язку, і передбачає передавання за допомогою телефонних апаратів усної інформації, якою обмінюються абоненти. У зв'язку з цим А.Б. Ткачик зазначає: «під телефонними розмовами потрібно вважати спілкування осіб із використанням телефонного зв'язку» [14, с. 38].

Відповідно до п. 7 ч. 1 ст. 162 КПК: «інформація, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо належить до охоронюваної законом таємниці, яка міститься в речах і документах» [7, ст. 162].

Також, у відповідності до ЗУ «Про електронні комунікації» від 16.12.2020, який регулює питання захисту інформації отриманої в результаті надання телекомунікаційних послуг: «закон зобов'язує постачальників електронних комунікаційних послуг забезпечувати і нести відповідальність за схоронність даних щодо кінцевого користувача, у тому числі щодо:

- 1) персональних даних споживача;
- 2) факту отримання кінцевим користувачем електронних комунікаційних послуг;

3) змісту інформації, що передається та/або отримується кінцевим користувачем;

4) обсягу, змісту, маршрутів передачі інформації (даних), у тому числі даних, що обробляються з метою передачі інформації в електронних комунікаційних мережах або оплати електронних комунікаційних послуг;

5) даних про місцезнаходження;

6) даних про спроби виклику між певними кінцевими точками електронної комунікаційної мережі, в тому числі про невдалі спроби виклику (таких, що були ініційовані і не отримали відповіді) або перерване з'єднання» [6, ст. 119].

Таким чином, закон охороняє не лише зміст телефонних розмов, що передається телекомунікаційною мережею, а й відомості про обсяг та специфіку наданих послуг, часові межі в яких відбувалися дзвінки, місце зв'язку з іншим абонентом, невдалі спроби телефонних комунікацій, тощо.

4. Аналізуючи поняття «*телеграфної кореспонденції*», зазначимо, що під телеграмою прийнято вважати: «назву офіційних та неофіційних документів, що становлять особливу групу за способом передачі повідомлення, листа або іншої інформації на відстань засобами телеграфного зв'язку. Телеграфний зв'язок – різновид зв'язку, що ґрунтується на передаванні певної інформації за допомогою спеціальних електричних (електронних) засобів. Здійснюється підприємствами та організаціями електрозв'язку або на договірних з ними засадах підприємствами поштового зв'язку» [21, с. 32]. В науковій спільноті склалася думка, що телеграфні повідомлення «можна одночасно відносити як до поштового, так і до електричного видів зв'язку» [22, с. 62]. Проте, незважаючи на всі переваги використання такого виду зв'язку у минулому, на сьогоднішній час він не використовується, а наявність даного поняття в законодавчих актах свідчить про застарілість термінології та необхідність її переосмислення. Як зазначається в новинних повідомленнях: «З 1 березня 2018 року найбільший український оператор фіксованого зв'язку ПАТ "Укртелеком" припинив

надавати послуги телеграфного зв'язку» [23]. Останню класичну телеграму в Україні було відправлено на початку березня 2018 р. Незважаючи на те, що в медіа від 2024 року було повідомлено про нібито відновлення надання послуг з пересилання телеграм, проте в переліку послуг на офіційному веб-сайті Укрпошти про можливість відправлення телеграм нічого не зазначається.

5. Таємниця інших форм спілкування в науковій літературі та дослідженнях розкривається через віднесення до них «безпосереднього спілкування осіб (не опосередкованого технічними чи іншими засобами), а також спілкування за допомогою телекомунікаційних засобів (електронної пошти, ICQ тощо) і ін.» [24, с. 55]. При цьому, визначення поняття «спілкування» в ч. 3 ст. 258 КПК подається таким чином: «Спілкуванням є передання інформації у будь-якій формі від однієї особи до іншої безпосередньо або за допомогою засобів зв'язку будь-якого типу. Спілкування є приватним, якщо інформація передається та зберігається за таких фізичних чи юридичних умов, при яких учасники спілкування можуть розраховувати на захист інформації від втручання інших осіб» [7, ст. 258]. Відзначимо, що в ст. 31 КУ взагалі не вказується про забезпечення кожній особі таємниці інших форм спілкування, тому в цій частині існує невідповідність між конституційною нормою та положеннями ч.1 ст. 14 КПК.

В дисертаційному дослідженні І.І. Савляк навела результати анкетування, на запитання «Як Ви вважаєте, що можна віднести до інших форм спілкування?, - 88 % опитаних відповіли, що до інших форм спілкування відноситься інтернет-зв'язок» [12, с. 219], з наданими статистичними даними важко не погодитися, адже в умовах інформатизації суспільства живе спілкування все частіше витісняється використанням в цьому процесі інформаційних систем, соціальних мереж та технологій зв'язку.

З огляду на вищенаведене, таємницю спілкування, як засаду кримінального провадження слід розуміти як нормативно визначену гарантію, що дозволяє кожному під час здійснення кримінального провадження розраховувати на «таємницю листування, телефонних розмов, телеграфної та

іншої кореспонденції, інших форм спілкування», яка може бути обмежена виключно на підставі рішення суду у чітко визначених законом випадках .

1.2 Міжнародні стандарти у сфері забезпечення права на таємницю спілкування

В Україні ключові основи дії та застосування норм міжнародного права зосереджені в Конституції, зокрема, це передусім ст. 9 Основного Закону України, згідно з якою: «чинні міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, є частиною національного законодавства України, а укладення міжнародних договорів, які суперечать Конституції України, можливе лише після внесення відповідних змін до Конституції України» [1]. При цьому важливою є норма ч. 2 ст. 9 ЗУ «Про міжнародні договори України», яка встановлює: «Якщо міжнародним договором України, який набрав чинності в установленому порядку, встановлено інші правила, ніж ті, що передбачені у відповідному акті законодавства України, то застосовуються правила міжнародного договору» [9, ст. 19]. Важливість врахування норм міжнародного права у процесі правозастосування та їх перевага над національними зумовлена вирішенням питання адаптації національного законодавства до міжнародно-правових стандартів у галузі захисту прав людини, що є якісним показником дотримання взятих Україною зобов'язань в рамках Євроінтеграційного процесу. У зв'язку з тим, що зміна внутрішнього законодавства та подальше його реформування здійснюється на основі міжнародних договорів, постає потреба в дослідженні їх змісту у сфері забезпечення права на таємницю спілкування.

Положеннями ст. 12 «Загальної декларації прав людини» від 10.12.1948, передбачено: «ніхто не може зазнавати безпідставного втручання у його особисте і сімейне життя, безпідставного посягання на

недоторканність його житла, тайну його кореспонденції або на його честь і репутацію. Кожна людина має право на захист закону від такого втручання або таких посягань» [8, ст. 12]. Норми декларації стали етичним орієнтиром людства, одним з перших документів, що заклав основу сучасної системи захисту прав людини в сфері приватного життя. «Міжнародний пакт про громадянські та політичні права» від 16.12.1966 так само унормував підхід до захисту цього права, в ст. 17 закріплюється: «ніхто не повинен зазнавати свавільного чи незаконного втручання в його особисте і сімейне життя, свавільних чи незаконних посягань на недоторканність його житла або таємницю його кореспонденції чи незаконних посягань на його честь і репутацію. Кожна людина має право на захист закону від такого втручання чи таких посягань» [28, ст. 17].

В Європейському співтоваристві основним джерелом, яке закріплює та регулює право на приватне життя, є «Конвенція про захист прав людини і основоположних свобод» від 04.11.1950 (далі- ЄКПЛ), ст. 8 якої гарантує невід'ємність права на повагу до приватного і сімейного життя, житла та кореспонденції, а також окреслює винятки, за яких дозволяється тимчасове обмеження цього права: «Органи державної влади не можуть втручатись у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб» [29, ст. 8]. Як бачимо, універсальні міжнародні договори відображують лише зміст права на таємницю спілкування і не розкривають можливості та шляхи обмеження такого права, тоді як ЄКПЛ якісно змінила підхід до унормування цієї проблеми, при цьому не тільки закріплюючи варіативність підстав законного втручання, а й створюючи механізм звернення до «Європейського суду з прав людини» (далі- Суд, ЄСПЛ) з метою захисту права на таємницю кореспонденції, яке не визнається, порушується чи обмежується державою-учасницею Конвенції.

Зокрема, ст. 34 ЄКПЛ регламентує можливість прийняття Судом «заяви від будь-якої особи, неурядової організації або групи осіб, які вважають себе потерпілими від допущеного однією з Високих Договірних Сторін порушення прав, викладених у Конвенції або Протоколах до неї. ЄКПЛ також застерігає, що Суд може брати справу до розгляду лише після того, як було вичерпано всі національні засоби правового захисту, згідно із загальновизнаними принципами міжнародного права, і впродовж чотирьох місяців від дати постановлення остаточного рішення на національному рівні» [29].

Використання у формулюванні ст. 8 ЄКПЛ терміну «повага» є гарантом позитивних і негативних зобов'язань держав-учасниць. Негативне покликане встановити заборону втручання у ці права без відповідного дозволу, водночас позитивні спрямовані на забезпечення існування достатніх правових засобів для вироблення поваги до кореспонденції особи, як у відносинах між державою та особою, так і між приватними особами. При цьому межу між позитивними і негативними зобов'язаннями складно визначити, хоча й принципи, що підлягають застосуванню є подібними, серед них потреба досягнення компромісу між протилежними інтересами. Наприклад, держава повинна забезпечити справедливу рівновагу між правом на повагу до кореспонденції і правом на свободу вираження поглядів, як це було констатовано у рішенні *Benediktsdóttir* проти Ісландії [43].

Беручи до уваги що практика ЄСПЛ є джерелом, яке надає можливість зрозуміти конкретний обсяг прав і свобод, визначених у Конвенції і протоколах до неї, адже як джерело права вона окремо визначена у ЗУ «Про виконання рішень та застосування практики Європейського суду з прав людини» [30], а ч. 5 ст. 9 КПК передбачає, що «Кримінальне процесуальне законодавство України застосовується з урахуванням практики ЄСПЛ» [7, ст. 9], - потребують роз'яснення та аналізу рішення ЄСПЛ в яких порушувалося питання щодо стандартів захисту таємниці спілкування.

Суд встановлюючи факт прийнятності скарги (окрім загальних умов прийнятності заяви, визначених у ст. 35 ЄКПЛ), встановлює, чи підпадає

порушене право під дію ст. 8, потім здійснює перевірку, чи відбулося втручання у це право відповідно до закону, який має відповідати вимогам щодо якості та чи було спрямоване таке втручання на досягнення законної мети, так як ч. 2 ст. 8 містить перелік умов, за яким таке втручання зі сторони держави було виправданим.

ЄСПЛ окреслює сферу застосування статті 8 ЄКПЛ досить широко, навіть за умови, що конкретне право чи його складник не передбачено статтею, наприклад, ЄСПЛ у справі "Класс та інші проти Німеччини" акцентує, що «хоча в пункті 1 статті 8 Конвенції телефонні розмови прямо не згадуються, Суд, як і Комісія, вважає, що такі розмови охоплюються поняттями "приватне життя" та "кореспонденція", які містяться в цьому положенні» [31]. До того ж як свідчать наукові узагальнення, вже не раз у рішеннях ЄСПЛ було актуалізовано, що «окрім традиційних засобів комунікації (листів, поштових відправлень) Суд відносить до кореспонденції: факсові повідомлення, телефонні розмови, електронні листи, повідомлення з пейджерів зміст інформації з мережі Інтернет, яку використовував користувач, приватну інформацію з каналів радіозв'язку, ділову кореспонденцію, пов'язану з діяльністю приватної юридичної особи, електронні бази даних, вилучені під час обшуку, посилки, вилучені працівниками митниці» [32, с. 371]. Тобто Суд розглядає «кореспонденцію» у широкому розумінні, використовуючи принцип динамічного бере до уваги постійно зростаючу інформатизацію суспільства, як фактор розширення видів і способів передачі інформації і наголошує, що вся інформація, яка передається такими пристроями підпадає під захист ст. 8 ЄКПЛ. На правильність цих суджень вказує і формулювання в рішенні *Хелфорд проти Сполученого Королівства*: «переговори за телефонами, встановленими в кабінеті пані Хелфорд в управлінні поліції Мерсисайда, підпадають під поняття «приватного життя» та «кореспонденції» за змістом статті 8 §1, оскільки Суд у своїй практиці прийняв широке тлумачення цих термінів» [39]. Даний підхід, на нашу думку, цілком застосовний і до національного законодавства, адже слідування «широкому»

тлумаченню терміну не обмежує розуміння таємниці спілкування класичними видами зв'язку та дозволяє охопити весь спектр засобів зв'язку сферою дії даного права.

Під спеціальний захист ст. 8 ЄКПЛ підпадають відносини між адвокатом та клієнтом, адже вона гарантує конфіденційність обміну інформацією між адвокатами та їхніми клієнтами в силу невід'ємної ролі адвокатури в суспільстві, діяльність якої може опинитися під загрозою, якщо захисники не зможуть гарантувати своїм підзахисним, що їх спілкування залишиться приватним. Під захист потрапляє і офіс адвоката, його житло, листування, комп'ютерне обладнання та телефонні лінії. Як зазначається в рішенні «*Мишо проти Франції*» (*Michaud v. France*) від 6.12.2012: «згідно зі статтею 8, листування між адвокатом та його клієнтом, незалежно від його мети (включаючи суто професійне листування), користується привілейованим статусом, коли йдеться про конфіденційність а також це стосується усіх форм обміну інформацією між адвокатами та їхніми клієнтами» [40].

Звертаємо увагу, що спілкування на робочому місці за своє суттю також охоплюється дією ст. 8 ЄКПЛ, ЄСПЛ у справі «*Copland v. the United Kingdom*» було констатовано, що «Перевірка користування державним службовцем телефоном, електронною поштою та інтернетом без законодавчої підстави є порушенням, так як коледж був державним органом, за дії якого уряд ніс відповідальність за Конвенцією, то питання стосувалось негативного зобов'язання держави не втручатися у приватне життя та кореспонденцію заявниці. З цього логічно випливало, що електронні повідомлення, надіслані з роботи, а також інформація, отримана від перевірки використання інтернету для власних потреб, так само захищались. Заявниця не отримала ніякого попередження, що її дзвінки будуть перевірятись, а відтак мала розумні очікування щодо конфіденційності дзвінків, зроблених з її робочого телефону. Те ж очікування повинно застосовуватись і до використання нею електронної пошти та інтернету» [35]. При винесенні рішення у справі «*Хелфорд проти Сполученого Королівства*» Судом було так само акцентовано, що

«переговори, які заявниця вела по своїх службових телефонах, підпадають під поняття «приватне життя» і «кореспонденція», оскільки особа могла мати розумні очікування щодо конфіденційності таких переговорів, і ці очікування підкріплювалися цілою низкою чинників, в якості помічника головного констебля вона мала окремий кабінет, де було встановлено два телефони, один з яких був спеціально призначений для її особистого користування» [39]. Як бачимо, Суд при оцінці наявності втручання використовує доктрину «розумного очікування приватності», це необхідно для встановлення того чи дійсно особа могла розраховувати на повагу до свого приватного життя за певних обставин та чи охоплюється таке втручання сферою дії ст. 8 Конвенції. Вже при розгляді заяви «Барбулеску проти Румунії» Суд дійшов висновку, що для того, аби перевірка переписки була правомірною, працівник має бути попереджений про особливості її проведення перед її початком [36], дане рішення позитивно змінило підхід до розгляду даної категорії справ, встановивши критерії, якими мають керуватися національні органи при оцінці пропорційності заходів роботодавця, які вживаються для контролю за перепискою працівників.

Ризик незаконного втручання в право на таємницю спілкування наразі стає дедалі вищим, адже навіть поштарка відкривши та прочитавши лист сторонньої особи може фактично здійснити акт втручання у приватне листування, не говорячи вже про те, яка відповідальність покладається на працівників правоохоронних органів в рамках розслідування, аби попередити несанкціонований доступ до приватної кореспонденції. Суд вимагає та наголошує, що «будь-яке втручання держави у право особи на повагу до приватного життя та кореспонденції має здійснюватися у відповідності до закону. Цей вираз не лише вимагає дотримання внутрішнього законодавства, також має відношення до якості цього закону, вимагаючи його сумісності з принципом верховенства права» [39]. В науковій літературі зазначається, що «Суд розробляючи концепцію законності, визначив, що законність (втручання здійснюється згідно із законом) стосується не лише національного

законодавства, а й верховенства права – принципу, спільного для демократичних суспільств. Не може бути законності, якщо особа не має змоги оскаржити межі цієї законності, тобто рішення державно-владних органів. У цій думці Суд підкреслив, що будь-яке втручання в права осіб з боку виконавчої влади має бути підконтрольним, причому судовий контроль є найефективнішим, оскільки він гарантує незалежність, неупередженість і дотримання процедури» [32, с. 351].

У справі ЄСПЛ «Габріель Вебер і Цезар Річард Саравія проти Німеччини» роз'яснюється, що «вираз «відповідно до закону», за змістом статті 8 § 2, означає, по-перше, що заходи, що оскаржуються, повинні мати підставу в національному законодавстві; воно також указує на якість відповідного закону, вимагаючи, щоб інформація була доступна зацікавленим особам, які повинні мати можливість передбачити наслідки моніторингу, і вимагає сумісності із принципом верховенства права» [37]. До прикладу, про порушення ст. 8 ЄКПЛ було визнано у справі «Ліберті та інші проти Сполученого Королівства» лише через те, що «закон про обмін, зберігання та знищення перехоплених матеріалів не було сформульовано у доступній для публіки формі, як це вимагає прецедентне право Суду і втручання в права заявників відповідно до статті 8 таким чином відбувалося не «відповідно до закону»» [38]. У заяві «Хеглас проти Чеської Республіки» Суд також констатував, що «прослуховування телефонних розмов заявника та запис розмов на аудіо-плівку під час особистих зустрічей не було здійснено «відповідно до закону», і постановив про порушення ст. 8 ЄКПЛ. Спираючись на свою прецедентну практику, Суд дійшов висновку, що зазначений захід не відповідав усім вимогам, сформульованим Судом у його попередніх рішеннях стосовно таких категорій справ. Зокрема, національний закон не визначав з достатньою чіткістю межі і способи доступу, контроль та використання інформації, отриманої шляхом таємного підслуховування та запису» [34]. Про недотримання ст. 8 Конвенції в частині «якості закону» було констатовано і в справах, щодо України. У рішенні «Беляєв та Дігтяр проти України від

16.02.2012 зроблено висновок про «порушення щодо прав обох заявників на повагу до кореспонденції під час попереднього ув'язнення в Сумському СІЗО у зв'язку з тим, що відповідне національне законодавство на той час не відповідало стандартам «якості закону» і що відсутність відповідних гарантій могла призвести до незаконної відмови надіслати деякі листи заявників» [45].

Критерій «у відповідності до закону» також вимагає аби вітчизняне законодавство було «в достатній мірі передбачуваним у частині, що стосується надання особам відповідної вказівки стосовно обставин та умов, за яких органи влади будуть мати право вдатися до заходів, що спричинить наслідки щодо їхніх прав (справа Фернандес Мартінес проти Іспанії)» [41], проте передбачуваність у спеціальному контексті таємних заходів нагляду, таких як перехоплення повідомлень, «не може означати, що особа повинна мати можливість передбачити, коли органи влади, можуть перехопити її повідомлення, щоб мати можливість відповідно адаптувати свою поведінку (справа *Leander v. Sweden*)» [42].

Акцентуємо, що втручання буде виправданим лише тоді, коли відповідає умовам пункту 2 статті 8, якщо воно "відповідає закону", а також переслідує одну або кілька законних цілей, зазначених у пункті 2, і є "необхідним у демократичному суспільстві" для досягнення наперед обумовлених цілей. Хоча й сам факт наявності в національному законі можливості встановлення таємного моніторингу зв'язку може потенційно спричинити загрозу нагляду за усіма, до кого така норма може застосовуватися, проте подекуди це єдиний механізм, аби встановити істину у справі. З цього ж приводу ЄСПЛ у рішенні в справі «Класс та інші проти Федеративної Республіки Німеччини» (1978 р.) зазначає, що «існування законодавства, що дає повноваження по здійсненню спостереження за листуванням, поштовими відправленнями і телефонними розмовами, є у виключних випадках необхідним у демократичному суспільстві в інтересах національної безпеки або для попередження безладдя або злочинів. При цьому у правовій державі повинні існувати адекватні і ефективні гарантії проти зловживання з боку органів державної влади,

уповноважених на здійснення такого спостереження» [31, с. 93-125]. До прикладу, у справі «Бен Файза проти Франції» (заява № 31446/12) Суд визнав, що «не було порушення статті 8 КЗПЛ щодо наказу суду, виданого оператору мобільного зв'язку 24 липня 2009 року, для отримання переліку стільникових вишок, прив'язаних до телефону пана Бен Файза для подальшого відстеження його пересувань. Суд встановив, що хоча й судовий наказ, виданий телефонному оператору, що дозволив владі отримати доступ до записів, що містять переліки дзвінків є втручанням у приватне життя особи, але відповідав закону та був спрямований на досягнення законної мети (запобігання заворушенням або злочину тощо). Крім того, ці заходи були необхідними в демократичному суспільстві, оскільки вони були спрямовані на перешкоджання масштабній оборудці з торгівлі наркотиками, а отримана інформація була використана під час розслідування у кримінальному провадженні, в ході якого пану Бен Файза було гарантовано ефективний розгляд, який відповідає верховенству права» [33]. У рішенні Adomaitis проти Литви Суд відзначає роль прослуховування телефонних розмов у контексті розслідування, якщо воно відповідає закону та є «необхідним для демократичного суспільства», зокрема для забезпечення громадської безпеки або запобігання заворушенням чи злочинам. Відзначається, що такі заходи допомагають поліції та судам у їхній діяльності з попередження та покарання кримінальних правопорушень або, у контексті корупційної діяльності, для забезпечення прозорості публічної установи [46, с. 149].

З вищенаведеного випливає, - аби встановити чи є втручання в охоронювані ст. 8 ЄКПЛ права «необхідним у демократичному суспільстві» суд застосовує метод співвідношення інтересів держави члена порівняно з правами заявника, враховуючи тяжкість вчиненого правопорушення, суспільну небезпеку та важливість для слідства отримати інформацію саме в такий спосіб. З цього приводу у справі "Роман Захаров проти Росії" ЄСПЛ зазначав: «оцінка також залежить від всіх обставин справи, таких, як характер, масштаби і тривалість можливих заходів, підстави, необхідні для наказу про

їх здійснення, органи, уповноважені вирішувати, здійснювати та контролювати їх, і засоби правового захисту, передбачені національним законодавством. Суд повинен визначити, чи є процедури контролю за впровадженням і здійсненням обмежувальних заходів достатніми для того, щоб «втручання» обмежувалося «необхідним у демократичному суспільстві» способом» [44]. В більшості справ з'ясування саме цієї вимоги є найскладнішим, адже не є достатнім, аби втручання просто належало до винятків встановлених п.2 ст. 8 ЄКПЛ чи підпадало під дію вітчизняної норми, представленої у формі абстрактних категорій, аби легітимізувати посягання на сферу приватного життя. ЄСПЛ повинен впевнитися, що втручання у взаємозв'язку з фактичними обставинами справи справді було необхідним та виправданим.

В контексті дослідження практики ЄСПЛ можемо констатувати, що втручання у приватне спілкування суперечитиме статті 8 Конвенції, якщо воно відбувається не «згідно із законом» (якщо закон не відповідає вимогам щодо якості та передбачуваності застосування), не має однієї або декількох легітимних наперед обумовлених цілей, зазначених у пункті 2 статті 8 Конвенції (втручання має переслідувати легітимну мету - захист національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб), а також не є «необхідним у демократичному суспільстві» (якщо не було дотримано принципу пропорційності інтересів і доводи, надані національними органами влади на його виправдання не були важливими та достатніми) для досягнення цих цілей.

1.3 Учасники кримінального провадження та таємниця спілкування

Таємниця спілкування, як засада кримінального провадження набуває особливого значення у взаємодії з учасниками кримінального провадження. КПК поділяє їх на суд, сторони (сторону обвинувачення та захисту), потерпілого та його представника, інших учасників кримінального провадження [7]. Суд, суддя, слідчий суддя, прокурор, слідчий, керівник органу досудового розслідування, оперативні підрозділи покликані забезпечити реалізацію цієї засади шляхом неухильного дотримання вимог Конституції України, КПК, міжнародних договорів, інших актів законодавства під час прийняття процесуальних рішень, особи, які захищають чи представляють свої інтереси в свою чергу мають право вимагати дотримання їх прав на всіх етапах кримінального провадження, не зловживати наданими процесуальними можливостями та оскаржувати рішення уповноважених осіб. Запропонований поділ на групи дозволяє відмежувати процесуальне становище учасників виходячи з їх ролі в забезпеченні таємниці спілкування.

Найбільш тісно з забезпеченням таємниці спілкування пов'язані ті суб'єкти, які подають клопотання про втручання у приватне спілкування, приймають рішення щодо надання дозволу на їх проведення та здійснюють виконання, при цьому їх процесуальна роль не обмежується виключно цими повноваженнями, тому вважаємо за необхідне дослідити особливості та проблематику правового статусу кожного з них:

Слідчий будучи службовою особою одного з органів визначених в п.17 ч.3 КПК, уповноважений здійснювати підготовку клопотання до слідчого судді про надання дозволу на проведення НСРД та звертається з ним до прокурора з метою погодження та повідомляє прокурора про прийняті ним рішення стосовно проведення певних НСРД та отримані результати [7, ч. 3 ст. 246].

Слідчий проводить НСРД у випадках, коли здійснює досудове розслідування кримінального правопорушення та надає доручення на проведення НСРД. За його вказівкою можуть діяти: «уповноважені оперативні підрозділи, а за рішенням слідчого чи прокурора до проведення негласних слідчих (розшукових) дій можуть залучатися також інші особи» [7, ч. 6 ст. 246]. На практиці саме оперативні працівники найчастіше проводять НСРД, А. А. Коваль в своїй монографії наводить результати опитування серед працівників органів досудового розслідування, яке свідчить, що «менше 10% слідчих проводять НСРД самостійно» [48], це обумовлено тим, що такі підрозділи наділені спеціальним технічним та методичним забезпеченням необхідним для проведення НСРД в найкоротші строки та з досягненням найбільшої ефективності, що дозволяє слідчим делегувати проведення НСРД без втрати якості. До безпосередніх повноважень слідчого належить також здійснювати огляд та виїмку кореспонденції, знімати копії чи отримувати зразки, надавати доручення про повернення оглянутої кореспонденції адресату. Вивчати інформацію отриману за результатами застосування спеціальних технічних засобів.

Прокурор, як представник сторони обвинувачення покликаний здійснювати наглядову функцію через процесуальне керівництво досудовим розслідуванням, відповідно до ст. 25 ЗУ «Про прокуратуру»: «прокурор здійснює нагляд за додержанням законів органами, що провадять оперативно-розшукову діяльність, дізнання, досудове слідство, користуючись при цьому правами і виконуючи обов'язки, передбачені Законом України «Про оперативно-розшукову діяльність» та Кримінальним процесуальним кодексом України» [49, ст. 25]. Основна мета його діяльності полягає у забезпеченні та утвердженні прав учасників провадження, прийняття обґрунтованих і процесуально доцільних рішень, дотримання засади розумності строків та законності розслідування у цілому, особливість прокурорського контролю в сфері НСРД з метою дотримання таємниці спілкування зводиться того, аби надати оцінку правомірності конкретної дії з точки зору її правової

обґрунтованості та необхідності вчинення, шляхом наділення його наступними повноваженнями:

- Згідно ч. 2 ст. 258 КПК: «Звертається до слідчого судді з клопотанням про дозвіл на втручання у приватне спілкування (або погоджує таке клопотання слідчого) в порядку, регламентованому статтями 246, 248, 249 КПК, якщо будь-яка слідча (розшукова) дія включатиме таке втручання» [7]. Предметом контролю за даних обставин буде перевірка дотримання законних підстав для проведення НСРД, їх обґрунтованість та необхідність. Прокурор погоджуючи клопотання слідчого повинен бути впевнений, що отримати докази у справі іншим шляхом неможливо, а сам характер розслідуваного злочину потребує такого втручання.

- На виконання вимог ч. 1 ст. 255 КПК: «Приймає рішення про знищення відомостей, речей та документів, отриманих в результаті проведення негласних слідчих (розшукових) дій, які він не визнає необхідними для подальшого проведення досудового розслідування» [7], з метою забезпечення режиму таємності та секретності, що притаманно для самої суті НСРД. Дане повноваження корелюється з вимогами ч. 3 ст. 14 КПК, яка зобов'язує не використовувати інформацію отриману внаслідок втручання у спілкування для цілей не пов'язаних з вирішенням завдань кримінального провадження. Проте, згідно ч. 1 ст. 257 КПК: «якщо в результаті проведення НСРД виявлено ознаки кримінального правопорушення, яке не розслідується у даному кримінальному провадженні, то отримана інформація може бути використана в іншому кримінальному провадженні тільки на підставі ухвали слідчого судді, яка приймається за клопотанням прокурора. Передання інформації, одержаної внаслідок проведення НСРД, здійснюється тільки через прокурора відповідно до ч. 2 ст. 257 КПК» [7]. Тут мається на увазі весь масив інформації, що знаходиться в протоколах НСРД, клопотаннях, постановках, додатках. Використання такої інформації знаходиться під суворим контролем, наприклад, у Постанові ККС ВСУ у справі № 751/7177/14 від 21.03.2018: «Суд визнав недопустимими докази отримані в ході здійснення іншого досудового

розслідування з огляду на положення статей 86, 87 КПК, так як у матеріалах кримінального провадження відсутня відповідна ухвала слідчого судді про використання результатів вказаних негласних слідчих дій у іншому кримінальному провадженні, як того вимагає ст. 257 КПК» [47]. КПК в ч.1 ст. 253 висуває вимоги щодо обов'язкового «повідомлення в письмовому вигляді прокурором чи слідчим за його дорученням осіб, конституційні права яких були тимчасово обмежені під час проведення НСРД, а також підозрюваного і його захисника про таке обмеження, в тому числі, коли такі матеріали знищені» [7], і хоча дана норма продукує додаткові гарантії для осіб, у приватне спілкування яких втручалися, проте відсутність в статті вимоги щодо змісту такого сповіщення дозволяє стороні обвинувачення самостійно вирішувати, який перелік та обсяг отриманої оперативної інформації буде розкритий особам. Особливо складні випадки в ситуаціях, коли матеріали проведених НСРД були знищені, адже тоді працівники органу досудового розслідування можуть діяти на власний розсуд та обмежитися лише коротким повідомленням про факт втручання у приватне спілкування.

- Забезпечує збереження всієї інформації або надає доручення слідчому забезпечити таке збереження шляхом створення належних умов для запобігання несанкціонованому доступу, поширенню і використанню, у випадках, коли згідно ст. 259 КПК «прокурор має намір використати під час судового розгляду як доказ інформацію, отриману внаслідок втручання у приватне спілкування, або певний її фрагмент» [7].

Слідчий суддя, в силу особливостей свого правового статусу, здійснює судовий контроль за дотриманням прав і свобод людини під час проведення НСРД шляхом постановлення «ухвали слідчого судді про дозвіл на проведення НСРД» за результатами розгляду клопотання прокурора чи слідчого погодженого з прокурором, виконуючи при цьому дослідження обставин справи з метою встановлення відсутності чи наявності переконливих факторів, що дозволяли б досягти завдань кримінального провадження саме шляхом втручання у приватне спілкування. Ця діяльність пов'язана із

перевіркою суддею законності правових підстав для проведення НСРД. Звертаємо увагу, що в КПК відсутній обов'язок прокурора повідомляти слідчого суддю про припинення НСРД, рішення на проведення яких він надавав, на нашу думку це звужує сутність судового контролю, адже інформування слідчого судді щодо неможливості подальшого проведення відповідних заходів з належним обґрунтуванням може запобігти випадкам, коли припинення зумовлюється необ'єктивними чинниками. Фактично після винесення ухвали повноваження слідчого судді припиняються, адже до його компетенції не входить подальший контроль за виконанням рішення чи можливість отримувати сповіщення про хід проведення НСРД, А.С. Гуменюк з цього приводу відзначає, що пріоритетом повинно стати: «розширення можливостей цього суб'єкта у сфері контролю за органами та особами, що приймають рішення та проводять НС(Р)Д, з тим, щоб його повноваження не закінчувалися на етапі надання/відмови у наданні дозволу на проведення відповідних процесуальних дій, а поширювалися на весь процес проведення негласного заходу» [50], ми розділяємо дану позицію, адже такі зміни можуть запобігти зловживанням з боку органів досудового розслідування, бо слідчий суддя матиме змогу припинити незаконні дії уповноважених осіб та не допустити застосування у доказуванні результатів НСРД, які отриманні з порушенням процедурних правил. А. С. Гуменюк у своєму дисертаційному дослідженні, оцінюючи існуючий стан законодавства, стверджує: «чинне кримінальне процесуальне законодавство істотно обмежує повноваження слідчого судді щодо реалізації наступного судового контролю, що потенційно створює дисбаланс у механізмах контролю та ризик надмірної концентрації повноважень у руках окремих учасників кримінального провадження» [51 с. 81]. Таким чином, значення судового контролю суттєво применшується законодавцем, що призводить до системних проблем у процедурі нагляду за виконанням рішень про втручання у приватне спілкування.

Окрему увагу слід приділити таким учасникам кримінального провадження, як захисник та священнослужитель, адже на них поширюється

дія так званого професійного привілею, який забезпечує виключну конфіденційність. За жодних умов втрутитися в їх спілкування є неможливим, крім того вони не можуть бути допитані з питань, які становлять адвокатську таємницю чи відомості отримані під час сповіді. КПК в ч.5 ст. 258 містить досить категоричне положення, яке наголошує, що «Втручання у приватне спілкування захисника, священнослужителя з підозрюваним, обвинуваченим, засудженим, виправданим заборонене», крім того, ст. 161 КПК заборонено «доступ до речей і документів, які є листуванням або іншою формою обміну інформацією між захисником та його клієнтом або будь-якою особою, яка представляє його клієнта» [7], так законодавець забезпечує гарантоване приватне та комфортне середовище для спілкування та надання професійної правничої допомоги, в якому унеможлиблюється перехоплення чи відслідковування змісту, часу та характеру розмови чи доступу до документів пов'язаних з наданням правової допомоги. Про недопустимість втручання у приватне спілкування захисника із засудженим наголошується і у «Кримінально-виконавчому кодексі України», ч. 5 ст. 113 передбачено: «Кореспонденція, яку засуджені адресують захиснику у кримінальному провадженні, що здійснює свої повноваження відповідно до КПК, перегляду не підлягає і надсилається за адресою протягом доби з часу її подачі. Кореспонденція, яку засуджені одержують від такого захисника, перегляду не підлягає» [52, ч. 5 ст. 113]. Такий підхід законодавця свідчить про особливу повагу до спілкування між даними учасниками провадження, що узгоджується з аналізованими напрацюваннями міжнародної правової доктрини та втілює найвищі стандарти, які висуває ЄСПЛ в своїх рішеннях.

Крім того, на адвоката покладається особливе завдання в рамках кримінального провадження – це забезпечення ефективного захисту, яке досягається через контроль за законністю проведених НСРД (на наявність постанови чи ухвали на їх проведення, відповідність вимогам глави 21 КПК), дотриманням строків проведення, відповідністю суб'єкта, який надав дозвіл

на проведення НСРД, а разі чого і на оскарження дій працівників правоохоронних органів.

Допоміжну роль у процесі забезпечення таємниці спілкування виконує спеціаліст, його залучають під час і після проведення НСРД для надання технічної допомоги чи пояснень, за умови володіння ним спеціальними навичками застосування технічних засобів та необхідності їх застосування в конкретному випадку на підставі клопотання про залучення спеціаліста або використання його пояснень і допомоги, наприклад, згідно ч.1 ст. 266 КПК: «дослідження інформації, отриманої при застосуванні технічних засобів, у разі необхідності здійснюється за участю спеціаліста» [7]. На нього також покладається обов'язок не розголошувати відомості, які стали відомі під час здійснення його професійної діяльності.

Експерти залучаються за зверненням сторони чи дорученням слідчого судді чи суду для проведення експертизи, пов'язаної з матеріалами НСРД за умови володіння ними спеціальними технічними, науковими та іншими знаннями згідно з ЗУ «Про судову експертизу». Як зазначається в ч.3 ст. 266 КПК: «Носії інформації, на яких зафіксовані відомості, отримані в результаті проведення зазначених негласних слідчих (розшукових) дій, можуть бути предметом дослідження відповідних спеціалістів або експертів у порядку, передбаченому цим Кодексом» [7].

Висновки до розділу I

Підсумовуючи розгляд розділу 1 «Поняття та зміст таємниці спілкування, як засади кримінального провадження», можна сформулювати наступні висновки:

1. Встановлено, що доктринальне розуміння таємниці спілкування, як засади кримінального провадження трактує її як багатовимірну процесуальну гарантію, яка є втіленням фундаментального конституційного права особи на

таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції. Дане право слід розглядати як невід'ємну складову права на повагу приватного (особистого) і сімейного життя особи, так як обсяг останнього є набагато ширшим та включає, зокрема, комунікативний елемент. Доктринальний підхід до розуміння об'єктів захисту таємницею спілкування є ширшим, порівняно з законодавчим. Предметом захисту визнаються не тільки класичні види комунікації (листи, телефонні дзвінки), а й весь обсяг інформації, що передається з використанням новітніх засобів зв'язку (месенджери, електронна пошта, мобільні застосунки).

2. Констатовано, що «таємницю спілкування, як засаду кримінального провадження» слід розуміти як нормативно визначену гарантію, що дозволяє кожному під час здійснення кримінального провадження розраховувати на «таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції, інших форм спілкування», яка може бути обмежена виключно на підставі рішення суду у чітко визначених законом випадках.

3. Обґрунтовано, що законодавче закріплення засади «таємниці спілкування» в КПК є відображенням високого розвитку та демократичності держави, свідчить про повагу до прав людини та втілює найкращі історичні здобутки. При цьому проблему становить відсутність нормативної визначеності щодо обсягу та цілісності змісту понять: «кореспонденція», «листування», «телефонні розмови», «телеграфна кореспонденція», «інші види спілкування». Це призводить до того, що значна частина інформації, яка за своєю суттю становить об'єкт охорони, залишається поза правовим регулюванням. Доведено, що правова недосконалість окремих положень закону щодо забезпечення таємниці спілкування унеможливорює належну реалізацію завдань, закріплених у ст. 2 КПК, а таке законодавство через низьку якість не здатне всебічно забезпечити охорону прав і свобод людини.

4. Досліджено, що міжнародні стандарти у галузі захисту таємниці спілкування становлять основу розвитку національного права, вони не тільки встановлюють мінімальні гарантії, а й якісно регулюють порядок та умови

обмеження права. Практика ЄСПЛ щодо тлумачення та захисту норм ЄКПЛ, визнана джерелом права в Україні та на сьогодні є одним з регуляторів питань, які українським законодавством не охоплюються. ЄСПЛ використовуючи принцип «динамічного тлумачення», інтерпретує ЄКПЛ в світлі сучасних соціальних і технологічних реалій. Під предметом охорони таємницею спілкування суд визначає весь обсяг комунікацій особи – від звичайних листів, телеграм та факсимільних повідомлень до спілкування з використанням інформаційно-комунікаційних технологій. Втручання визнається виправданим, якщо здійснюється згідно із законом, має одну чи декілька легітимних цілей та є необхідним у демократичному суспільстві для досягнення цих цілей.

5. Встановлено, що взаємодія учасників кримінального провадження з таємницею спілкування виявляється в наділенні кожного з цих специфічними гарантіями та завданнями. Слідчий погоджує клопотання про дозвіл на проведення НСРД, надає доручення на їх проведення та координує процес. Прокурор здійснює наглядову функцію, як представник сторони обвинувачення через процесуальне керівництво досудовим розслідуванням. Слідчий суддя в свою чергу, забезпечує здійснення судового контролю, який, як нами досліджено є поверхневими та обмеженими. Повноваження слідчого судді закінчуються на етапі надання дозволу, без інструментів подальшого нагляду за виконанням рішення чи можливості отримувати сповіщення про хід проведення та підстави припинення НСРД, яка була попередньо ним санкціонована. Автором запропоновано розширити сферу контролю шляхом встановлення обов'язку щодо повідомлення слідчого судді про підстави припинення та результати проведення санкціонованих ним НСРД.

РОЗДІЛ II. ПРОЦЕСУАЛЬНІ ДІЇ, ЩО ОБМЕЖУЮТЬ ТАЄМНИЦЮ СПІЛКУВАННЯ

2.1. Підстави та процесуальний порядок обмеження таємниці спілкування

Таємниця спілкування не є абсолютним правом особи і це цілком узгоджується з міжнародними стандартами та національною доктриною, перш за все, про винятковість втручання йдеться в ст. 31 КУ, яка дозволяє за наявності виключних правових та формальних підстав втрутитись в таємницю спілкування з метою запобігання злочинів чи з'ясування істини при розслідуванні справи, проте за умов, коли отримати інформацію в інший спосіб неможливо. Конституційне твердження корелюється з положеннями ч. 2 ст. 14 КПК, згідно якої: «втручання у таємницю спілкування можливе лише на підставі судового рішення у випадках, передбачених цим Кодексом, з метою виявлення та запобігання тяжкому чи особливо тяжкому злочину, встановлення його обставин, особи, яка вчинила злочин, якщо в інший спосіб неможливо досягти цієї мети» [7], аналогічні підстави втручання передбачені й ч. 2 ст. 246 КПК. Такі винятки є об'єктивно зумовленою реакцією держави, стримуючим фактором перед безладдям та злочинами, можливість обмеження є необхідною передумовою не тільки для встановлення істини у справі, а й для захисту інших осіб та суспільства.

Підстави втручання можна виділити у дві групи – фактичні, які вказують на мету проведення та юридичні, що позначають сформульовані у КПК вимоги за дотримання яких втручання легітимізується. До фактичних належить встановлена слідчим чи прокурором неможливість отримати інформацію про кримінальне правопорушення та особу, що його вчинила інакшим способом, ніж шляхом тимчасового обмеження таємниці спілкування та необхідність органу досудового розслідування діяти негласно в інтересах провадження. Вважаємо неможливим з достатньою чіткістю виділити

складники категорії «неможливість отримання у інший спосіб», адже оцінка залежить від особливостей конкретної справи та окремих факторів, які впливають на успішність її досудового розслідування, включаючи особу правопорушника. Тут основна роль відводиться навичкам аналізу слідчого, прокурора та слідчого судді які повинні розглядати кожну ситуацію комплексно, усвідомлюючи, що під загрозою потенційно може опинитися конституційне право особи. Юридичною підставою ж буде - прийняте уповноваженою законом особою та в встановленому порядку рішення про проведення НСРД. Пов'язуючи підстави між собою нам імпонує думка Ю. М. Мирошниченко, який зазначає: «фактичними підставами для ухвалення рішення щодо проведення НСРД є отримані з належного процесуального джерела відомості (фактичні дані, докази), які підтверджують наявність юридичних умов, що передбачені в КПК» [54].

Безпосереднє обмеження таємниці спілкування здійснюється при проведенні певних НСРД, серед яких відповідно до ст. 258 КПК є: «аудіо-, відеоконтроль особи; арешт, огляд і виїмка кореспонденції; зняття інформації з електронних комунікаційних мереж; зняття інформації з електронних інформаційних систем» [7]. Для того щоб отримати дозвіл на проведення НСРД у вигляді ухвали слідчого судді прокурор чи слідчий за погодженням з прокурором звертається до слідчого судді з клопотання про дозвіл на втручання у приватне спілкування.

Клопотання повинно відповідати критеріям викладеним у ч. 2 ст. 248 КПК та складатися з вступної, мотивувальною та заключної частини, що повинні містити інформацію про:

- «1) найменування кримінального провадження та його реєстраційний номер;
- 2) короткий виклад обставин кримінального правопорушення, у зв'язку з розслідуванням якого подається клопотання;
- 3) правова кваліфікація кримінального правопорушення із зазначенням статті (частини статті) Кримінального кодексу України;

- 4) відомості про особу (осіб), місце або річ, щодо яких необхідно провести негласну слідчу (розшукову) дію;
- 5) обставини, що дають підстави підозрювати особу у вчиненні кримінального правопорушення;
- 6) вид негласної слідчої (розшукової) дії та обґрунтування строку її проведення;
- 7) обґрунтування неможливості отримання відомостей про кримінальне правопорушення та особу, яка його вчинила, в інший спосіб;
- 8) відомості залежно від виду негласної слідчої дії про ідентифікаційні ознаки, які дозволять унікально ідентифікувати абонента спостереження, електронну комунікаційну мережу, кінцеве (термінальне) обладнання тощо;
- 9) обґрунтування можливості отримання під час проведення негласної слідчої (розшукової) дії доказів, які самостійно або в сукупності з іншими доказами можуть мати суттєве значення для з'ясування обставин кримінального правопорушення або встановлення осіб, які його вчинили» [7, ст. 248].

Клопотання не може ґрунтуватися на загальних міркуваннях, припущеннях чи гіпотетичних ризиках, воно повинно містити детально викладені, логічно послідовні, об'єктивно підтверджені обставини справи, що свідчать про необхідність такого втручання. До клопотання обов'язково додається витяг з Єдиного реєстру досудових розслідувань щодо кримінального провадження, у рамках якого подається клопотання, адже його відсутність призводить до визнання недопустимими доказів, отриманих у результаті проведення НСРД на підставі такої ухвали, про що свідчить постанова ВСУ у справі № 235/5633/18 від 07.10.2020 р. [53].

Звертаємо увагу, що на практиці виникають ситуації, коли сторона обвинувачення вдається до штучного створення матеріалів досудового розслідування з визначенням більш тяжких правових кваліфікацій, так до ЄРДР вносяться відомості про більш тяжкий злочин з метою створити формальні підстави для втручання у приватне спілкування і тоді обмеження

таємниці спілкування фактично здійснюється незаконно. Як зазначається у Постанові ККС ВСУ від 14.05.2024: «Про штучність підстав свідчить те, що під час послідуючого розслідування не встановлено відомостей, які не були відомі стороні обвинувачення на час внесення відомостей до ЄРДР і звернення за дозволами на проведення НСРД» [55], таким чином, за відсутності на час проведення НСРД реальних передумов відносити відповідне діяння до категорії тяжких злочинів (коли така кваліфікація була помилково застосована або умисно завищена), інформація, отримана в результаті цих дій, не може набувати статусу допустимого доказового матеріалу, проте в Постанові ККС ВСУ від 24.01.2022 викладається правова позиція згідно якої, «проведення НСРД у кримінальному провадженні щодо тяжкого злочину з подальшою зміною кваліфікації на менш тяжкий злочин не становить порушень вимог КПК (ч. 2 ст. 246), якщо відсутні підстави вважати дії правоохоронних органів щодо попередньої кваліфікації, за якою відомості були внесені до ЄРДР, умисними, здійсненими з метою отримати докази шляхом проведення НСРД» [56]. Проблематика виникає і через те, що на етапі розгляду клопотання про дозвіл на проведення НСРД у слідчого судді немає можливості отримати відомості на підтвердження правильності кваліфікації і те, яким чином він повинен встановлювати, що вчинене правопорушення відповідної тяжкості – залишається відкритим і є підтвердженням думки, що контроль слідчого судді за дотриманням прав, свобод та інтересів осіб у кримінальному провадженні є обмеженим. Правової визначеності з цього питання можна досягти, якщо внести зміни до п. 3 ч. 2 ст. 248 КПК, щодо обов'язку зазначення в клопотанні не тільки правової кваліфікації діяння, а й обґрунтування наявності у сторони обвинувачення переконливих підстав, що кримінальне правопорушення і на момент внесення відомостей до ЄРДР, і на час звернення з клопотанням відповідає необхідному ступеню тяжкості.

У випадках, коли слідчий на виконання вимог ч. 3 ст. 246 КПК звертається до прокурора з метою погодження клопотання про дозвіл на проведення НСРД, що передбачають втручання у приватне спілкування

виникає проблема в відсутності порядку такого узгодження в КПК, натомість це питання регламентує «Інструкція про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні» (Далі - Інструкція), п.2.4 якої передбачає: «Розгляд та погодження прокурором клопотання слідчого про надання дозволу на проведення НСРД здійснюється невідкладно з моменту надходження. Прокурором вивчаються матеріали кримінального провадження, які є підставою для прийняття рішення про погодження клопотання. Відмова в погодженні клопотання приймається у формі постанови і не виключає повторного звернення слідчого після отримання додаткових доказів або усунення недоліків, вказаних прокурором у рішенні» [57]. У випадках відмови у погодженні клопотання відповідно до ч. 3 ст. 40 КПК слідчий може «звернутися до керівника органу досудового розслідування, який після вивчення клопотання за необхідності ініціює розгляд питань, порушених у ньому, перед прокурором вищого рівня, який протягом трьох днів погоджує відповідне клопотання або відмовляє у його погодженні» [7].

Клопотання відповідно до ст. 247 КПК повинно бути розглянуто «слідчим суддею апеляційного суду в межах територіальної юрисдикції якого знаходиться орган досудового розслідування, а в кримінальних провадженнях щодо кримінальних правопорушень, віднесених до підсудності Вищого антикорупційного суду, - слідчим суддею Вищого антикорупційного суду» [7]. Особлива увага законодавця приділяється термінам розгляду такого клопотання, слідчий суддя відповідно до ч. 1 ст. 248 КПК повинен «розглянути клопотання про надання дозволу на проведення негласної слідчої (розшукової) дії протягом шести годин з моменту його отримання за обов'язкової участі особи, яка подала клопотання» [7], такий термін розгляду, на нашу думку, є оптимальним для того щоб ознайомитися з матеріалами провадження та водночас запобігти втратам важливої для слідства інформації, яку потенційно можна отримати.

Завданням слідчого судді при постановленні ухвали про надання дозволу на втручання у приватне спілкування є у взаємозв'язку з відомостями зазначеними в клопотанні відповідно до вимог ч. 3 ст. 248 КПК встановити: «1) чи є вчинене кримінальне правопорушення відповідної тяжкості, 2) чи можливо під час НСРД отримати докази, які самостійно або в сукупності з іншими доказами можуть мати суттєве значення для з'ясування обставин кримінального правопорушення або встановлення осіб, які вчинили кримінальне правопорушення» [7]. Як вже зазначалося, крім витягу з ЄРДР щодо кримінального провадження стосовно якого було подано клопотання, будь-які додаткові матеріали не додаються і фактом розгляду в суді є лише дані, які заявлені в клопотанні. Єдиною можливістю отримати додаткові відомості є п. 2.2. Інструкції, що дозволяє на вимогу слідчого судді на підтвердження необхідності проведення НСРД надати матеріали провадження [57], так у слідчого судді хоча б виникає змога дізнатися чи були вичерпані в рамках провадження всі менш інвазивні способи отримання доказової бази перед тим, як до нього звернулися з клопотанням. Це чудова процесуальна можливість, проте врегульована повинна бути не Інструкцією, а КПК. З цього приводу В. О. Шерудило пропонує доповнити ч.2 ст. 248 КПК положенням, що «для підтвердження необхідності проведення НСРД, пов'язаних з втручанням у приватне спілкування, на вимогу слідчого судді надаються матеріали кримінального провадження» [58, с. 313], що вважаємо слушною пропозицією, яка вплине на якість кримінального процесуального закону. При розгляді клопотання повинен братися до уваги і строк між внесенням відомостей до ЄРДР та моментом звернення з клопотанням до слідчого судді, якщо минуло занадто мало або, навпаки, надто багато часу, виникають сумніви в необхідності такого втручання. Надто короткий строк може свідчити, що інші слідчі дії не проводились, а надто тривалий про втрату моменту та сумнівну ефективність НСРД. І знову ж таки наголошуємо, що кожна справа індивідуальна і найважливішу роль тут відіграє внутрішнє переконання судді,

що повинно ґрунтуватися на оцінці всіх ризиків втручання в співвідношенні з інтересами слідства.

Ухвала слідчого судді про дозвіл на проведення НСРД повинна відповідати загальним вимогам до судових рішень викладених у главі 29 КПК та додатково містити: «відомості про прокурора, слідчого, який звернувся з клопотанням; кримінальне правопорушення щодо якого видається ухвала; особу, місце або річ стосовно яких потрібно провести НСРД; вид НСРД та відомості залежно від типу НСРД про ідентифікаційні ознаки, що дозволять ідентифікувати абонента спостереження, електронну комунікаційну мережу чи кінцеве обладнання; строк дії ухвали» [7]. Строк дії ухвали за загальним правилом не може становити більше 2 місяців, якщо строк проведення НСРД потрібно продовжити, то в порядку ст. 248 КПК «слідчий, прокурор має право звернутися до слідчого судді з клопотанням про постановлення ухвали про продовження НСРД» [7]. При цьому слідчий, прокурор в клопотанні повинен надати додаткові відомості, які мотивували б необхідність продовження відповідної НСРД. Загальний термін проведення НСРД не може перевищувати максимальні строки досудового розслідування, передбачені ст. 219 КПК, а це 18 місяців. Рішення про припинення НСРД, до моменту закінченні дії ухвали приймає прокурор за умови, що подальша доцільність проведення НСРД відпала.

В подальшому, ухвала слідчого судді про дозвіл на проведення НСРД, які обмежують таємницю спілкування повинна бути розсекречена та долучена до матеріалів справи для відкриття іншій стороні згідно ст. 290 КПК з метою ознайомлення, за її відсутності використати у доказуванні результати проведених на її підставі НСРД буде неможливо. В постанові *колегії суддів Великої палати ВСУ від 16.10.2019 у справі № 640/6847/15-к* йдеться про те, що «сторона обвинувачення повинна вживати необхідних і достатніх заходів для розсекречення матеріалів, які стали процесуальною підставою для проведення НСРД, з метою їх надання стороні захисту, і виконувати в такий спосіб вимоги щодо відкриття матеріалів іншій стороні відповідно до статті

290 КПК. Важливо зазначити, що суд не повинен автоматично визнавати такі докази недопустимим, спершу слід оцінити відомості отримані в результаті НСРД в комплексі із розсекреченими документами, які стали підставою для їх проведення. Оцінці підлягає поведінка сторони обвинувачення, якщо було вжито всіх необхідних заходів спрямованих на розсекречення процесуальних документів, які стали підставою для проведення НСРД, однак вони не були розсекречені до моменту передачі справи у суд з причин, що не залежали від волі або процесуальної поведінки прокурора, то в такому разі порушень вимог статті 290 КПК з боку сторони обвинувачення немає» [59].

З огляду на вищевикладене, тимчасове обмеження таємниці спілкування за законодавством України буде законним, якщо буде доведено неможливість отримати відомості про тяжке чи особливо тяжке кримінальне правопорушення та особу інакшим способом, ніж шляхом втручання у приватне спілкування за умови наявності ухвали слідчого судді, дотримання процедурних вимог щодо проведення НСРД та використання здобутих результатів у доказуванні. В випадках невиконання приписів КПК щодо підстав та процесуального порядку обмеження таємниці спілкування передбачено кримінальну відповідальність, відповідно до ст. 163 КК України: «порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер» [60, ст. 163].

2.2 Обмеження таємниці спілкування в ході проведення аудіо-, відеоконтролю особи та місця.

Аудіо-, відеоконтроль особи є різновидом втручання у приватне спілкування та однією з найпопулярніших НСРД, яка проводиться відповідно до ч. 3 ст. 248 КПК: «під час розслідування тяжких та особливо тяжких кримінальних правопорушень на підставі ухвали слідчого судді, якщо є

достатні підстави вважати, що розмови цієї особи або інші звуки, рухи, дії, пов'язані з її діяльністю або місцем перебування тощо, можуть містити відомості, які мають значення для досудового розслідування» [7]. Згідно п. 1.11.2 Інструкції: «Аудіо-, відеоконтроль особи полягає в негласній (без відома особи) фіксації та обробці із використанням технічних засобів розмови цієї особи або інших звуків, рухів, дій, пов'язаних з її діяльністю або місцем перебування тощо» [57]. Обов'язковою підставою проведення аудіо-, відеоконтролю особи є наявність в матеріалах справи ухвали слідчого судді, за її відсутності всі зібрані докази за результатами НСРД будуть визнані незаконними, а складені протоколи – недопустимими доказами.

Сфера застосування аудіо-, відеоконтролю особи стосується випадків, коли необхідно отримати інформацію без відома особи, стосовно якої здійснюється втручання у приватне спілкування, при цьому основною ознакою, яка характеризує її сутність це «пасивність», адже допустимим є лише пасивне спостереження за особою в повсякденній обстановці, а не створення ситуацій, які штучно викликають кримінально карану поведінку та є фактично «провокацією».

Аудіоконтроль проводиться з використанням технічних засобів фіксації інформації (через прослуховування та фіксацію змісту розмов), що обумовлює необхідність залучення оперативних підрозділів, які наділені спеціальними технічними знаннями на підставі письмового доручення слідчого у порядку п. 2 ч. 2 ст. 40, ст. 41 та ч. 6 ст. 246 КПК. Залежно від потреб слідства аудіоконтроль може проводитись як епізодично — у чітко визначені часові проміжки, так і безперервно, тобто цілодобово протягом усього строку дії ухвали слідчого судді.

Крім того, законодавець не вимагає отримувати дозвіл стосовно кожного співрозмовника особи, яка перебуває під дією ухвали окремо, що є цілком допустим на нашу думку. Це обумовлено тим, що під значенням слів «спілкування», «розмови» вже розуміється процес усної комунікації декількох осіб (двох або більше), які здійснюють між собою обмін інформацією і щодо

кожного отримувати дозвіл не є процесуально доцільним, до того ж як свідчить вирок Вищого антикорупційного суду від 30.05.2023 р. у справі № 127/13972/17: «фіксація діяльності інших осіб, які випадково опинилися в колі спілкування і стосовно яких НСРД не здійснюється, не може визнаватися істотним порушенням прав людини, якщо особа, яка зазнає такого втручання не набуває у подальшому статусу підозрюваного чи обвинуваченого у кримінальному провадженні і докази, отримані в результаті такого втручання, не використовуються проти неї» [64].

Відеоконтроль особи здійснюється у формі негласного візуального спостереження (через відео- та аудіозапис) за її поведінкою, переміщеннями, контактами та спілкуванням, що можуть мати доказове значення. З цією метою застосовуються спеціальні технічні засоби відеофіксації, що забезпечують приховане спостереження без присутності оперативних підрозділів. До того ж відеоконтроль дозволяє отримати більш деталізовану інформацію, порівняно з аудіоконтролем, адже уможлиблюється зафіксувати дії, поведінкові реакції та невербальні сигнали в поведінці особи.

Відеоконтроль, як і аудіоконтроль може проводитися у будь-якому місці фактичного перебування особи – помешканні, іншому володінні, транспортному засобі, службових чи публічних приміщеннях, так як процесуальний закон не має вказівок щодо визначення місць на території яких може проводитися спостереження, тому допускається встановлення спостереження за будь-якою ділянкою в просторі.

Незначні відмінності від аудіо-, відеоконтролю особи має така НСРД, як аудіо-, відеоконтроль місця. Остання згідно ч. 1 ст. 270 КПК проводиться шляхом встановлення технічного обладнання «всередині публічно доступних місць, без відома їх власника, володільця або присутніх у цьому місці осіб, за наявності відомостей про те, що розмови і поведінка осіб у цьому місці, а також інші події, що там відбуваються, можуть містити інформацію, яка має значення для кримінального провадження» [7]. Визначальною характеристикою цієї НСРД, яка відрізняє її від Аудіо-, відеоконтролю особи

є те, що спостереження здійснюється не стосовно конкретної особи, а щодо певної локації. За таких умов в ухвалі слідчого судді повинна бути зазначена точна адреса, де планується спостереження, чого не вимагається для аудіо-, відеоконтролю особи. За своїм характером обидві НСРД мають на меті обмеження таємниці спілкування, проте під час «Аудіо-, відеоконтролю особи» нас цікавить певна особа, тоді як під час «Аудіо-, відеоконтролю місця», – обмежується таємниця спілкування невизначеного кола громадян.

Доступ до змісту спілкування в ході проведення аудіо-, відеоконтролю особи буде легітимним, якщо учасники спілкування мали розумні очікування щодо приватності свого спілкування. Так, до прикладу, у постанові ККС ВСУ у справі № 723/884/17 від 18.03.2025 було констатовано «недопустимість протоколів за результатами проведення НСРД (аудіо-, відео контролю осіб) у зв'язку з тим, що спілкування засуджених з працівниками поліції з приводу обставин вчиненого розбійного нападу є різновидом допиту, який не можна визнати аудіо-, відеоконтролем в значенні ст. 258 КПК, оскільки учасники такого спілкування не мали жодних підстав вважати, що це спілкування є приватним» [61]. За таких умов не йдеться про дотримання таємниці спілкування, адже особа перебувала під контролем працівників поліції і усвідомлювала, що фактично дає показання. Відсутність ознак допиту у бесіді, на наше переконання, є однією з ключових вимог, що дозволяють визнати результати НСРД у вигляді аудіо-, відеоконтролю особи допустимими доказами.

При опрацюванні записів з технічних пристроїв долучених до протоколу за фактом проведення цієї НСРД також слід звертати увагу чи є спілкування осіб вільним, - без обману чи примусу з боку сторонніх осіб (в тому числі з'ясовувати чи залучалися «інші особи» в порядку конфіденційного співробітництва) та чи особа на власний розсуд спілкується на обрані теми та доповідає про певні події. В постанові ККС ВСУ від 26.05.2022 у справі № 753/16804/17, суд висловився про «недопустимість доказів, отриманих при проведенні НСРД аудіо-, відеоконтролю особи, як вбачається зі змісту

протоколу за результатами проведення аудіо-, відеоконтролю та стенограми до нього, слідча дія проводилася за участю працівника поліції, а бесіда складалася з послідовних запитань та відповідей» [62], тобто фактично був проведений допит особи. Така непоодинокa тенденція щодо підміни змісту однієї НСРД іншою є намаганнями сторони обвинувачення отримати докази винуватості будь-яким чином, вдаючись до неофіційної розмови і негласно фіксуючи її, відбувається не просто примітивний обман, а й неприпустиме порушення прав людини. Запобігти таким випадкам можна, якщо з більшою чіткістю визначити зміст та порядок аудіо-, відеоконтролю особи в ст. 260 КПК, адже наразі ступінь нормативної розробки є низьким, що підтверджується досі функціонуючими методами зловживань та обману, якими користуються завдяки недолікам процесуального законодавства.

Окремої уваги заслуговують питання складання протоколу за результатами проведення аудіо-, відеоконтролю особи. Згідно ч. 1 ст. 252 КПК : «За результатами проведення негласної слідчої (розшукової) дії складається протокол, до якого в разі необхідності долучаються додатки» [7], в даній нормі не конкретизовано, яким вимогам повинен відповідати протокол, проте дана інформація міститься в ч. 3 ст. 104 КПК. Так як хід та результати проведення аудіо-, відеоконтролю особи фіксуються за допомогою технічних засобів, то результати їх застосування в ідеалі повинні долучатися як додатки. Відповідно до ч.2 ст. 106 КПК: «до складу слідчої дії входять дії щодо належного упакування речей і документів» [7], це стосується речей за допомогою яких відбувається фіксування (карти пам'яті, флешки, жорсткі диски), що унеможлиблює їх використання для фіксування іншої інформації. Проте, як свідчить *постанова ККС ВСУ від 23.11.2023 у справі №731/275/19*: «допустимість доказів за результатами аудіо-, відеоконтролю особи не залежить від того, чи є вони додатками до протоколів за результатами проведення НСРД або надані суду для дослідження як окремі електронні документ, така позиція суду вмотивована тим, що КПК не містить імперативної норми щодо обов'язкового долучення до протоколів НСРД, як

додатку, аудіо- або відеозаписів зроблених за допомогою технічних засобів, як і вимоги щодо зазначення у протоколах опису індивідуальних ознак технічного носія з зафіксованою інформацією» [63]. Тобто не вважається порушенням закону, якщо до протоколу не було додано носій інформації з результатами проведеної НСРД і при цьому цей доказ був окремо наданий для дослідження судом.

2.3. Обмеження таємниці спілкування в ході проведення тимчасового доступу до речей та документів

Відповідно до положень ч.1 ст. 159 КПК: «Тимчасовий доступ до речей і документів полягає у наданні стороні кримінального провадження особою, у володінні якої знаходяться такі речі і документи, можливості ознайомитися з ними, зробити їх копії та вилучити їх (здійснити їх виїмку)» [7]. Тимчасовий доступ до речей та документів є процесуальним інструментом забезпечення інтересів провадження з метою запобігання втраті доказової інформації, що міститься в речах та документах, його застосовують за умови, коли володілець відмовляється добровільно надати докази. Аналізований захід забезпечення кримінального провадження становить особливий інтерес в межах нашого магістерського дослідження, адже як свідчить аналіз ст. 162 КПК, - доступ дозволяється і до «особистого листування особи, інших записів особистого характеру, а також до інформації, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо, які містять охоронювану законом таємницю спілкування» [7]. З огляду на це виникає логічне питання, до якого обсягу відомостей може бути отриманий доступ в ході здійснення тимчасового доступу до речей та документів та його відмінність від НСРД, якщо ст. 14 та ст. 258 ККУ

визначено, що втручання у таємницю спілкування можливе лише шляхом проведення НСРД.

Сучасні науковці відзначають про наявність юридичної колізії у практичному застосуванні двох інститутів доступу до особистого спілкування особи: через захід забезпечення кримінального провадження у формі тимчасового доступу до речей, документів та шляхом проведення НСРД. Як справедливо відзначає С. І. Перепелиця: «на практиці, під виглядом тимчасового доступу до речей та документів фактично відбувається втручання у приватне спілкування, шляхом зняття та копіювання інформації, яка міститься в програмному забезпеченні технічного обладнання, тобто відбувається зняття інформації з транспортних телекомунікаційних мереж та зняття інформації з електронних інформаційних систем, порядок здійснення яких закріплено статтями 263, 264 КПК та є втручанням у приватне спілкування» [2, с. 75-76], тому хоч ці інститути і досить подібні, проте не слід ототожнювати їх між собою, вони мають кардинально різний ступінь дозволеного втручання, на чому і слід зосередитися.

У випадку проведення тимчасового доступу до речей і документів можна оглянути та вилучити лише листи, які вже написані або/та отримані адресатом та перебувають на зберіганні у особи, й не знаходяться на етапі відправлення співрозмовнику, це ж стосується і особистих записів особи (щоденників, аудіо-, відеозаписів, електронних файлів, накопичувачів інформації). Подекуди такі документи можуть самі по собі не бути доказами, проте слугують, як зразки для проведення експертиз, тобто як матеріал на підставі якого можна отримати докази (до прикладу: вільні зразки почерку з записника особи для судово-почеркознавчого дослідження). Якщо ж доступ потрібен до спілкування, як дії в форматі реального часу між конкретними особами, то вилучення паперових та електронних листів, записів здійснюється лише в форматі НСРД відповідно до ст. ст. 258, 261-265 КПК. Так, наприклад, у вироку ВАКС від 14.07.2021 у справі №707/146/17 було констатовано про недопустимість, як доказу - протоколу тимчасового доступу до речей і

документів, так як отримання на підставі ухвали слідчого судді про тимчасовий доступ до речей та документів доступу до відеореєстратора, на якому зафіксовано приватне спілкування осіб суперечить процесуальному порядку отримання допуску до такої інформації, така аргументація суду зумовлена тим, що на вказаних відеозаписах зафіксовано спілкування приватного характеру, а прокурор не надав суду жодних доказів на спростування доводів сторони захисту щодо неправомірності втручання у приватне спілкування та підтвердження процесуального походження вказаних відеозаписів [66].

Розмежовуючи тимчасовий доступ до речей і документів, які містять інформацію, яка знаходиться в операторів та провайдерів телекомунікацій із «Зняттям інформації з транспортних телекомунікаційних мереж», варто звернути увагу на п. 17 «Інформаційного листа Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ» від 05.04.2013 № 223-559/0/4-13 «Про деякі питання здійснення слідчим суддею суду першої інстанції судового контролю за дотриманням прав, свобод та інтересів осіб під час застосування заходів забезпечення кримінального провадження» (Далі - Лист): «Тимчасовий доступ надається до документів, які містять інформацію про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалість, зміст (вихідні чи вхідні з'єднання, SMS, MMS тощо), маршрути передавання тощо і не дають можливості втрутитися у приватне спілкування, тобто отримати доступ до змісту інформації, що передається. А зняття інформації з транспортних телекомунікаційних мереж (ст. 263 КПК) є різновидом втручання у приватне спілкування, оскільки здійснюється доступ до змісту повідомлень будь-якого виду та інформації, що передається особою під час зв'язку» [65], тому при доступі до речей і документів можливо лише встановити певний факт, що відбувся в минулому і стосується інформації щодо ідентифікаційних ознак кінцевого обладнання телекомунікацій (абонентський номер SIM-картки, IMEI, MAC-адреса, IP-адреса), ПІБ споживача послуг, про типи з'єднань (вхідні/вихідні), доступ

надається виключно на опрацювання так званої «статичної» інформації про споживача і послуги, яка зберігається у операторів і провайдерів певний проміжок часу і не стосується змісту розмов. Тимчасовий доступ до речей і документів дозволяє отримати відомості, які зберігаються в операторів та провайдерів телекомунікацій про зв'язок абонента, його тривалість та місце в якому було зафіксовано передачу інформації лише постфактум, а не в діючий проміжок часу визначений в ухвалі слідчого судді, як це відбувається при проведенні Зняття інформації з електронних комунікаційних мереж.

Особлива увага законодавця приділяється категорії речей і документів доступ до яких забороняється за будь-яких умов, згідно ст. 161 КПК це «листування чи інші форми обміну інформацією, а також об'єкти додані до них між захисником та його клієнтом або будь-якою особою, яка представляє його клієнта, у зв'язку з наданням правової допомоги» [7]. Так як формулювання доданих об'єктів в контексті ч. 2 ст. 161 КПК не є вичерпним, то сюди можна віднести будь-які речі та документи, які особа передає своєму захиснику в контексті отримання правової допомоги та які містять інформацію пов'язану з наданням правової допомоги. Дане застереження пов'язане з гарантіями адвокатської діяльності, а також правом клієнта на обґрунтоване очікування, що їхнє спілкування з захисником є приватним та конфіденційним.

На підставі вищевикладеного можна виокремити такі основні відмінності тимчасового доступу до речей і документів від НСРД:

- «тимчасовий доступ до речей і документів» є заходом забезпечення кримінального провадження, його першочергова мета не збирання доказів, а запобігання їх втраті та забезпечення отримання засобів доказування, тоді як аналізовані НСРД є безпосереднім процесуальним інструментом збору доказової інформації;

- НСРД здійснюються негласно, без попереднього повідомлення особи стосовно якої планується їх проведення, так як за ч. 4 ст. 258 КПК: «втручанням у приватне спілкування є доступ до змісту спілкування за умов,

якщо учасники спілкування мають достатні підстави вважати, що спілкування є приватним» [7], тоді як доступ до речей і документів здійснюється в умовах явної очевидності для володільця інформації (він передає самостійно для ознайомлення речі чи документи);

- різниця і межа втручання - при «тимчасовому доступі до речей і документів» уможлиблюється доступ виключно до інформації про комунікації особи, що мали місце в минулому, а в контексті проведення НСРД важливим є фіксація живого спілкування в проміжок часу зазначений в ухвалі слідчого судді.

Віднесення інформації в речах і документах до такої, що становить охоронювану законом таємницю має особливості і в контексті розгляду клопотань про надання дозволу на тимчасовий доступ до речей і документів. Маючи намір звернутися до слідчого судді, сторони кримінального провадження повинні оформити своє клопотання в відповідності з вимогами ч. 2 ст. 160 КПК, важливо повно та конкретизовано вказати характеристику та ознаки речей, доступ до яких планується отримати, адже відсутність деталізації може призвести до відмови у задоволенні клопотання, так п.16 вищезгаданого Листа передбачено, що при поданні клопотань про надання тимчасового доступу до документів, які знаходяться в операторів і провайдерів телекомунікацій необхідно вказувати: «1) інформацію про ідентифікаційні ознаки кінцевого обладнання телекомунікацій (абонентський номер SIM-картки, IMEI, MAC-адреса, IP-адреса тощо), яке перебувало у зоні дії певних базових станцій у певний час; 2) інформацію про прізвища, імена, по батькові та інші відомості про споживача телекомунікаційних послуг та абонентів зазначеного кінцевого обладнання телекомунікацій (за наявності таких відомостей); 3) інформацію про типи з'єднань зазначеного кінцевого обладнання телекомунікацій (вхідні та вихідні з'єднання) за певний період часу включно із зазначенням дати і часу, тривалості таких з'єднань, маршрутів передавання даних; 4) зазначену в пунктах 1, 2, 3 інформацію щодо кінцевого обладнання телекомунікацій, з якими з'єднувалося кінцеве обладнання

телекомунікацій, що перебувало у зоні дії певних базових станцій у певний час, та щодо їх наступних з'єднань; 5) іншу інформацію про телекомунікації» [65].

Значення речей і документів для встановлення обставин у кримінальному провадженні може бути обґрунтовано тим, що вказані дані допоможуть встановити особу злочинця, осіб, яким відомі обставини вчиненого кримінального правопорушення, а інтереси досудового розслідування потребують такого втручання (до прикладу: «встановлення причетності власників абонентів сім-карт до скоєння кримінального правопорушення, буде можливе лише шляхом тимчасового доступу до речей і документів, а саме через отримання інформації, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок абонента, надання телекомунікаційних послуг у тому числі отримання послуг їх тривалості, змісту, маршрутів пересування»). Слід також зазначити про підстави вважати, що речі і документи перебувають або можуть перебувати у володінні конкретної фізичної або юридичної особи, обґрунтувати необхідність вилучення речей і оригіналів або копій документів, якщо відповідне питання порушується стороною кримінального провадження. Для отримання доступу до речей і документів, які містять таємницю спілкування згідно п.6 ч.2 ст. 160 КПК також потрібно обов'язково довести «неможливість іншими способами довести обставини, які передбачається довести за допомогою цих речей і документів, тобто на сторону покладається тягар доказування виключної необхідності даного заходу» [7].

На етапі підготовки до розгляду клопотання слідчим суддею, судом в відповідності до ст. 163 КПК здійснюється судовий виклик особи у володінні якої знаходяться такі речі і документи, а за наявності «достатніх підстав вважати що існує реальна загроза зміни або знищення речей чи документів, клопотання може бути розглянуто слідчим суддею, судом без виклику особи, у володінні якої вони знаходяться» [7]. Проблематичним є те, що зміст формулювання «достатні підстав вважати що існує реальна загроза зміни або

знищення речей чи документів», як порогу для доказування не розкривається в КПК, як правило сторона кримінального провадження в клопотанні посилається на обставини кримінального провадження, що пов'язані з поведінкою особи (володільця речей чи/або документів) та її стосунків з іншими учасниками, які підкріплюються масивом належних та допустимих доказів. Як справедливо зазначає І. В. Гловюк: «реальність загрози є оцінною категорією, що ускладнює застосування цієї норми на практиці, адже у цій нормі закладено надто високий стандарт доказування при вирішенні питання про тимчасовий доступ до речей та документів» [67, с. 53-54].

Слідчий суддя, суд розглядає клопотання за участю сторони кримінального провадження, яка подала клопотання, та особи, у володінні якої знаходяться речі і документи, крім випадків, розгляду без виклику особи в володінні якої вони знаходяться. І знову ж таки ми виявляємо недоліки законодавчого формулювання, які проявляються в відсутності строків розгляду клопотання. Питання строків врегульовано лише у п.8 згаданого вище Листа: «клопотання про тимчасовий доступ до речей і документів, повинно бути розглянуте не пізніше трьох днів із дня надходження клопотання до суду. У разі ж якщо особа, яка подала клопотання, обґрунтує у ньому наявність реальної загрози зміни або знищення речей і документів, слідчий суддя має розглянути зазначене клопотання невідкладно» [65], проте так як такі роз'яснення носять здебільшого рекомендаційний характер та не завжди беруться до уваги при розгляді клопотань суддями, тому вважаємо необхідним доповнити ч. 4 ст. 163 КПК відомостями, які б вказували на конкретні часові межі, протягом яких слідчий суддя, суд зобов'язані ухвалити рішення, а за основу можна взяти частково або повністю зміст наведеного роз'яснення.

КПК в ч. 5 ст. 163 містить деталізовану вказівку на те, що «Слідчий суддя, суд постановляє ухвалу про надання тимчасового доступу до речей і документів, якщо сторона кримінального провадження у своєму клопотанні доведе наявність достатніх підстав вважати, що ці речі або документи: 1) перебувають або можуть перебувати у володінні відповідної фізичної або

юридичної особи; 2) самі по собі або в сукупності з іншими речами і документами кримінального провадження, у зв'язку з яким подається клопотання, мають суттєве значення для встановлення важливих обставин у кримінальному провадженні; 3) не становлять собою або не включають речей і документів, які містять охоронювану законом таємницю» [7]. По суті законодавець вимагає, аби ініціатор клопотання зазначав не лише ознаки, які можуть ідентифікувати документи чи речі до яких потрібно отримати доступ, а й переконливо обґрунтував їх зв'язок з досудовим розслідуванням та реальну можливість знаходження таких предметів матеріального світу у конкретної особи.

Для того щоб уникнути помилок при здійсненні тимчасового доступу до речей і документів, ухвала слідчого судді, суду повинна відповідати вимогам ст. 164 КПК, а також як зазначається науковцями містити чітку вказівку на те:

«- хто повинен надати тимчасовий доступ до речей і документів (із зазначенням повної та точної назви юридичної особи її юридичної адреси);

- якщо вказаний обов'язок покладено на фізичну особу, то зазначається її прізвище, ім'я та по батькові;

- кому повинно бути надано тимчасовий доступ до речей і документів (із зазначенням прізвища, імені, по батькові, а також посади уповноваженої особи);

- які саме необхідно надати документи для ознайомлення, отримання їх копій чи здійснення виїмки;

- який строк встановлено для застосування вказаного заходу» [68, с. 512].

Таким чином, не слід ототожнювати «тимчасовий доступ до речей і документів», як захід забезпечення кримінального провадження з НСРД, що передбачають втручання у приватне спілкування. Вони відрізняються, підставами, метою та способами втручання, мають різнорідний ступінь доступу до приватних записів та/або спілкування осіб, проте в обох випадках за своєю суттю вимагають дотримання таємниці спілкування під час їх

санкціонування та проведення, так як напряду зачіпають сторону приватного життя осіб та їх комунікацій.

2.4 Обмеження таємниці спілкування в ході проведення огляду і виїмки кореспонденції.

Арешт, огляд та виїмка кореспонденції є однією з типових НСРД пов'язаних з втручанням у приватне спілкування. Підхід до її розуміння ускладняється тим, що законодавець окремо виділяє накладення арешту на кореспонденцію (ст. 261 КПК) та огляд і виїмку кореспонденції (ст. 262 КПК) , в п. 1.11, 1.11.3, 1.11.4 Інструкції накладення арешту на кореспонденцію та огляд і виїмка кореспонденції [57], так само виокремлюються як дві різні, самостійні види НСРД. Ми вбачаємо в цьому недолік процесуальної регламентації та розділяємо думку Д. Б. Сергєєвої, яка вважає: «статтями 261 та 262 КПК передбачений процесуальний порядок проведення однієї негласної слідчої (розшукової) дії – накладення арешту на кореспонденцію. Мета провадження цього негласного заходу може бути досягнута лише у випадку послідовного провадження арешту, огляду, а в необхідних випадках, виїмки кореспонденції, що у своїй єдності складають етапи провадження негласної слідчої (розшукової) дії, процесуальний порядок провадження якої закріплено у декількох статтях КПК» [69, с. 70]. До того ж як свідчить ч. 3 ст. 261 КПК: «накладення арешту на кореспонденцію надає право слідчому здійснювати огляд і виїмку цієї кореспонденції» [7], що є підтвердженням правильності думки про те, що арешт, огляд та виїмка кореспонденції - це єдина НСРД, яка складається з трьох послідовних етапів.

Накладення арешту на кореспонденцію особи відповідно до положень ст. 261 КПК відбувається без її відома у виняткових випадках за наявності фактичних підстав вважати, що у поштово-телеграфній кореспонденції певної особи містяться дані про вчинене правопорушення або документи і речі, що

мають доказове значення і іншими способами отримати такі відомості неможливо.

Юридичною підставою для арешту, огляду, виїмки поштово-телеграфної кореспонденції є ухвала слідчого судді прийнята в порядку регламентованому ст. ст. 246-249 КПК. Відсутність вказівки на відомості, які повинна містити ухвала слідчого судді про надання дозволу на накладення арешту на кореспонденцію в ст. 261 КПК, викликає непоодинокі полеміку в юридичних колах. Зокрема, А.Б. Ткачик пропонує доповнити ч. 1 ст. 261 КПК спеціальними вимогами щодо змісту згаданої ухвали. Так, в ухвалі слідчого судді на думку науковця мають бути вказані: «підстави на яких буде проводитись слідча (розшукова) дія, прізвище, ім'я та по батькові особи, кореспонденція якої має затримуватися, точна адреса цієї особи, види кореспонденції, на яку накладається арешт, строк дії ухвали, назва установи зв'язку, на яку покладається обов'язок затримувати кореспонденцію та повідомляти про це слідчого» [14, с. 121]. Як відзначають В. І. Галаган, В. В. Шум, «у дозвільному процесуальному документі слідчого судді не можуть зазначатися конкретні речі й документи, що підлягають виїмці під час їх виявлення й огляду хоча б тому, що вкрай складно прогнозувати, які з них будуть виявлені в кореспонденції та які важливі фактичні дані може бути встановлено» [70]. На наше ж переконання, недоцільно в ухвалі посилатися на конкретні види кореспонденції, на які може бути накладено арешт, адже потенційно передбачити який з об'єктів кореспонденції буде пересилатися неможливо, питання їх придатності, як джерела доказів може бути вирішене лише в момент безпосереднього огляду слідчим всіх поштових відправлень особи.

Ухвала слідчого судді покладає на фінансові установи та установи зв'язку заборону на вручення кореспонденції адресату до моменту отримання вказівки слідчого, прокурора. Керівники та працівники установ зв'язку зобов'язані сприяти проведенню негласної слідчої (розшукової) дії і не розголошувати факт її проведення чи отриману інформацію. Чинний КПК не

містить вказівки про які саме установи зв'язку йде мова, проте як свідчать положення ЗУ «Про поштовий зв'язок», під операторами поштового зв'язку слід розуміти: «суб'єкта господарювання, що здійснює діяльність на території України та у встановленому законодавством порядку надає послуги поштового зв'язку» [5], як свідчать відомості з Єдиного державного реєстру операторів поштового зв'язку наразі таких суб'єктів 50 на території України.

З моменту накладення арешту у слідчого з'являється можливість здійснити огляд та виїмку кореспонденції, до якої ст. 261 КПК відносить: «листи усіх видів, бандеролі, посилки, поштові контейнери, перекази, телеграми, інші матеріальні носії передання інформації між особами» [7], хоч даний перелік є досить широким, проте не вичерпним, в ЗУ «Про поштовий зв'язок» наведено розширений перелік об'єктів кореспонденції: «листи, поштові картки, дрібні пакети, мішки "М", адресна поштова розсилка та відправлення для сліпих» [5].

Згідно п.1.11.4. Інструкції: «огляд і виїмка кореспонденції (ст. 262 КПК) полягає в негласному відкритті й огляді затриманої кореспонденції, на яку накладено арешт, її виїмки або зняття копії чи отриманні зразків, нанесенні на виявлені речі і документи спеціальних позначок, обладнанні їх технічними засобами контролю, заміні речей і речовин, що становлять загрозу для оточуючих чи заборонені у вільному обігу, на їх безпечні аналоги» [57].

Огляд за змістом ч.1 ст. 262 КПК відбувається «в установі зв'язку якій доручено здійснювати контроль і затримувати цю кореспонденцію, за участю представника цієї установи, а за необхідності - за участю спеціаліста» [7]. Залучення спеціаліста провадиться з метою забезпечення безпеки під час огляду кореспонденції, адже подекуди відправлення можуть містити вибухові, радіоактивні, отруйні речовини та детонуючі пристрої, а без застосування спеціальних знань виявити та деактивувати їх неможливо. У присутності зазначених осіб слідчий вирішує питання про відкриття і оглядає затриману кореспонденцію, при цьому слід вживати заходів щодо збереження первинного пакування та розташування вмісту згідно з оригінальним

відправленням, аби в адресата не виникало підозр про проведену НСРД. На думку В. І. Галаган, В. В. Шум: «сутність огляду полягає в тому, що слідчий безпосередньо за допомогою власних органів чуття, проте за визначеним планом дій оцінює існування та характеристики фактичних даних і переконується, що вони мають доказове значення. Після цього слідчий надає можливість іншим учасникам цієї процесуальної дії оглянути кореспонденцію» [70, с. 98]. Таким чином, відкриваючи конверти, посилки, слідчий оцінює чи містяться в цих предметах матеріального світу відомості, які б допомогли встановити обставини у справі, у разі відсутності речей чи документів, які б сприяли слідству, надається вказівка про вручення оглянутої кореспонденції адресату. Вилучення предметів чи/та документів, які не мають безпосереднього зв'язку з розслідуванням конкретного кримінального правопорушення, є недопустимим.

За результатами огляду кореспонденції може бути прийняте одне з таких процесуальних рішень:

«1) виїмка кореспонденції (за умови виявлення в кореспонденції речей, речовин, документів, що мають певне значення для розслідування справи і обмежитися зняттям копій неможливо або слід запобігти обміну інформацією певних осіб);

2) зняття копій,

3) отримання зразків з відповідних відправлень;

4) нанесення на речі і документи спеціальних позначок ;

5) обладнання кореспонденції технічними засобами контролю;

6) заміна речей і речовин, що становлять загрозу для оточуючих чи заборонені у вільному обігу, на їх безпечні аналоги.;

7) вручення оглянутої кореспонденції адресату (ч. 2, 3, 4 ст. 262 КПК)» [7].

Підставами для проведення виїмки, затриманої в установі зв'язку, кореспонденції, є:

«— наявність в ухвалі слідчого судді про накладення арешту на кореспонденцію дозволу на проведення її виїмки при встановленні в ній відомостей про обставини, які мають значення для досудового розслідування, або речей і документів, що мають істотне значення для досудового розслідування;

— фактичне встановлення слідчим за результатами проведення огляду затриманої кореспонденції, що конкретне поштово-телеграфне відправлення містить відомості про обставини, які мають значення для досудового розслідування, або речі і документи, що мають істотне значення для досудового розслідування, і що зняття з них копій або їх фотографування, проведення відеозапису вмісту чи отримання зразків з цих відправлень не може забезпечити встановлення відомостей, які мають значення для досудового розслідування» [71, 40].

За результатами кожного проведеного огляду, виїмки або затримання кореспонденції складається протокол згідно з вимогами КПК. У протоколі обов'язково зазначається, які саме відправлення були оглянуті, що з них вилучено і що має бути доставлено адресату або тимчасово затримано, з яких відправлень знято копії чи отримано зразки, а також про проведення інших дій, перелічених у ч.2 ст. 262 КПК. Чітке документування процесу та результатів огляду й виїмки кореспонденції у протоколі сприяють ухваленню обґрунтованих рішень у кримінальному провадженні та мінімізують ризики розголошення таємниці спілкування. Основою дотримання таємниці спілкування в умовах проведеного арешту, огляду, виїмки кореспонденції та дотичних до цієї НСРД процесуальних заходів є й необхідність забезпечення високого рівня культури та професійності серед усіх учасників проведеної НСРД. На слідчого, спеціаліста, керівника та працівників установ зв'язку покладається зобов'язання щодо збереження в таємниці факту проведеної НСРД, забезпечення цілісності затриманої кореспонденції та нерозголошення відомостей, що містяться в кореспонденції. Виключно за таких умов можна говорити про досягнення справедливого балансу між втручання в

охоронюване законом право особи на таємницю спілкування та досягненням інтересів кримінального провадження.

2.5 Обмеження таємниці спілкування в ході проведення зняття інформації з електронних комунікаційних мереж та зняття інформації з електронних інформаційних систем.

Зняття інформації з електронних комунікаційних мереж регламентоване ст. 263 КПК та Зняття інформації з електронних інформаційних систем передбачене ст. 264 КПК є двома самостійними видами НСРД, які передбачають безпосереднє втручання у приватне спілкування осіб та можуть здійснюватися лише на підставі ухвали слідчого судді. Сутність кожної з них визначається певними особливостям проведення, характером та способом втручання, що вважаємо за необхідне дослідити в контексті нашої магістерської роботи у взаємозв'язку з впливом на охоронюване законом право на таємницю спілкування.

Згідно ч. 1 ст. 264 КПК: «Зняття інформації з електронних комунікаційних мереж (комплекс технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг) є різновидом втручання у приватне спілкування, що проводиться без відома осіб, які використовують засоби електронних комунікацій (телекомунікацій) для передавання інформації, на підставі ухвали слідчого судді, якщо під час його проведення можливо встановити обставини, які мають значення для кримінального провадження» [7]. Підключеність до мережі зв'язку при прослуховуванні осіб відрізняє цю НСРД від аудіо-, відеоконтролю особи, де так само використовуються технічні засоби прослуховування, але не відбувається підключення до телефонного каналу чи сканування радіоканалу. Згідно Інструкції: «Зняття інформації з транспортних телекомунікаційних мереж полягає в негласному проведенні із застосуванням відповідних

технічних засобів спостереження, відбору та фіксації змісту інформації, яка передається особою, а також одержанні, перетворенні і фіксації різних видів сигналів, що передаються каналами зв'язку (знаки, сигнали, письмовий текст, зображення, звуки, повідомлення будь-якого виду)» [57]. Звертаємо увагу, що одна і та сама НСРД має різну назву у КПК («Зняття інформації з електронних комунікаційних мереж») та Інструкції («Зняття інформації з транспортних телекомунікаційних мереж»). Така неузгодженість понятійного апарату виникла після внесення змін до КПК від 15.03.2022 р., якими було змінено назву аналізованої НСРД, проте нововведення наразі досі не застосовано по відношенню до Інструкції. За такої ситуації п. п. 1.11.5 Інструкції підлягають зміні в частині назви вказаної дії, аби не викликати відмінності між нормативними актами.

Інструкція не просто вказує на суть самої НСРД, а ще й виокремлює два її різновиди, про що не зазначається в кодифікованому акті: «контроль за телефонними розмовами, що полягає в негласному проведенні із застосуванням відповідних технічних засобів, у тому числі встановлених на транспортних телекомунікаційних мережах, спостереження, відбору та фіксації змісту телефонних розмов, іншої інформації та сигналів (SMS, MMS, факсимільний зв'язок, модемний зв'язок тощо), які передаються телефонним каналом зв'язку, що контролюється; - зняття інформації з каналів зв'язку, що полягає в негласному одержанні, перетворенні і фіксації із застосуванням технічних засобів, у тому числі встановлених на транспортних телекомунікаційних мережах, у відповідній формі різних видів сигналів, які передаються каналами зв'язку мережі Інтернет, інших мереж передачі даних, що контролюються» [57]. Як відзначає В.В. Луцик: «об'єктом першого виду зняття інформації з електронних комунікаційних мереж будуть: телефонні лінії загального користування; відомчі мережі, що мають вихід на телефоні лінії загального користування; виділені мережі зв'язку невиробничого призначення; мережі пересувного радіотелефонного зв'язку; системи пересувного супутникового зв'язку, а об'єктом другого - телексні,

факсимільні, селекторні, радіорелейні, пейджингові канали обміну інформації між абонентами, комп'ютерні мережі різного рівня» [73].

За вищенаведених обставин вважаємо, що сутність «Зняття інформації з електронних комунікаційних мереж» полягає в отриманні доступу до інформації безпосередньо в момент її руху між абонентами, наприклад, під час спілкування телефонним зв'язком, надсилання текстових, графічних повідомлень та файлів. Технічно це здійснюється через використання спеціалізованого обладнання або програмного забезпечення, інтегрованого у комунікаційну мережу операторів електронних комунікацій. Спеціальні технічні засоби дозволяють правоохоронним органам копіювати інформацію під час її передачі без зміни змісту та маршруту.

Ухвала слідчого судді про дозвіл на проведення зняття інформації з електронних комунікаційних мереж повинна відповідати не тільки загальним вимогам сформульованим в ч. 4 ст. 248 КПК, а й додатково, відповідно до вимог ч. 2 ст. 263 КПК містити відомості про «ідентифікаційні ознаки, які дозволять унікально ідентифікувати абонента спостереження, електронну комунікаційну мережу, кінцеве (термінальне) обладнання, на якому може здійснюватися втручання у приватне спілкування» [7]. Відповідно до п. 25 ч. 1 ст. 2 ЗУ «Про електронні комунікації» під електронною комунікаційною мережею маються на увазі «комплекс технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг, а кінцевим (термінальним) обладнанням є обладнання, призначене для з'єднання з кінцевим пунктом електронної комунікаційної мережі з метою забезпечення доступу до електронних комунікаційних послуг» [6].

Відомості про ідентифікаційні ознаки, які дозволять унікально ідентифікувати абонента спостереження, електронну комунікаційну мережу, кінцеве (термінальне) обладнання працівники органу досудового розслідування зазвичай отримують шляхом тимчасового доступу до речей і документів, які зберігаються в постачальників електронних комунікаційних послуг, мереж в порядку ст. ст. 159-166 КПК. Надзвичайно важливо здійснити

повну ідентифікацію особи, не обмежуючись зазначенням тільки електронного коду (ідентифікатора) кінцевого (термінального) обладнання (міжнародних серійних кодів телефонів та інших пристроїв: IMEI, ESN, MEID). Як вірно зазначає В.С. Бабкова: «У такій ситуації завжди залишається імовірність того, що телекомунікаційне обладнання використовував не особисто підозрюваний, обвинувачений, навіть якщо на належність йому такого обладнання вказують матеріали справи, а інша особа. Інформація, що в такому разі була предметом зняття, може не належати до особи підозрюваного, обвинуваченого та/або не входити до предмета доказування. Тобто отримані в такий спосіб докази не можуть визнаватися належними і допустимими» [72, с. 73].

Певні проблеми донині виникають з встановленням ідентифікаційних ознак абонента зв'язку, які дозволяють унікально ідентифікувати об'єкта спостереження (SIM-картка, USIM-картка, R-UIM-картка, e-SIM), коли слід здійснити втручання у приватне спілкування, яке здійснюється за допомогою мобільного зв'язку. Основна складність обумовлена відсутністю в Україні процедури обов'язкової реєстрації абонентів мобільного зв'язку за паспортними даними під час укладення договору з постачальником комунікаційних послуг. Мільйони SIM-карток залишаються «анонімними» і встановлення активної абонентської картки особи за розмовами якою планується спостереження є складним і не завжди результативним процесом. Законодавець намагався унормувати обов'язковість реєстрації SIM-карт та користування послугами зв'язку лише за умови пред'явлення документів, які ідентифікують особу, проте жоден з таких законопроектів не було прийнято. На нашу думку, наразі це одна з ключових проблем, яка створює ризики неправомірного втручання у приватне спілкування в силу відсутності документального підтвердження належності особи до певної SIM-картки. Відтак, впровадження системи обов'язкової, а не добровільної реєстрації та перереєстрації абонентів мобільного зв'язку із застосуванням паспортних даних або електронної ідентифікації (через BankID чи Дія. Підпис) могло б

стати вагомим кроком у напрямку удосконалення механізму доступу до інформації необхідної для проведення НСРД, і водночас інструментом зміцнення національної безпеки та правопорядку. По-перше, це дозволить точно встановлювати ідентифікаційні ознаки особи, як об'єкта спостереження з метою проведення зняття інформації з електронних комунікаційних мереж. По-друге, відпаде необхідність проведення додаткових слідчо-оперативних заходів для їх з'ясування, що значно відобразиться на процесуальній економії. По-третє, суттєво зменшиться ризик випадкового несанкціонованого втручання у приватне спілкування сторонніх осіб, оскільки існуватиме документальне підтвердження прив'язки абонентської картки до конкретної особи .

Зняття інформації з електронних інформаційних систем за змістом ч.1 ст. 264 КПК являє собою «процес пошуку, виявлення і фіксації відомостей, що містяться в електронній інформаційній системі або її частині, доступ до електронної інформаційної системи або її частини, а також отримання таких відомостей без відома її власника, володільця або утримувача» [7]. Згідно п. 1.11.6 Інструкції: «Зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача полягає в одержанні інформації, у тому числі із застосуванням технічного обладнання, яка міститься в електронно-обчислювальних машинах (комп'ютер), автоматичних системах, комп'ютерній мережі» [57]. Зміст поняття «електронна інформаційна система» з достатньою чіткістю в законодавстві не визначається, проте ЗУ «Про захист інформації в інформаційно-комунікаційних системах» містить термін «інформаційна (автоматизована) система», під якою розуміють «організаційно-технічну систему, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів» [74]. В юридичній та технічній літературі під електронною інформаційною системою найчастіше визначається: «взаємозв'язок технічних засобів (комп'ютерів, серверів, апаратно-програмних комплексів, зовнішніх накопичувачів інформації, локальних комп'ютерних мереж та/або інших технічних засобів. В

той же час, під частинами електронних інформаційних систем слід вважати бази даних, системи управління базами даних, клієнтське програмне забезпечення, доступ до яких обмежується їх власником, володільцем або утримувачем, зокрема застосуванням системи логічного захисту» [75].

З огляду на правову природу, метою даної НСРД є зчитування інформації, яка вже була збережена в певний момент, незалежно від того, чи передавалася вона мережею. Йдеться, зокрема, про доступ до даних, що накопичуються у пам'яті пристроїв, серверів чи у хмарних сховищах. Технічно така операція відбувається, як шляхом безпосереднього фізичного доступу до пристрою (комп'ютера, сервера, мобільного телефону тощо), так і способом віддаленого доступу з використанням спеціалізованих програмно-апаратних комплексів, здатних зчитувати вміст пам'яті, файлів та іншої цифрової інформації.

Застосування системи логічного захисту в інформаційній системі виступає одним із чинників, що унеможлиблює втручання у приватне спілкування без наявності вмотивованої ухвали слідчого судді. При цьому відповідно до ч. 2 ст. 264 КПК: «не потребує дозволу слідчого судді здобуття відомостей з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту» [7]. В таких випадках складається тільки протокол про зняття інформації з електронних інформаційних систем з долученими додатками відповідно до вимог ст. 104-107, 252 та 265 КПК. До прикладу, в постанові ВСУ від 09.04.2020 у справі № 727/6578/17: «наявна в мобільному телефоні засудженого була досліджена шляхом включення телефону та огляду текстових повідомлень, які в ньому знаходились та доступ до яких не був пов'язаний із наданням володільцем відповідного серверу (оператором мобільного зв'язку) доступу до електронних інформаційних систем. За таких обставин суд не виявив порушень процесуального закону, посилаючись на ч. 2 ст. 264 КПК, адже доступ до телефону власником не обмежувався» [76]. Не вимагають дозволу і

ті випадки, коли слідчий, прокурор ознайомлюється з інформацією про особу, яка розміщена в відкритих інтернет-джерелах (соціальних мережах, форумах, блогах), тобто перебуває в вільному доступі.

Ухвала слідчого судді про дозвіл на втручання у приватне спілкування в цьому випадку повинна обов'язково додатково містити ідентифікаційні ознаки електронної інформаційної системи, в якій може здійснюватися втручання у приватне спілкування (ч. 3 ст. 264 КПК). Ідентифікаційними ознаками електронної інформаційної системи є: «1) IP-адреса (IP-Internet Protocol), яка є унікальним ідентифікатором (адресою) пристрою (звичайно комп'ютера або маршрутизатора), підключеного до локальної мережі або Інтернету; 2) доменне ім'я, що дозволяє ідентифікувати в мережі Інтернет веб-сайт або адресу електронної пошти; 3) серійний номер та характеристики автоматизованої системи та ЕОМ» [77, с. 238].

За результатами здійснення «Зняття інформації з електронних комунікаційних мереж» та «Зняття відомостей з електронних інформаційних систем» складається протокол, який повинен відповідати загальним правилам сформульованим в ст. ст. 104-107, 262 КПК. Обсяг інформації, який передавався через комунікаційні мережі підлягає зазначенню в протоколі, а якщо в інформації виявлені відомості мають значення для розслідування певної справи, в протоколі відтворюється певна частина такої інформації (ч. 1 ст. 265 КПК). Зміст інформації, одержаної внаслідок здійснення зняття відомостей з електронних інформаційних систем або їх частин, в свою чергу повинен фіксуватися на відповідному носіїві особою, яка здійснювала зняття у спосіб, що забезпечує обробку, збереження або передання інформації [7]. Такою особою може бути спеціаліст чи уповноважений оперативно-технічного підрозділу залучений на підставі письмового доручення слідчого.

Проаналізувавши два види НСРД, які передбачають негласне втручання у приватне спілкування осіб можемо виокремити такі основні відмінності між ними: «зняття інформації з електронних інформаційних систем або їх частин» передбачає отримання доступу до попередньо збереженої інформації,

яка знаходиться в різноманітних системах зберігання та обробки даних, таких як: персональні комп'ютери, web-сервери, хмарні сховища, бази персональних даних, фізичні накопичувачі інформації (флешки, жорсткі та CD- диски), системи відеоспостереження, CRM/ERP-системи. «Зняття інформації з електронних комунікаційних мереж», в свою чергу, являє технічний процес доступу в реальному часі до інформації, яка передається між абонентами через мережі зв'язку поєднаний з зчитуванням або копіюванням змісту спілкування, яке перехоплюється.

Висновки до розділу II:

1. Проведення НСРД істотно пов'язано з ризиками неправомірного обмеження таємниці спілкування, якщо не було досягнуто розумного балансу між правами особи та інтересами слідства. Вимагається найвищий рівень доведеності «виключної» необхідності такого втручання і взаємозв'язок юридичних та фактичних підстав для його здійснення. Поширеною практикою є штучне завищення правової кваліфікації діянь з метою створити формальні підстави для втручання у приватне спілкування. За таких умов пропонується доповнити п. 3 ч. 2 ст. 248 КПК вимогою про зазначення в клопотанні слідчого, прокурора не тільки правової кваліфікації діяння, а й обґрунтування, що вчинене особою правопорушення відповідає і на момент внесення відомостей до ЄРДР, і на час звернення з клопотанням відповідає необхідному ступеню тяжкості.

2. Сформовано підходи до визначення правової природи кожного з аналізованих видів НСРД, які передбачають втручання у приватне спілкування. Визначено їх суть, зміст, підстави та процесуальний порядок проведення. Здійснено формування рекомендацій щодо удосконалення КПК в частині пов'язаній з їх регламентацією.

3. Доведено недопустимість підміни гласних слідчих дій аудіо-, відеоконтролем особи. Відсутність ознак допиту під час фіксації бесіди особи

є визначальною умовою, дотримання якої забезпечує визнання результатів аудіо, відеоконтролю особи допустимими доказами. Зафіксована бесіда повинна бути невимушеною, без присутності працівників правоохоронних органів та інших осіб залучених в порядку конфіденційного співробітництва, які б задавали послідовні питання щодо розслідуваної справи. За описаних умов «приватність» спілкування не забезпечується (підозрюваний не може розраховувати, що зміст буде збережений в таємниці), а отже дотримання таємниці спілкування не досягається.

4. Обґрунтовано, що кримінальний процесуальний закон містить суттєві недоліки пов'язані з неточністю законодавчого формулювання «тимчасового доступу до речей і документів, які містять охоронювану законом таємницю», в силу чого на практиці виникають численні проблеми з відмежуванням даного заходу забезпечення кримінального провадження від НСРД з втручанням у приватне спілкування. Допустимий обсяг відомостей до яких може бути отриманий доступ в ході «тимчасового доступу до речей та документів» в ст. 162 КПК визначається недостатньо конкретизовано, що призводить до різного розуміння однієї й тієї ж норми і як наслідок створює ризики надмірного втручання у приватне спілкування без належної правової підстави.

5. Встановлено ключові ознаки за якими відбувається відмежування НСРД «зняття інформації з електронних інформаційних систем» від НСРД «зняття інформації з електронних комунікаційних мереж». Зняття інформації з електронних інформаційних систем або їх частин передбачає отримання доступу до попередньо збереженої інформації, яка знаходиться в різноманітних системах зберігання та обробки даних. Зняття інформації з електронних комунікаційних мереж, в свою чергу, являє технічний процес доступу в реальному часі до інформації, яка передається між абонентами через мережі зв'язку поєднаний з зчитуванням або копіюванням змісту спілкування, яке перехоплюється.

6. Обґрунтовано необхідність впровадження обов'язкової реєстрації користувачів послуг мобільного зв'язку за паспортними даними в момент укладення договору з постачальником комунікаційних послуг. По-перше, це дозволить точно встановлювати ідентифікаційні ознаки особи, як об'єкта спостереження з метою проведення зняття інформації з електронних комунікаційних мереж. По-друге, відпаде необхідність проведення додаткових слідчо-оперативних заходів для їх з'ясування, що значно відобразиться на процесуальній економії. По-третє, суттєво зменшиться ризик випадкового неправомірного втручання у приватне спілкування сторонніх осіб, оскільки існуватиме документальне підтвердження прив'язки абонентської картки до конкретної особи .

РОЗДІЛ III. ОСКАРЖЕННЯ РІШЕНЬ ПРО ДОЗВІЛ НА ВТРУЧАННЯ У ПРИВАТНЕ СПІЛКУВАННЯ

Оскарження рішень про дозвіл на втручання у приватне спілкування продовжує залишатися однією з найбільш дискусійних тем у науці кримінального процесуального права, оскільки існують серйозні проблеми з ефективністю правового механізму, що регулює цей процес. Попередньо, в нашому дослідженні було встановлено, що рішення про дозвіл на проведення НСРД пов'язаної з втручанням у приватне спілкування приймається виключно способом постановлення ухвали слідчого судді апеляційного суду в порядку передбаченому ст. ст. 246-249, 258 КПК, а тому завданням подальшого аналізу є дослідження можливостей оспорування законності такого рішення.

Згідно ст. 24 КПК: «кожному гарантується право на оскарження процесуальних рішень, дій чи бездіяльності суду, слідчого судді, прокурора, слідчого в порядку, передбаченому цим Кодексом. Гарантується право на перегляд вироку, ухвали суду, що стосується прав, свобод чи інтересів особи, судом вищого рівня в порядку, передбаченому цим Кодексом, незалежно від того, чи брала така особа участь у судовому розгляді» [7]. Як зазначає М. Є. Савенко: «Запровадження судового контролю за дотриманням прав, свобод та інтересів осіб у кримінальному провадженні не забезпечує достатніх гарантій законності та обґрунтованості обмеження конституційних прав особи на стадії досудового розслідування. Додатковою та необхідною гарантією є можливість апеляційного оскарження цих рішень» [78, с. 100]. Дійсно, як вже було аналізовано у нашому дослідженні, слідчі судді часто вдаються до надмірного формалізму під час постановлення рішень про втручання у приватне спілкування. Уникають дослідження важливих деталей, аби прискорити процес розгляду та надто покладаються на відомості викладені в клопотанні слідчого, прокурора, при цьому не здійснюючи перевірку їх достатності та не співвідносячи ризики втручання.

Вичерпний перелік ухвал слідчого судді, які можуть бути оскаржені в апеляційному порядку під час досудового розслідування встановлюється ч. 1 ст. 309 КПК і до такого списку не віднесено ухвалу слідчого судді про дозвіл на втручання у приватне спілкування (ухвала слідчого судді про дозвіл на проведення НСРД пов'язаної з втручанням у приватне спілкування). Отже, за приписами КПК, оскаржити таку ухвалу окремо в апеляційному порядку неможливо. Складнощів додає і те, що приймається вона слідчим суддею апеляційного суду, що відповідно породжує питання, як тоді взагалі повинен функціонувати механізм оскарження. Неможливість розглядати окремо від рішення суду скаргу на ухвалу слідчого судді про дозвіл на втручання у приватне спілкування, є відображенням волі законодавця обмежити окреме оскарження лише певними рішеннями, а також специфікою самих НСРД.

З огляду на саму суть НСРД (їх неочевидність, негласність, прихованість) та проблеми з неоднозначністю підходів до розсекречення матеріалів, як вже було розглянуто в попередніх розділах, сторони ознайомлюються з правовими підставами проведення НСРД не одразу, а лише з моменту ознайомлення з матеріалами справи (коли слідча дія вже проведена, а досудове розслідування завершено), а в деяких випадках вже на етапі судового розгляду, що потребує специфічного механізму реакції на виявлені порушення в постановлених ухвалях. В рішенні ЄСПЛ у справі «Беллет проти Франції» від 04.12.1995 акцентується: «стаття 6 § 1 Конвенції містить гарантії справедливого судочинства, одним з аспектів яких є доступ до суду. Рівень доступу, наданий національним законодавством, має бути достатнім для забезпечення права особи на суд з огляду на принцип верховенства права в демократичному суспільстві. Для того, щоб доступ був ефективним, особа повинна мати чітку практичну можливість оскаржити дії, які становлять втручання у її права» [79].

Питань про те, як повинно формуватися новітнє бачення шляхів оскарження ухвали слідчого судді про втручання у приватне спілкування постає все більше. Для того щоб втілити ці міркування в реальність,

кримінальне процесуальне законодавство потребує низки концептуальних та докорінних змін, які стосуватимуться не тільки інституту оскарження рішень, а й порядку та умов розсекречення матеріалів, адже як можна вчасно оскаржити ухвалу слідчого судді, коли вона до певного моменту є засекреченою і сторонам про її існування нічого не відомо? А. А. Коваль, в своєму монографічному висловлює наступну думку: «вважаємо, що необхідно передбачити можливість оскарження ухвали слідчого судді суб'єктом, стосовно якого проводилось НСРД, раніше, а саме з моменту її розсекречення. Якщо апеляційний суд визнає незаконними підстави проведення НСРД, то в подальшому це може призвести до визнання доказів недопустимим, а у підсумку – до закриття кримінального провадження ще до початку судових стадій» [48, с. 73]. Хоч пропозиція і видається слушною, проте неоднозначною в моментах її практичної реалізації. Дане питання наразі вченими докорінно не досліджувалося, а тому становить інтерес для подальших наукових напрацювань, так як складнощів на шляху змін надто багато.

За вищевикладених умов процесуальної недоступності апеляційного оскарження ухвал слідчого судді про дозвіл на проведення НСРД пов'язаних з втручанням у приватне спілкування, законодавцем у ч. 3 ст. 309 КПК передбачено можливість висловити заперечення проти суті ухвали під час підготовчого провадження в суді, проте порядок розгляду та наслідки їх подання КПК не врегульовані. Заперечення мають ґрунтуватися на конкретизації істотних порушень норм КПК, допущених при ухваленні рішення слідчим суддею. Наприклад, під час її ухвалення не забезпечено повного й неупередженого з'ясування фактичних обставин, а подані матеріали та докази, покладені в основу висновків, належним чином не перевірено й не досліджено. Таким чином навіть найцінніші для слідства відомості отримані на підставі такої ухвали можуть втратити свою значущість для доказування, бо за доктриною «плодів отруєного дерева» будуть визнані недопустимими.

Основною можливістю розглянути, як відбувається процес подання заперечень та його ефективність для охорони права особи на таємницю

спілкування є дослідження судової практики. До прикладу, у постанові ККС ВСУ від 06.06.2023 у справі № 489/6721/21 було зазначено: «Законодавець, позбавивши сторони права на апеляційне оскарження певних ухвал слідчого судді під час досудового розслідування, не залишив сторони без засобів правового захисту від незаконних або необґрунтованих рішень слідчого судді. Закон надає можливість розглянути ці питання під час судового провадження, передбачивши у частині 3 статті 309 КПК, що щодо ухвал, які не оскаржуються під час досудового розслідування, можуть бути подані заперечення під час підготовчого провадження в суді. Суд, отримавши такі заперечення має їх розглянути під час підготовчого провадження або під час судового розгляду, в залежності від характеру поставленого питання, і прийняти вмотивоване рішення» [80]. За такого тлумачення нормативних приписів судом, дещо розширюється сфера застосування ч. 3 ст. 309 КПК. Учасники справи мають право на розгляд їх заперечень не тільки під час підготовчого провадження в суді, а й під час судового розгляду. На жаль, на практиці судді не завжди дотримуються вимог ч. 3 ст. 309 КПК, наприклад, у постанові ККС ВС від 18.07.2023 (справа № 760/2468/22) констатував, що «суд першої інстанції не перевірів доводи сторін, які стосуються їхньої незгоди із ухвалами слідчих суддів, що не підлягають окремому апеляційному оскарженню. Ненадання відповідей на доводи такого заперечення не лише не ґрунтуються на положеннях чинного кримінального процесуального закону, але й суперечать положенням ч. 3 ст. 309 КПК. Суди зобов'язані належним чином розглянути ці заперечення та прийняти рішення по суті питання, ґрунтуючись на власній оцінці обставин провадження» [81].

На складність застосування цієї норми вказує і Велика палата ВСУ у справі № 243/6674/17-к від 23.05.2018: «зазначена перевірка не є ефективним засобом захисту від можливого порушення ст. 8 ЄКПЛ і статті 1 Першого протоколу до Конвенції, оскільки, по-перше, не в усіх випадках кримінальні справи, у яких було здійснено позапланові перевірки, будуть передані до суду з обвинувальним актом. По-друге, підготовче засідання в суді першої

інстанції, навіть якщо обвинувальний акт передано до суду, може відбутися запізно для того, щоб бути здатним виправити порушення. По-третє, під час підготовчого судового засідання суддя не має повноважень вчиняти дії та приймати рішення, які можуть призвести до виправлення порушення Конвенції, спричиненого втручанням з боку держави» [82]. За такої ситуації дійсно видається справжня критичність умов за яких особа повинна домагатися захисту своїх прав, наявний системний розрив між формальною процедурою і реальною практикою розгляду заперечень, до того ж процесуальні інструменти захисту передбачені КПК через свою запізнілість позбавлені ефективності. Якщо порушення правил розгляду і постановлення ухвали слідчого судді всупереч правам людини констатується вже на етапах підготовчого провадження та судового розгляду, то їх поновлення в повному обсязі вже буде неможливо, адже НСРД санкціоновані такою ухвалою вже будуть проведені, а їх результати можуть стати основою формування обвинувального акту. Д. І. Клепка також відзначає про суто «декларативну» мету існування ч.3 ст. 309 КПК, як висловлюється автор: «у ст. 314–317 КПК не передбачена ані процедура, ані можливість ухвалення рішення за результатами розгляду такого заперечення» [83, с. 295].

О. В. Бабаєва також вказує на недоліки такого способу оспорювання законності ухвал слідчих суддів у підготовчому судовому провадженні, у зв'язку з тим, що суди уникають їх розгляду кількома шляхами: «1) суддя в підготовчому судовому засіданні відмовляє у розгляді такого заперечення, мотивуючи це тим, що КПК не передбачає порядку його розгляду та вирішення; 2) суддя в підготовчому провадженні, призначаючи судовий розгляд на підставі обвинувального акту долучає таке заперечення до ухвали, зазначаючи, що оцінку йому буде надано у судовому розгляді; 3) коли скарга надходить під час судового розгляду, суд відмовляє у розгляді скарги відповідно до ч. 3 ст. 309 КПК, мотивуючи, що подавати її необхідно саме у підготовчому провадженні, а не у судовому розгляді» [84, с. 90]. Ми розділяємо думку науковця і стверджуємо, що така модель оскарження не

гарантує абсолютно нічого для ефективного захисту прав та інтересів осіб, а мета її існування суто формальна, - без гарантій, без процедури та вочевидь без результатів.

Здебільшого, більш поширеною є практика за якої ухвали слідчих суддів стають об'єктом досліджень вже під час судового розгляду разом з протоколом проведеної НСРД. У постанові Великої Палати Верховного Суду від 16.10.2019 р. у справі № 640/6847/15-к наводиться позиція, яка стверджує: «для оцінки доказів, отриманих в результаті НСРД, необхідно дослідити процесуальні документи, які стали підставою для проведення НСРД. Процесуальні документи про дозвіл на проведення НСРД повинні бути взяті до уваги судом, який розглядає справу, оскільки без з'ясування їх змісту неможливо прийняти рішення про допустимість доказів, отриманих в результаті проведення НСРД» [85].

Вочевидь це наштовхує нас на висновок, що суд оцінює докази отримані у результаті проведеної НСРД у взаємозв'язку з ухвалою слідчого судді про дозвіл на втручання у приватне спілкування, як правову підставу втручання у приватне спілкування. За умов дефектності та невідповідності правилам постановлення останньої, весь комплекс отриманої доказової бази за результатами проведеної на її підставі НСРД буде визнаний недопустимими доказами. Як доречно відзначає з цього приводу А.С. Гуменюк в своєму дисертаційному дослідженні: «навіть ті матеріали, які, на перший погляд, можуть здаватися побічними чи незначущими у порівнянні з безпосередніми результатами НС(Р)Д, мають істотне значення для оцінки допустимості доказів. У таких документах – зокрема в постановках слідчого або прокурора, клопотаннях про надання дозволу на проведення НС(Р)Д, відповідних ухвалях слідчого судді, а також дорученнях – може міститися інформація, що вказує на порушення кримінального процесуального законодавства: недотримання вимог до форми та змісту процесуальних рішень, відсутність достатнього обґрунтування необхідності втручання у приватне життя, невідповідність заходів принципу пропорційності тощо» [51 с. 101].

Особливої уваги заслуговує нещодавнє рішення ЄСПЛ прийняте у справі «Денисюк проти України» від 13 лютого 2025 р. (заява № 22790/19), де було чітко наголошено на неспроможності української правової системи забезпечити ефективний правовий захист, який би дозволив заявникам оскаржити законність та необхідність проведення НСРД санкціонованих ухвалою слідчого судді. Заявники стверджували, що під час розгляду їх справ зіткнулися з низкою системних проблем: судовий контроль на етапі надання дозволу був формальним, судді здебільшого копіювали шаблонні формулювання з клопотань слідчих, не здійснюючи оцінки їхньої необхідності і не вимагаючи яких-небудь підтверджуючих матеріалів; нагляду за виконанням ухвал не проводилось. Найбільш істотним порушенням була відмова надати заявникам доступ до матеріалів, що стали підставою для проведення НСРД. ЄСПЛ підтверджуючи наявність нормативних недоліків та констатує порушення ст. 8 ЄКПЛ щодо вимог заявників, зазначив наступне: «Жодна з процедур оскарження передбачена у ч.2 ст. 303, ч.3 ст 309 КПК не може бути застосована незалежно, оскільки суб'єкти НСРД мають дочекатися, коли буде призначено підготовчі засідання у їхніх кримінальних провадженнях, перш ніж подавати відповідні скарги. Ця вимога потенційно може призвести до непередбачуваних затримок», крім того, Суд вказав: «обсяг питань, які вирішуються кримінальним судом у підготовчому засіданні, не включає конкретних повноважень, наданих суддям для перевірки законності чи необхідності дій працівників правоохоронних органів у зв'язку з НСРД, не говорячи вже про будь-які повноваження щодо перегляду обґрунтування, наведеного слідчими суддями під час ухвалення дозволу на проведення таких слідчих дій» [86]. За аналізованих обставин ми переконуємося, що вітчизняне законодавство не забезпечує якісну можливість перевірки законності і необхідності постановлення ухвал слідчих суддів про дозвіл на проведення НСРД пов'язаних з втручанням у приватне спілкування, а наявний механізми оспорювання передбачений ч.3 ст. 309 КПК не працює в сучасних реаліях. Дане рішення, на наше особисте переконання, повинно стати відправною

точкою для позитивних змін, адже наявне свавілля та неврегульованість не сприяє реалізації конституційних прав та свобод громадян.

Критично аналізуючи ситуацію, яка склалася на сьогоднішній день можна констатувати, що інститут оскарження рішень про дозвіл на втручання у приватне спілкування залишається концептуально і нормативно неврегульованим, що породжує серйозні проблеми із забезпеченням справедливого судового розгляду та реалізації права на захист, що негативно відображається і на реалізації права на таємницю спілкування. В силу відсутності механізму окремого апеляційного оскарження даного типу ухвал можна виокремити два доступних, шляхи їх оспорювання: 1) Подання заперечень проти ухвал слідчого судді під час підготовчого провадження та судового розгляду (ч. 3 ст. 309 КПК); 2) Дослідження протоколів та інших матеріалів НСРД у взаємозв'язку з ухвалою слідчого судді про дозвіл на втручання у приватне спілкування під час дослідження доказів у процесі судового розгляду.

Висновки до розділу III

1. Встановлено, що національна модель контролю за постановленими ухвалами слідчих суддів про дозвіл на проведення НСРД пов'язаних з втручанням у приватне спілкування є обмеженою та недостатньо ефективною. Сама суть права на таємницю спілкування потребує найвищого рівня захисту та цілої сукупності гарантій, щодо перегляду рішень, які санкціонують її обмеження. В силу відсутності механізму окремого апеляційного оскарження даного типу ухвал можна виокремити два існуючих шляхи їх оспорювання: 1) Подання заперечень проти ухвал слідчого судді під час підготовчого провадження та судового розгляду (ч. 3 ст. 309 КПК); 2) Дослідження протоколів та інших матеріалів НСРД у взаємозв'язку з ухвалою слідчого

судді про дозвіл на втручання у приватне спілкування під час дослідження доказів у процесі судового розгляду;

2. Констатовано, що весь фактичний контроль за дозвільною діяльністю слідчих суддів зводиться до подання заперечень під час підготовчого провадження та судового розгляду, що на практиці є суто декларативним. Процес розгляду заперечень та спосіб реагування на виявленні помилки в КПК не унормовано, відсутні будь-які повноваження суддів щодо перегляду обґрунтування висловленого слідчими суддями на етапі ухвалення дозволу на проведення НСРД. На практиці не всі суди беруть до уваги доводи сторін, що стосуються незгоди з ухвалами слідчих суддів, що не підлягають окремому апеляційному оскарженню, таким чином видається справжня критичність умов за яких особа повинна домагатися захисту свого права.

3. Механізм передбачений ч. 3 ст. 309 КПК не є способом ефективної заміни окремого оскарження, дані норми КПК не відповідають вимогам щодо якості та зрозумілості закону та породжують лише неоднаковість розуміння процесуального закону. З огляду на це зміст ч. 3 ст. 309 КПК потребує доопрацювання та конкретизації.

4. Ухвала слідчого судді про дозвіл на втручання у приватне спілкування повинна досліджуватися в системі з протоколами та іншими матеріалами проведеної НСРД під час дослідження доказів у процесі судового розгляду. Процесуальний документ, який став підставою для проведення НСРД є ключовим компонентом, який підтверджує допустимість одержаних у подальшому відомостей. Без встановлення його змісту неможливо говорити про повну та об'єктивну перевірку дотримання таємниці спілкування під час проведення процесуальних дій, які її обмежують.

ВИСНОВКИ

У результаті проведеного дослідження сформульовано низку висновків, наукових пропозицій та практичних рекомендацій спрямованих на подолання проблем реалізації таємниці спілкування, як засади кримінального провадження та досягнення поставленої мети та завдань, а саме:

1. Обґрунтовано, що з точки зору доктринального розуміння, «таємниця спілкування, як засада кримінального провадження» є продовженням та відображенням фундаментального конституційного права особи гарантованого ст. 31 КУ - на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції. Підтверджено, що право на повагу до приватного життя є ширшим по відношенню до права на таємницю спілкування, адже останнє становить одну з ключових сфер приватності людини та функціонального втілює комунікативний його вимір. Здатність держави поважати приватність комунікацій особи є одним з ключових елементів, який визначає якість життя сучасної людини та втілює принцип верховенства права.

2. Досліджено, що доктринальне розуміння об'єктів захисту таємницею спілкування є ширшим порівняно з законодавчим, предметом захисту науковцями визначається весь обсяг комунікацій осіб, від класичних листів до переписки в соціальних мережах, мобільних застосунках та месенджерах (таких як Viber, Telegram), адже такі додатки використовують наскрізне шифрування (метод захисту даних), що дозволяє учасникам листування розраховувати на те, що їх спілкування є приватним.

3. Встановлено, що національне законодавство не повною мірою гарантує ясність та однозначність розуміння в питаннях, що стосуються визначення об'єктів, що підпадають під захист «таємниці спілкування». Законодавчі акти не містять легальних дефініцій понять «кореспонденція», «листування», «телефонні розмови», «інші види спілкування». Для того щоб уникнути поширеної серед суб'єктів правозастосування варіативності

розуміння, слід встановити змістовні характеристики кожного з видів передачі інформації. Необхідно переглянути й доцільність закріплення поняття «телеграфної кореспонденції», адже станом на 2025 р. такого засобу зв'язку в Україні не існує, що тільки вказує на моральну застарілість законодавства

4. В світлі міжнародних стандартів та практики ЄСПЛ втручання у приватне спілкування порушуватиме ст. 8 ЄКПЛ, якщо здійснюється не «згідно із законом» (якщо закон не відповідає вимогам щодо якості та передбачуваності застосування), не має однієї або кількох легітимних цілей, зазначених у пункті 2 статті 8 Конвенції (втручання має переслідувати легітимну мету - захист національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб), а також не є «необхідним у демократичному суспільстві» (якщо не було дотримано принципу пропорційності інтересів і причини, надані національними органами влади на його виправдання не були важливими та достатніми) для досягнення цих цілей. Рівною мірою охороняється не тільки «домашнє» спілкування осіб, а й те, яке відбувається на робочому місці, в офісах адвоката, кабінетах державних службовців.

5. Доведено обмеженість судового контролю в сфері дотримання прав людини під час здійснення НСРД. Повноваження слідчого судді закінчуються на етапі надання дозволу, без наявних інструментів подальшого нагляду за виконанням рішення чи можливості отримувати сповіщення про хід проведення та підстави припинення НСРД, яка була попередньо була ним санкціонована. Запропоновано розширити сферу контролю шляхом встановлення обов'язку щодо повідомлення слідчого судді про підстави припинення та результати проведення санкціонованих ним НСРД.

6. Наголошено на проблемі «штучного» створення більш тяжких правових кваліфікацій слідчими, прокурорами з метою спотворення формальних підстав для втручання у приватне спілкування. Вперше запропоновано доповнити п.3 ч.2 ст. 248 КПК вимогою про зазначення в

клопотанні слідчого, прокурора не тільки правової кваліфікації діяння, а й обґрунтування, що вчинене особою правопорушення відповідає і на момент внесення відомостей до ЄРДР, і на час звернення з клопотанням відповідає необхідному ступеню тяжкості.

7. Констатовано, що відсутність ознак допиту під час фіксації бесіди особи є визначальною умовою, дотримання якої забезпечує визнання результатів аудіо, відеоконтролю особи допустимими доказами. Зафіксована бесіда повинна бути невимушеною, без присутності працівників правоохоронних органів та інших осіб залучених в порядку конфіденційного співробітництва, які б задавали послідовні питання щодо розслідуваної справи. За описаних умов «приватність» спілкування не забезпечується (підозрюваний не може розраховувати, що зміст буде збережений в таємниці), а отже дотримання таємниці спілкування не досягається.

8. Доведено, що обсяг інформації до якої може бути отримано доступ в порядку тимчасового доступу до речей і документів, що містять охоронювану законом таємницю суттєво відрізняється від сфери втручання у приватні комунікації особи в порядку проведення НСРД. Незважаючи на те, що законодавство не містить чіткості в цих питаннях, проте на підставі аналізу встановлено, що під час тимчасового доступу до речей і документів дозвіл надається виключно на опрацювання так званої «статичної» інформації про споживача і послуги, яка зберігається у операторів і провайдерів певний проміжок часу і не стосується змісту розмов. Що стосується листів і документів, то можна оглянути та вилучити лише листи, які вже написані або/та отримані адресатом та перебувають на зберіганні у особи, й не знаходяться на етапі відправлення співрозмовнику.

9. Підкреслено, що арешт, огляд та виїмка кореспонденції складають єдину НСРД, яка складається з трьох послідовних етапів. Порядок та підстави проведення арешту, огляду та виїмки кореспонденції в цілому є належно регламентованими та цілісними, що забезпечує ясність їх розуміння на практиці та не викликає особливих проблем.

10. Встановлено критерії відмежування НСРД «зняття інформації з електронних інформаційних систем» від НСРД «зняття інформації з електронних комунікаційних мереж». Зняття інформації з електронних інформаційних систем або їх частин передбачає отримання доступу до попередньо збереженої інформації, яка знаходиться в різноманітних системах зберігання та обробки даних. Зняття інформації з електронних комунікаційних мереж, в свою чергу, являє технічний процес доступу в реальному часі до інформації, яка передається між абонентами через мережі зв'язку поєднаний з зчитуванням або копіюванням змісту спілкування, яке перехоплюється.

11. Вперше обґрунтовано необхідність впровадження процедури обов'язкової реєстрації користувачів послуг мобільного зв'язку за паспортними даними в момент укладення договору з постачальником комунікаційних послуг, як передумову досягнення завдань кримінального провадження. По-перше, це дозволить точно встановлювати ідентифікаційні ознаки особи, як об'єкта спостереження з метою проведення зняття інформації з електронних комунікаційних мереж. По-друге, відпаде необхідність проведення додаткових слідчо-оперативних заходів для їх з'ясування, що значно відобразиться на процесуальній економії. По-третє, суттєво зменшиться ризик випадкового неправомірного втручання у приватне спілкування сторонніх осіб, оскільки існуватиме документальне підтвердження прив'язки абонентської картки до конкретної особи.

12. Встановлено, що національна модель контролю за постановленими ухвалами слідчих суддів про дозвіл на проведення НСРД пов'язаних з втручанням у приватне спілкування є обмеженою та недостатньо ефективною. В силу відсутності механізму окремого апеляційного оскарження даного типу ухвал можна виокремити лише два існуючих шляхи їх оспорювання: 1) Подання заперечень проти ухвал слідчого судді під час підготовчого провадження та судового розгляду (ч.3 ст. 309 КПК); 2) Дослідження протоколів та інших матеріалів НСРД у взаємозв'язку з ухвалою слідчого

судді про дозвіл на втручання у приватне спілкування під час дослідження доказів у процесі судового розгляду;

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України : від 28.06.1996 № 254к/96-ВР : станом на 1 січ. 2020 р. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text> (дата звернення: 27.03.2025).
2. Перепелиця С.І. Дотримання прав особи під час втручання у приватне спілкування в кримінальному провадженні. *Форум права*. 2019. № 55(2). С. 70–79.
3. Про правовий статус іноземців та осіб без громадянства : Закон України від 22.09.2011 № 3773-VI : станом на 6 лют. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/3773-17#Text> (дата звернення: 27.03.2025).
4. Цивільний кодекс України : Кодекс України від 16.01.2003 № 435-IV : станом на 9 квіт. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text> (дата звернення: 27.03.2025).
5. Про поштовий зв'язок : Закон України від 03.11.2022 № 2722-IX : станом на 21 черв. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/2722-20#Text> (дата звернення: 27.03.2025).
6. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX : станом на 1 квіт. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/1089-20#Text> (дата звернення: 04.05.2025).
7. Кримінальний процесуальний кодекс України : Кодекс України від 13.04.2012 № 4651-VI : станом на 26 груд. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/4651-17#Text> (дата звернення: 27.03.2025).
8. Загальна декларація прав людини (рос/укр) : Декларація Орг. Об'єдн. Націй від 10.12.1948. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text (дата звернення: 25.05.2025).

9. Про міжнародні договори України : Закон України від 29.06.2004 № 1906-IV : станом на 15 берез. 2022 р.
URL: <https://zakon.rada.gov.ua/laws/show/1906-15#Text> (дата звернення: 18.05.2025).
10. Шевчук С.В. Українське ділове мовлення: навчальний посібник. 6-те вид., випр. і допов. Київ: Алерта, 2008. 301 с.
11. Шевчук С. Судовий захист прав людини: практика Європейського суду з прав людини у контексті західної правової традиції. Київ: Реферат, 2007. 848 с.
12. Савляк І. І. Таємниця спілкування як засада кримінального провадження: дис. ... канд. юрид. наук : 12.00.09 / Нац. акад. внутр. справ. Київ, 2018. 25 с.
13. Шумило М. Є., Рудей В. С. Реалізація конституційного принципу таємниці листування, телефонній розмов, телеграфної та іншої кореспонденції у досудових стадій кримінального процесу України : монографія. Харків : Бровін О. В., 2012. 208 с.
14. Ткачик А.Б. Таємниця спілкування та її обмеження в кримінальному провадженні: дис. ... доктор філософії : 12.00.09. Львів, 2021. 185 с.
15. Кримінальне процесуальне право України: навч. посібник / Р. І. Благута, Ю. В. Гуцуляк, О. М. Дуфенюк та ін.; за заг. ред. А. Я. Хитри, Р. М. Шехавцова. Львів: ЛьвДУВС, 2017. 774 с.
16. Стрекалов А. Є. Актуальні аспекти прав громадян на приватне життя - таємницю листування, телефонного зв'язку, телеграфної і іншої кореспонденції. *Актуальні проблеми права: теорія і практика*. 2010. № 17. С. 411-420.
17. Вирок Рівненського міського суду Рівненської області від 13.09.2019 р. , судова справа № 569/12334/19 (провадження №1-кп/569/905/19).
URL: <https://reyestr.court.gov.ua/Review/84251500>.(дата звернення: 04.05.2025).

18. Бордун І. В. Захист таємниці кореспонденції в соціальних мережах: підхід Європейського суду з прав людини / І. В. Бордун. Суми, 2020. 37 с.
19. Telegram Datenschutzerklärung. *Telegram*. URL: <https://telegram.org/privacy/ua#7-storonn-platzhn-servsi> (дата звернення: 04.05.2025).
20. Кримінальний процес : підручник / Ю. М. Грошевий, В. Я. Тацій, А. Р. Туманянц, та ін.; за заг. ред. В. Я. Тація, Ю. М. Грошевого, О. В. Капліної, О. Г. Шило. Харків: Право, 2013. 824 с.
21. Шемчушенко Ю. С. Юридична енциклопедія : у 6 т. / редкол.: Ю. С. Шемчушенко (гол.) та ін. Київ. Українська енциклопедія ім. М. П. Бажана, 2004.
22. Садовник Т. В. Обмеження таємниці листування, телефонних розмов, телеграфної та іншої кореспонденції шляхом зняття інформації з телекомунікаційних мереж. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2010. № 2. С. 61 - 64.
23. Кінець епохи: "Укртелеком" припиняє прийом телеграм. *24 Канал*. URL: https://24tv.ua/kinets_epohi_ukrtelekom_pripinyaye_priyom_telegram_n893231 (дата звернення: 04.05.2025).
24. Ківалов С. В., Міщенко С. М., Захарченко В. Ю. Кримінальний процесуальний кодекс України: науково-практичний коментар. Харків: Одісей, 2013. 1104 с.
25. Довідник із застосування статті 8 Європейської конвенції з прав людини. Право на повагу до приватного і сімейного життя, житла і кореспонденції. URL: https://www.echr.coe.int/Documents/Guide_Art_8_UKR.pdf (дата звернення: 04.05.2025).
26. Кондратов Д. Ю. Порухення таємниці кореспонденції (коментар до статті 163 КК України). *Вісник Харківського національного університету внутрішніх справ*. 2010. № 1. С. 71-79

27. Ємчук Л.В. Конституційно-правове регулювання особистого та сімейного життя людини і громадянина : дис. ... канд. юрид. наук : 12.00.02. Ужгород, 2015. 225 с.

28. Міжнародний пакт про економічні, соціальні і культурні права: Резолюція Генеральної Асамблеї від 16 грудня 1966 р. № 2200 А (XXI). URL: http://zakon2.rada.gov.ua/laws/show/995_042 (дата звернення: 24.05.2025).

29. Конвенція про захист прав людини і основоположних свобод: Рада Європи. URL: http://zakon2.rada.gov.ua/laws/show/995_004 (дата звернення: 24.05.2025)

30. Про виконання рішень та застосування практики Європейського суду з прав людини : Закон України від 23.02.2006 № 3477-IV : станом на 2 груд. 2012 р. URL: <https://zakon.rada.gov.ua/laws/show/3477-15#Text> (дата звернення: 25.05.2025).

31. Справа «Класс та інші проти Федеративної Республіки Німеччини». Рішення Європейського суду з прав людини. Практика Європейського суду з прав людини. Рішення. Коментарі. 2002. №4. С. 93-125.

32. Міжнародний захист прав людини : навчальний посібник / кол. авторів ; за заг. ред. О. Б. Онишко. Львів : Львівський державний університет внутрішніх справ, 2022. 540 с.

33. Affaire ben faiza c. France (Application no. 31446/12): Judgment European Court of Human Rights (Fifth Section), 08.02.2018. URL: [https://hudoc.echr.coe.int/eng#%7B"itemid":\["001180657"\]%7D](https://hudoc.echr.coe.int/eng#%7B%22itemid%3A%5B%5D%7D) (дата звернення: 01.06.2025).

34. Справа «Хеглас проти Чеської Республіки» (заява № 5935/02): Європейський суд з прав людини (Секція V), 01.03.2007. URL: [https://hudoc.echr.coe.int/eng#%7B"itemid":\["001-126092"\]%7D](https://hudoc.echr.coe.int/eng#%7B) (дата звернення: 01.06.2025).

35. Справа «Copland проти Сполученого Королівства» (заява № 62617/00): Європейський суд з прав людини (Секція IV), 03.04.2007.

URL: [https://hudoc.echr.coe.int/eng#%7B"itemid": \["001-118562"\]%7D](https://hudoc.echr.coe.int/eng#%7B) (дата звернення: 01.06.2025).

36. Європейський суд з прав людини. Справа «Барбулеску проти Румунії». *Право на приватність*. URL: <https://privacy.khpg.org/1604922584> (дата звернення: 01.06.2025).

37. Європейський суд з прав людини. Справа «Габріель Вебер і Цезар Річард Саравія проти Німеччини». *Право на приватність*. URL: <https://privacy.khpg.org/1604922592> (дата звернення: 03.06.2025).

38. Європейський суд з прав людини. Справа Ліберті та інші проти Сполученого Королівства. *Право на приватність*. URL: <https://privacy.khpg.org/1604922632> (дата звернення: 03.06.2025).

39. Хелфорд проти Сполученого Королівства. *Права людини в Україні*. URL: <https://khpg.org/1363591929> (дата звернення: 11.06.2025).

40. Case Of Michaud V. France (Application no. 12323/11): Judgment European Court of Human Rights (Fifth Section), 06.12.2012. URL: [https://hudoc.echr.coe.int/eng#%7B"itemid%22:%22001-115377%22%7D](https://hudoc.echr.coe.int/eng#%7B) (дата звернення 01.06.2025).

41. Справа «Фернандес Мартінес проти Іспанії» (Заява № 56030/07): Європейський суд з прав людини, (Велика палата), 12 червня 2014р. URL: <https://hudoc.echr.coe.int/app/conversion/pdf> (дата звернення 01.06.2025).

42. Case of Leander v. Sweden (Application no.9248/81): Judgment European Court of Human Rights (Chamber), 26.03.1987. URL: [https://hudoc.echr.coe.int/eng#%7B"itemid%22:%22001-57519%22%7D](https://hudoc.echr.coe.int/eng#%7B) (дата звернення: 01.06.2025).

43. Case Benediktsdóttir V. Iceland (Application no. 38079/06): Judgment European Court of Human Rights (Fourth Section), 16.06.2009. URL: [https://hudoc.echr.coe.int/eng#%7B"itemid%22:%22001-93526%22%7D](https://hudoc.echr.coe.int/eng#%7B) (дата звернення: 10.06.2025).

44. Case of Roman Zakharov v. Russia (Application no. 47143/06): Judgment European Court of Human Rights (Grand Chamber), 04.12.2015. URL:

<https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-159324%22%5D%7D> (дата звернення: 19.06.2025).

45. Справа «Беляєв та Дігтяр проти України» (Заяви №№ 16984/04 та 9947/05): Рішення Європейського суду з прав людини від 16.02.2012. URL: https://zakon.rada.gov.ua/laws/show/974_938#Text (дата звернення: 25.06.2025).

46. Посібник зі статті 8 - Право на повагу до приватного і сімейного життя, житла і кореспонденції. Рада Європи / Європейський суд з людини. 2024. URL: https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_ukr (дата звернення: 25.06.2025).

47. Постанова Касаційного кримінального суду Верховного Суду від 21.03.2018 р., судова справа № 751/7177/14. URL: <https://www.reyestr.court.gov.ua/Review/72938764> (дата звернення: 18.06.2025).

48. Коваль А. А. Забезпечення прав людини при провадженні негласних слідчих (розшукових) дій : монографія , Миколаїв: ЧНУ ім. Петра Могили, 2019. 264 с.

49. Про прокуратуру : Закон України від 14.10.2014 № 1697-VII : станом на 4 квіт. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/1697-18#Text> (дата звернення: 30.06.2025).

50. Гуменюк А. Судовий контроль як інструмент забезпечення законності проведення негласних слідчих (розшукових) дій. *Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру (з нагоди 30-річчя проголошення незалежності України та 25-річчя прийняття Конституції України)* : матеріали Міжнародної науково-практичної конференції (м. Одеса, 21.05.2021 р.). У 2-х т. / за заг. ред. С. Ківалова. Одеса : Видавничий дім «Гельветика», 2021. Т. 2. С. 337 – 340.

51. Гуменюк А. С. Допустимість доказів, отриманих у результаті проведення негласних слідчих (розшукових) дій : дис. ... доктора філос. : / Національний університет «Одеська юридична академія» , Одеса, 2025. 248 с.

52. Кримінально-виконавчий кодекс України : Кодекс України від 11.07.2003 № 1129-IV : станом на 4 лип. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/1129-15#Text> (дата звернення: 04.07.2025).

53. Постанова Касаційного кримінального суду Верховного суду від 07.10.2020 р., судова справа № 235/5633/18 (провадження № 51-1770км20). URL: <http://reyestr.court.gov.ua/Review/92173700>. (дата звернення: 04.07.2025).

54. Мирошниченко Ю.М. Негласні слідчі (розшукові) дії: підстави проведення. *Правова позиція*. 2019. № 2 (23). С. 117-121.

55. Постанова Касаційного кримінального суду Верховного Суду від 14.05.2024 р., судова справа № 164/1293/17 (провадження № 51-4339км23). URL: <https://reyestr.court.gov.ua/Review/119212842>. (дата звернення: 10.07.2025).

56. Постанова Касаційного кримінального суду Верховного Суду від 24.01.2022 р., судова справа № 758/5744/17 (провадження № 51-5191км19) URL:<https://reyestr.court.gov.ua/Review/102865750>. (дата звернення: 10.07.2025).

57. Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : Наказ Ген. прокуратури України від 16.11.2012 № 114/1042/516/1199/936/1687/5.

URL: <https://zakon.rada.gov.ua/laws/show/v0114900-12#Text> (дата звернення: 23.07.2025).

58. Шерудило В.О. Судовий контроль під час проведення негласних слідчих (розшукових) дій, пов'язаних з втручанням у приватне спілкування. *Право і суспільство*. 2018. №3. Частина 2. С. 310-315.

59. Постанова колегії суддів Великої палати ВС від 16.10.2019 р. , судова справа № 640/6847/15-к (провадження № 13-43кс19) URL: <https://reyestr.court.gov.ua/Review/85174578>. (дата звернення:24.07.2025).

60. Кримінальний кодекс України : Кодекс України від 05.04.2001 № 2341-III : станом на 17 лип. 2025 р.
URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (дата звернення: 27.07.2025).

61. Постанова Касаційного кримінального суду Верховного суду від 18.03.2025 р., судова справа № 723/884/17 (провадження № 51-6556км23)
URL: <https://reyestr.court.gov.ua/Review/126259374>. (дата звернення: 27.07.2025).

62. Постанова Касаційного кримінального суду Верховного суду від 26.05.2022 р., судова справа № 753/16804/17 (провадження № 51-5813км21)
URL: <https://reyestr.court.gov.ua/Review/104583150>. (дата звернення: 27.07.2025).

63. Постанова Касаційного кримінального суду Верховного суду 23.11.2023 р., судова справа №731/275/19 (провадження №51-1524км23).
URL:<https://reyestr.court.gov.ua/Review/115860918>. (дата звернення: 29.07.2025).

64. Вирок Вищого антикорупційного суду від 30.05.2023 р., судова справа № 127/13972/17 (Провадження № 1-кп/991/177/19). URL: <https://reyestr.court.gov.ua/Review/111192800>. (дата звернення: 29.07.2025).

65. Про деякі питання здійснення слідчим суддею суду першої інстанції судового контролю за дотриманням прав, свобод та інтересів осіб під час застосування заходів забезпечення кримінального провадження: Лист Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ від 05.04.2013 р. № 223-559/0/4-13. URL: <https://zakon.rada.gov.ua/laws/show/v0558740-13#Text>. (дата звернення: 30.07.2025).

66. Вирок Вищого антикорупційного суду від 14.07.2021 р., судова справа №707/146/17 (провадження 1-кп/991/175/19). URL: <https://reyestr.court.gov.ua/Review/98293910>. (дата звернення: 10.08.2025).

67. Гловюк І. В. Розгляд слідчим суддею клопотання про тимчасовий доступ до речей і документів. *Актуальні питання досудового розслідування слідчими органів внутрішніх справ: проблеми теорії та практики*: матеріали всеукр. наук.-практ. конф., м.Дніпропетровськ, 18-19 квітня 2013р. Київ, 2013. С. 52 – 56.

68. Сліпченко В. І. Тимчасовий доступ до речей і документів: процесуальний порядок отримання. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2013. № 2. С. 507 – 514.

69. Сергєєва Д. Б. Щодо класифікації негласних слідчих (розшукових) дій. *Вісник кримінального судочинства*. 2015. № 2. С. 69-76.

70. Галаган В. І., Шум В. В. Процесуальний порядок накладення арешту на кореспонденцію у кримінальному провадженні України: монографія, Київ, 2017. 168 с.

71. Негласні слідчі (розшукові) дії та використання результатів оперативно розшукової діяльності у кримінальному провадженні: навч.-практ. посіб. / Кудінов С. С. , Шехавцов Р.М., Дроздов О.М., Гриненко С. О. Харків: Оберіг, 2013. 344 с.

72. Бабкова В. С. Проблеми визнання результатів зняття інформації з транспортних телекомунікаційних мереж належними та допустимими доказами. *Юрист України*. 2018. № 2. С. 68-75.

73. Луцик В.В. Зняття інформації з електронних комунікаційних мереж: фокус новел. *Юридичний науковий електронний журнал*. 2022. №. 8. С. 500–504. URL: <https://doi.org/10.32782/2524-0374/2022-8/113> . (дата звернення: 25.08.2025).

74. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР : станом на 20 квіт. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/80/94-вр#Text> (дата звернення: 29.08.2025).

75. Говоруха В. І., Степанов В. А. Зняття інформації з електронних інформаційних систем як різновид негласних слідчих (розшукових) дій. *Інформація і право*. 2020. № 3 (34). С. 69–74.

76. Постанова Верховного Суду від 09 квітня 2020 р., судова справа №727/6578/17 (провадження № 51-4494км19). URL: <https://reyestr.court.gov.ua/Review/88749345>. (дата звернення: 29.08.2025).

77. Олашин М. М. Кримінальні процесуальні аспекти зняття інформації з електронних інформаційних систем. *Вісник Львівського торговельно-економічного університету. Юридичні науки*. Львів, 2018. № 7. С. 233 - 242.

78. Савенко М.Є. Апеляційне оскарження та перегляд ухвал слідчого судді, постановлених під час досудового розслідування: дис. ... канд. юрид. наук : 12.00.09. Харків, 2020. 281 с.

79. Case of Bellet V. France (Application no. 23805/94): Judgment European Court of Human Rights (Chamber), 4 december 1995. URL: <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-57952%22%5D%7D>. (дата звернення 30.08.2025)

80. Постанова Касаційного кримінального суду Верховного суду від 06.06.2023, судова справа № 489/6721/21(провадження № 51-4081км22). URL: <https://reyestr.court.gov.ua/Review/111431187>(дата звернення: 29.08.2025).

81. Постанова Касаційного кримінального суду Верховного суду від 18.07.2023 р., судова справа № 760/2468/22 (провадження № 51-2937км23). URL: <https://reyestr.court.gov.ua/Review/112315631>. (дата звернення: 30.08.2025).

82. Постанова Великої палати Верховного Суду від 23.05.2018 р., судова справа № 243/6674/17. URL: <https://reyestr.court.gov.ua/Review/74188517>. (дата звернення: 30.08.2025).

83. Клепка Д.І. Якісна характеристика нормативного регулювання порядку оскарження ухвал слідчого судді під час досудового розслідування. *Юридичний науковий електронний журнал*. 2021. № 1. С. 292–295.

84. Бабаєва О. В. Підготовче провадження у системі стадій кримінального процесу України: дис. ... канд. юрид. наук: 12.00.09. Харків, 2019. 292 с.

85. Постанова Великої Палати Верховного Суду від 16.10.2019 р., судова справа № 640/6847/15-к (провадження № 13-43к19). URL: <https://reyestr.court.gov.ua/Review/85174578> (дата звернення: 29.08.2025).

86. Case of Denysyuk and Others v. Ukraine (Application no. 22790/19, 23896/20, 25803/20 and 31352/20): Judgment European Court of Human Rights (Fifth Section), 13 February 2025. URL: <https://hudoc.echr.coe.int/eng?i=001-241747> (дата звернення: 29.08.2025).