

Міністерство освіти і науки України
Національний університет «Києво-Могилянська академія»
Факультет правничих наук
Кафедра кримінального та кримінального процесуального права

Магістерська робота

освітній ступінь – магістр

на тему: **«Таємниця спілкування та її охорона у кримінальному провадженні
України»**

«Privacy of communication and its protection in criminal proceedings of Ukraine»

Виконала: студентка 2-го року навчання

Спеціальності 081 «Право»

Двірник Олена Сергіївна

Керівник: Удовенко Ж.В.

кандидат юридичних наук, доцент

кафедри кримінального та

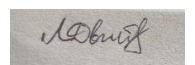
кримінального процесуального права,

Рецензент _____

Магістерська робота захищена з оцінкою

Секретар ЕК _____

«___» _____ 20__ р.



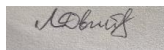
Київ - 2022

**Декларація
академічної доброчесності
студента/ студентки НаУКМА**

Я, Двірник Олена Сергіївна, студентка 2 року навчання факультету правничих наук, спеціальність 081 право, адреса електронної пошти olena.dvirnyk@ukma.edu.ua

- підтверджую, що написана мною кваліфікаційна/магістерська робота на тему «Таємниця спілкування та її охорона у кримінальному провадженні України» відповідає вимогам академічної доброчесності та не містить порушень, передбачених пунктами 3.1.1-3.1.6 Положення про академічну доброчесність здобувачів НаУКМА від 07.03.2018 року, зі змістом якого ознайомлена;
- підтверджую, що надана мною електронна версія роботи є остаточною і готовою до перевірки;
- згодна на перевірку моєї роботи на відповідність критеріям академічної доброчесності, у будь-який спосіб, у тому числі порівняння змісту роботи та формування звіту подібності за допомогою електронної системи Unicheck.
- даю згоду на архівування моєї роботи в репозитаріях та базах даних університету для порівняння цієї та майбутніх робіт.

17.05.2022



О. С. Двірник

Дата

Підпис

Прізвище, ініціали

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ	3
ВСТУП.....	4
РОЗДІЛ 1. ПОНЯТТЯ ТАЄМНИЦІ СПІЛКУВАННЯ У МІЖНАРОДНОМУ ТА НАЦІОНАЛЬНОМУ ПРАВІ	6
1.1. Міжнародні стандарти захисту таємниці спілкування.....	6
1.2. Теоретико-правові аспекти таємниці спілкування в Україні.....	20
РОЗДІЛ 2. ОХОРОНА ТАЄМНИЦІ СПІЛКУВАННЯ ПІД ЧАС КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ.....	38
2.1. Охорона таємниці спілкування під час здійснення тимчасового доступу до речей і документів.....	38
2.2. Охорона таємниці спілкування під час проведення негласних слідчих (розшукових) дій.....	47
2.3. Іноземний досвід втручання у приватне спілкування.....	61
2.3.1. Втручання у приватне спілкування за законодавством Федеративної Республіки Німеччина.....	62
2.3.2. Втручання у приватне спілкування за законодавством Естонської Республіки.....	64
2.3.3. Втручання у приватне спілкування за законодавством Швейцарської Конфедерації.....	66
ВИСНОВКИ	69
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	73

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

Пакт	Міжнародний пакт про громадянські і політичні права
Конвенція	Конвенція про захист прав і основоположних свобод
Суд, ЄСПЛ	Європейський суд з прав людини
КПК України	Кримінальний процесуальний кодекс України
НСРД	Негласні слідчі (розшукові) дії
Інструкція	Інструкція про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні

ВСТУП

Актуальність дослідження. Конституцією України визначено, що утвердження і забезпечення прав і свобод людини є головним обов'язком держави. Отже, Україна в особі органів влади має сприяти реалізації людиною її прав та свобод та створити належні гарантії їх захисту від порушень. В той же час достатньо складним залишається питання забезпечення балансу між необхідністю дотримання прав людини та інтересами суспільства і держави у захисті від кримінальних правопорушень і швидкому досудовому розслідуванні та судовому розгляді під час кримінального провадження. Не виключенням у цьому контексті є й охорона права особи на таємницю спілкування, адже здійснюючи втручання у приватні комунікації особи, з одного боку органи досудового розслідування можуть отримати відомості, необхідні для встановлення усіх обставин вчинення злочину та особи й місцезнаходження злочинця, проте з іншої сторони такі обмеження неминуче зачіпають й третіх осіб, що спілкуються з підозрюваним, та створюють ризики зловживань у цій сфері, що може призвести зокрема до розголошення інформації щодо обставин приватного життя, які вони бажають зберегти в таємниці. Іншою проблемою є обсяг таємниці спілкування, оскільки стрімкий науково-технічний розвиток призводить до появи нових способів передачі інформації між людьми та постійного змінення вже існуючих, і законодавець може не завжди встигати охопити сферою правового регулювання таємниці спілкування усі існуючі засоби зв'язку. Саме тому необхідним є ґрунтовний аналіз поняття таємниці спілкування, особливостей її охорони на національному та міжнародному рівні задля визначення допустимих меж втручання у право особи на таємницю спілкування під час кримінального провадження, а також пошуку недоліків українського правового регулювання та шляхів їх вирішення.

Ступінь наукової розробки теми. Різні аспекти таємниці спілкування широко висвітлювалася науковцями, серед яких: В.І. Галаган,

Д.Ю.Кондратов, В.В. Назаров, В.С.Рудей, А.Б. Ткачик, Ж.В.Удовенко, М.Є.Шумило та інші.

Об'єктом дослідження є правовідносини, що виникають під час здійснення втручання у таємницю спілкування у кримінальному провадженні.

Предметом дослідження є таємниця спілкування та її охорона у кримінальному провадженні України.

Метою дослідження є визначення теоретичних основ та розробка практичних рекомендацій, спрямованих на встановлення правових механізмів забезпечення охорони права особи на таємницю спілкування.

Для досягнення цієї мети потрібно було виконати такі *завдання*:

1) *визначити* міжнародні стандарти захисту таємниці спілкування на основі аналізу міжнародно-правових актів та практики Європейського суду з прав людини;

2) *розкрити* зміст поняття «таємниця спілкування» відповідно до українського законодавства та національної судової практики;

3) *проаналізувати* особливості охорони на нормативному рівні таємниці спілкування під час здійснення тимчасового доступу до речей і документів та втручання у приватне спілкування у кримінальному провадженні України;

4) *встановити* можливі недоліки правового регулювання та порушення прав особи з боку компетентних органів;

5) *порівняти* гарантії забезпечення таємниці спілкування в Україні та в інших державах і на основі цього *визначити* способи усунення недоліків українського законодавства.

РОЗДІЛ 1

ПОНЯТТЯ ТАЄМНИЦІ СПІЛКУВАННЯ У МІЖНАРОДНОМУ ТА НАЦІОНАЛЬНОМУ ПРАВІ

1.1. Міжнародні стандарти захисту таємниці спілкування.

Відповідно до ст. 9 Конституції України чинні міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, є частиною національного законодавства України [1]. Згідно з ч. 2 ст. 19 Закону України «Про міжнародні договори України» 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 [2]. З цього випливає, що в Україні встановлено примат міжнародного права над національним, тому на державу покладено обов'язок забезпечувати реалізацію взятих на себе зобов'язань за міжнародними договорами, що проявляється зокрема у імплементації відповідних положень в національне законодавство. Отже, дослідження сутності таємниці спілкування потрібно розпочати з аналізу міжнародних стандартів її правового регулювання та захисту як підґрунтя для формування національної законодавчої бази.

Вперше на міжнародному рівні гарантії таємниці спілкування були проголошені у ст. 12 Загальної декларації прав людини від 10 грудня 1948 року, згідно з якою 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. Як зазначено у ч. 2 ст. 29 Декларації, при здійсненні своїх прав і свобод кожна людина повинна зазнавати тільки таких обмежень, які встановлені законом виключно з метою забезпечення належного визнання і поваги прав і свобод інших та забезпечення справедливих вимог моралі, громадського

порядку і загального добробуту в демократичному суспільстві [3].

Схожі гарантії наявні і у ст. 17 Міжнародного пакту про громадянські і політичні права від 16 грудня 1966 року, відповідно до якої 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. Також, як зазначено у ст. 2 кожна держава-учасниця Пакту зобов'язана забезпечити всякій особі, права і свободи якої, визнані в цьому Пакті, порушено, ефективний засіб правового захисту, навіть коли це порушення було вчинене особами, що діяли як особи офіційні; забезпечити, щоб право на правовий захист для будь-якої особи, яка потребує такого захисту, встановлювалось компетентними судовими, адміністративними чи законодавчими властями або будь-яким іншим компетентним органом, передбаченим правовою системою держави, і розвивати можливості судового захисту; забезпечити застосування компетентними властями засобів правового захисту, коли вони надаються [4].

У Конвенції про захист прав і основоположних свобод від 4 листопада 1950 року таємниця спілкування виокремлена як складова права на повагу до приватного і сімейного життя. Так, згідно зі ст. 8 Конвенції кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції. 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 [5]. Особливістю Конвенції у порівнянні з наведеними вище документами є наявність юридичного механізму захисту гарантованих нею прав, який полягає у можливості будь-якої особи після вичерпання всіх національних засобів юридичного захисту звернутися зі

скаргою до Європейського суду з прав людини. Розглядаючи справи, Суд здійснює тлумачення положень Конвенції, та визначає, чи мало місце порушення Конвенції з урахуванням критеріїв, сформованих у ході правозастосовної діяльності. Враховуючи, що відповідно до ст. 17 Закону України «Про виконання рішень та застосування практики Європейського суду з прав людини» Конвенцію та рішення ЄСПЛ українські суди мають використовувати як джерело права, необхідним є дослідження прецедентної практики ЄСПЛ щодо захисту таємниці спілкування [6].

Для того щоб встановити, чи відбулося втручання в права, гарантовані ст. 8 Конвенції, Суд повинен перевірити, чи підпадає спілкування заявника під поняття «кореспонденція» та «приватне життя». Враховуючи швидкий розвиток технологій, що спричиняє появу нових форм спілкування, ЄСПЛ застосовує динамічний підхід до тлумачення кореспонденції і відносить до неї найрізноманітніші форми міжособистісних комунікацій. Поняттям «кореспонденція» охоплюються як письмова кореспонденція, що передається поштово-телеграфним зв'язком (листи, телеграми тощо), так і телефонні розмови, а також спілкування, що здійснюється з використанням нових технологій, зокрема, повідомлення електронної пошти, Інтернет-спілкування, телекси, повідомлення на пейджери, приватна радіотрансляція, дані, що зберігаються на комп'ютерних серверах тощо [7, с. 80]. Термін «приватне життя» так само тлумачиться досить широко і не має вичерпного визначення [8, с. 26]. У справі «Niemietz v. Germany» Суд зазначив, що¹

«не вважає за можливе або необхідне намагатися надати вичерпне визначення поняття «приватне життя». Було б надмірно суворим обмежувати його «внутрішнім колом», у якому кожен може жити власним життям на свій розсуд, і повністю виключати з нього зовнішній світ, не охоплений цим колом. Повага до приватного життя до деякої міри має включати в себе й право встановлювати й розвивати відносини з іншими людьми. Більше того, немає принципових підстав вважати, що таке розуміння «приватного життя» виключає діяльність професійного та ділового характеру; саме у своїй роботі більшість людей мають значну, якщо не найістотнішу, можливість розвивати відносини із зовнішнім світом. Ця точка

¹ Тут і далі переклад автора (Двірник О. С.), якщо не зазначено інше

зору підтверджується тим фактом, що, як справедливо зазначила Комісія, не завжди чітко можна розрізнити, які види діяльності особи є частиною її професійного чи ділового життя, а які ні. Таким чином, особливо якщо особа займається незалежною професійною діяльністю, її робота в цьому контексті може бути невід'ємною частиною її життя до такої міри, що стає неможливим дізнатися, в якості кого вона діє в даний момент часу. Відмова у захисті за ст. 8 на тій підставі, що оскаржуваний захід пов'язаний лише з професійною діяльністю – як запропонував Уряд у цій справі – в даному випадку може призвести до нерівного ставлення, оскільки такий захист залишався б доступним лише для того, чия професійна і непрофесійна діяльність були настільки переплетені, що їх неможливо було б розрізнити... Не завжди можна здійснити чітке розмежування також і з тієї причини, що займатися діяльністю, яку можна віднести до професійної або ділової, можна й за своїм місцем проживання, і навпаки, можна займатися справами, що не стосуються професійної сфери, в офісі або комерційних службових приміщеннях» [9].

Отже, за тлумаченням ЄСПЛ поняття «приватне життя» не обов'язково зводиться виключно до приватних комунікацій особи з її родиною та друзями, і може охоплювати ділову активність особи, а тому й поняття «кореспонденція» може включати в себе пов'язані з професійною діяльністю документи. Так, у справі «M.N. and Others v. San Marino» Суд поширив дію ст. 8 Конвенції на особисті документи особи, а саме банківські дані, отримані з банківських виписок, чеків, довірчих розпоряджень і електронних листів, зазначивши, що

«інформація, отримана з банківських документів, безсумнівно, є персональними даними щодо особи, незалежно від того, чи є вона конфіденційною інформацією чи ні... така інформація може також стосуватися ділових операцій, і немає принципових підстав для виправдання виключення діяльності професійного чи ділового характеру з поняття «приватне життя»... Стаття 8 захищає конфіденційність усіх обмінів, у яких особи можуть брати участь з метою комунікації. Більше того, електронні листи чітко підпадають під визначення кореспонденції» [10].

Спілкування, що здійснюється на робочому місці, за певних обставин може потрапляти під охорону ст. 8 Конвенції. Наприклад, у справі «Хелфорд проти Сполученого Королівства» заявниця скаржилася на незаконне перехоплювання дзвінків з її службового телефону з метою отримання інформації для використання проти неї у справі про дискримінацію, що на її

думку становило порушення Конвенції. Суд дійшов висновку, що телефонні розмови, які здійснюються зі службових приміщень, а також з дому, підпадають під поняття «приватне життя» та «кореспонденція» за змістом ст.8 адже заявниця «могла мати розумні очікування щодо конфіденційності таких переговорів, і ці очікування підкріплювалися низкою чинників», а саме у її кабінеті було встановлено два телефони, один із яких спеціально призначався для її особистого користування. Також заявницю запевнили, що вона може використовувати свої службові телефони для переговорів з приводу розгляду її справи про статеву дискримінацію, не було доказів попередження її про те, що переговори за допомогою внутрішньої телекомунікаційної системи управління поліції Мерсисайда, у якому вона тоді працювала, можуть бути піддані перехопленню [11].

У справі «Copland v. the United Kingdom» Суд вказав, що збір та зберігання інформації, що стосувалася використання заявницею телефону, електронної пошти та Інтернету без її відома, становило втручання в її право на повагу до приватного життя та кореспонденції, адже їй не було надано жодного попередження про те, що її дзвінки підлягають моніторингу, тому вона мала розумні очікування конфіденційності дзвінків з її робочого телефону; те саме стосувалося й використання електронної пошти та Інтернету. При цьому «не має значення, що дані, які зберігав коледж, не були розголошені або використані проти заявниці у дисциплінарному або іншому провадженні» [12].

Як впливає з проаналізованих рішень, важливим критерієм для оцінки, чи охоплюється спілкування особи, що здійснювалося на робочому місці, поняттями «приватне життя» та «кореспонденція» для цілей ст. 8 Конвенції, є розумність очікувань особи щодо приватності спілкування, яка полягає у відсутності обґрунтованих підстав вважати, що особисті комунікації особи можуть бути піддані втручання, зокрема, через відсутність інформування про моніторинг. Водночас ЄСПЛ не заперечує можливості моніторингу службової кореспонденції роботодавцем. Однак, як зазначив

Суд у справі «Барбулеску проти Румунії», що стосувалася звільнення заявника за особисте листування через Yahoo Messenger під час роботи, «національні органи влади повинні забезпечити, щоб введення роботодавцем заходів моніторингу кореспонденції та інших комунікацій, незалежно від обсягу та тривалості таких заходів, супроводжувалося належними та достатніми гарантіями проти зловживання» [13].

При визначенні правомірності спостереження за комунікаціями на робочому місці мають бути враховані наступні чинники:

- «(i) чи було повідомлено працівнику про можливість того, що роботодавець може вжити заходи для моніторингу кореспонденції та інших комунікацій, і про втілення таких заходів. Хоча на практиці працівники можуть бути проінформовані різними шляхами в залежності від конкретних фактичних обставин кожної справи, Суд вважає, що для того, щоб заходи вважалися тими, що відповідають вимогам статті 8 Конвенції, повідомлення повинно бути чітким щодо характеру моніторингу та повинно надаватися заздалегідь;
- (ii) обсяг моніторингу з боку роботодавця та ступінь втручання у приватність працівника. У цьому відношенні слід розрізняти моніторинг потоку повідомлень та їх змісту. Слід також взяти до уваги те, чи усі повідомлення підлягали моніторингу, або лише їх частина, як і питання того, чи обмежувався моніторинг часом та кількістю осіб, які мали доступ до результату. Це також стосується обмежень у просторі моніторингу;
- (iii) чи надав роботодавець законні підстави для виправдання моніторингу повідомлень та доступу до їх фактичного контексту. Оскільки моніторинг змісту повідомлень є за своїм характером більш агресивним методом, він потребує більш значного виправдання;
- (iv) чи було можливо встановити систему моніторингу на основі менш агресивних методів та засобів, ніж прямий доступ до змісту повідомлень працівника. У цьому зв'язку повинна мати місце оцінка того, чи могла мета, яку переслідував роботодавець, бути досягнута без прямого доступу до повного змісту повідомлень працівника, у світлі конкретних обставин кожної справи;
- (v) наслідки моніторингу для працівника, який йому підлягає;
- (vi) чи надавалися працівнику належні гарантії, особливо коли моніторинг, здійснюваний роботодавцем, носив агресивний характер. Такі гарантії повинні забезпечити, зокрема, щоб роботодавець не міг отримати доступ до фактичного змісту відповідних повідомлень, якщо працівник не міг бути проінформований заздалегідь про таку можливість» [13].

Суд встановив порушення ст. 8 Конвенції у цій справі, аргументувавши

це тим, що національні суди не дослідили, чи було завчасно (до початку моніторингу) повідомлено заявника про можливість моніторингу повідомлень з робочого месенджера, характер та обсяг моніторингу, рівень втручання у приватне життя та кореспонденцію; також не було визначено «конкретні підстави, які б виправдовували введення моніторингу; чи міг роботодавець скористуватися заходами, пов'язаними з меншим рівнем втручання у приватне життя та кореспонденцію заявника; чи можна було отримати доступ до розмов без його відома» [13].

Перевіряючи дотримання вимог Конвенції при здійсненні втручання у приватне спілкування, ЄСПЛ аналізує, чи відбувалося воно з дотриманням наступних критеріїв: здійснювалося згідно з законом, переслідувало мету, передбачену ч. 2 ст. 8, та було необхідним у демократичному суспільстві. У справі «Круслен проти Франції» Суд зазначив, що словосполучення «згідно з законом» вимагає, щоб «захід, який розглядається, мав певні підстави в національному праві; воно також передбачає певну якість такого закону, вимагаючи, щоб він був доступний для даної особи і вона також могла передбачити наслідки його застосування до неї та щоб закон не суперечив принципіві верховенства права» [14]. У справі «Ювіг проти Франції» Суд вказав, що в якості правових підстав він розглядає як статутне право, так і прецеденту практику [15]. У згаданих вище справах «Copland v. the United Kingdom» та «Хелфорд проти Сполученого Королівства» Судом було встановлено порушення вимоги здійснення втручання відповідно до закону з огляду на відсутність будь-яких положень у національному законодавстві, що регулювали таке втручання [11; 12]. Доступність закону передбачає можливість особи вільно ознайомитися з його змістом, для чого достатньо його офіційного опублікування, або ж за відсутності такого опублікування, доступності у правовій базі даних Інтернету [16; 17]. Як відмітив Суд у справі «Кеннеді проти Сполученого Королівства», передбачуваність закону

«не може означати, що особа повинна мати можливість передбачити, коли органи влади можуть перехопити її повідомлення, щоб мати можливість адаптувати свою

поведінку. Однак особливо там, де повноваження виконавчої влади, здійснюються таємно, ризики свавілля очевидні. Тому важливо мати чіткі, детальні правила перехоплення телефонних розмов, особливо, оскільки технологія, доступна для використання, постійно стає все більш досконалою. Внутрішнє законодавство повинно бути достатньо чітким, щоб дати громадянам належну інформацію про обставини та умови, на яких органи державної влади уповноважені вдаватися до таких заходів» [18].

У справі «Malone v. United Kingdom» Суд констатував, що закон суперечитиме принципу верховенства права, якщо дискреція компетентних органів не буде обмеженою. Тому у законі мають «бути визначені обсяг та умови здійснення владних повноважень з достатньою ясністю по відношенню до встановленої законом мети з тим, щоб забезпечити особі адекватний захист проти свавілля» [19]. Згідно з висновком Суду у справі «Dudchenko v. Russia» у правових нормах, що регулюють процедуру здійснення втручання у спілкування, задля уникнення зловживань мають бути чітко визначені наступні гарантії: «характер, масштаби і тривалість можливих заходів, підстави, необхідні для наказу про їх здійснення, органи, уповноважені вирішувати, здійснювати і контролювати їх, і засоби правового захисту, передбачені національним законодавством» [20]. Так, у справі «Волохи проти України» Суд дійшов висновку, що положення законодавства, яке регулювало перегляд кореспонденції, не визначали з достатньою чіткістю межі та умови здійснення повноважень органами влади, та не передбачали гарантій захисту від зловживань, тому що в ньому не містилися вказівки щодо осіб, до яких застосовуються заходи, обставин, за яких вони вживаються, та строків, які мають встановлюватись і дотримуватись [16]. Крім того, Суд акцентував увагу і на необхідності здійснення ефективного судового контролю над втручанням, адже саме «судовий контроль надає найбільші гарантії незалежності, безсторонності та здійснення належного провадження»; у даному випадку законодавство не передбачало «жодного проміжного перегляду постанови у розумні проміжки часу або будь-яких строків для такого втручання... додаткового залучення

судових органів для нагляду за діяльністю правоохоронних органів», внаслідок чого постанова про накладення арешту на кореспонденцію заявників залишалася чинною протягом року після закриття справи проти їхнього родича [16]. У справі «Кеннеді проти Сполученого Королівства» в контексті розгляду питання щодо правомірності прослуховування телефонних розмов ЄСПЛ було дещо доповнено правові гарантії. Окрім зазначеного, закон має також передбачати

«характер правопорушень, які можуть спричинити наказ про перехоплення, категорії людей, телефони яких можуть прослуховуватися, процедуру вивчення, використання та зберігання отриманих даних, запобіжні заходи, які слід вживати при передачі даних іншим особам, та обставини, за яких записи можуть або повинні бути стерті, а стрічки знищені» [18].

На нашу думку, слід детально проаналізувати зміст кожної з гарантій. Стосовно характеру правопорушень у справі «Роман Захаров проти Росії» Суд підкреслив, що «умова передбачуваності не вимагає, щоб держава перерахувала у вичерпній формі, за найменуванням, конкретні злочини, які можуть призвести до перехоплення. Однак слід навести достатньо подробиць про характер злочинів, про які йде мова» [17]. Обґрунтовуючи порушення вимог ст. 8 Конвенції у справі «Йордакі та інші проти Молдови» Суд вказав, що «характер злочинів, які можуть давати підстави для ордеру на прослуховування, не є досить чітко визначеними у законодавстві», та звернув увагу на надмірне розширення спектру правопорушень, у провадженні щодо яких може бути застосовано настільки серйозне втручання у права людини: більше половини передбачених Кримінальним кодексом злочинів потрапляли у таку категорію [8, с. 157]. У законодавстві має бути чітко роз'яснено, до кого можуть застосовуватися заходи спостереження: загальні формулювання «особа, здатна володіти інформацією про кримінальний злочин» або «інші особи, причетні до кримінального злочину» без будь-яких уточнень щодо цих термінів, на думку Суду не відповідають цій вимозі [8, с.157-158; 17]. Порушення таємниці спілкування має здійснюватися виключно на підставі обґрунтованої підозри у тому, що особа може бути причетна до злочинної

діяльності, «зокрема, коли є фактичні свідчення для підозри цієї особи в плануванні, продовженні або вчиненні кримінальних діянь або інших дій, які можуть призвести до введення таємних заходів спостереження, як, наприклад, дії, що створюють загрозу національній безпеці», і орган, що видав дозвіл, має бути здатним підтвердити її наявність [17]. Обмеження у тривалості застосованого заходу означає чіткі часові межі, протягом яких може здійснюватися перехоплення, та наявність визначених підстав для продовження такого заходу і вимоги про його припинення якщо в ньому більше немає необхідності [18]. У самому дозволі на здійснення обмежувального заходу мають бути вказані строки його проведення, а також конкретну особу, до якої він застосовується, або конкретні приміщення, щодо яких дозволяється спостереження; «така ідентифікація може бути зроблена за допомогою імен, адрес, телефонних номерів або іншої відповідної інформації» [17]. Дані, отримані в результаті таємних заходів спостереження, «повинні бути опечатані і зберігатися в умовах, що виключають будь-який ризик несанкціонованого доступу», і можуть бути розкриті лише тим посадовим особам, які дійсно потребують їх для виконання своїх обов'язків і мають відповідний рівень допуску [17]. Інформація має розкриватися у обсязі, необхідному для цілей розслідування, і «там, де буде достатньо короткого викладу матеріалу, слід розкривати лише короткий зміст» [18]. У законі мають бути визначені умови та процедури для передачі перехоплених даних, що містять інформацію про злочин, до інших органів, та умови їх зберігання і використання як доказів під час судового розгляду [17]. Зібрана інформація, яка чітко не стосується справи, має бути негайно знищена. Інші дані повинні зберігатися протягом визначених законом строків з врахуванням потреб у їх використанні в кримінальному провадженні [17; 18]. Судовий контроль за дотриманням вимог закону має полягати не лише у наданні дозволу на втручання, а й у подальшому ознайомленню з ходом та результатами заходу [8, с. 158]. Також Суд наполягає на необхідності сповіщення особи про вжиті заходи втручання у її

спілкування щодо неї. У справі «Класс та інші проти Німеччини» Суд зазначив, що

«у випадку, коли держава запроваджує заходи таємного стеження, про що особи, які є об'єктом таких заходів, не сповіщаються і тому не мають змоги їх оскаржити, значна частина гарантій статті 8 виявляється нікчемною. У такій ситуації існує можливість поводження з особою у спосіб, який суперечить статті 8, або навіть можливість позбавлення її права, гарантованого цією статтею, без відповідного її сповіщення, а отже, без можливості для неї отримати засіб правового захисту чи в національному органі, чи в органах Конвенції» [21].

У справі «Сабо і Віші проти Угорщини» Суд вказав, що як тільки повідомлення може бути здійснено без загрози для мети обмеження, після завершення заходів спостереження інформація повинна бути надана особі задля можливості оскарження законності заходів [22].

Другий критерій правомірності обмеження таємниці спілкування передбачає, що «втручання має переслідувати законну мету, зазначену у ч. 2 ст. 8 Конвенції»: захист національної та громадської безпеки чи економічного добробуту країни, запобігання заворушенням чи злочинам, захист здоров'я чи моралі або захист прав і свобод інших осіб [23, с.145].

Необхідність у демократичному суспільстві означає, що «для втручання є нагальна суспільна потреба і втручання є пропорційним законній меті його здійснення». Кожна держава на власний розсуд визначає, що є необхідним за певних обставин. Питання того, чи вийшла держава за межі розсуду, досліджується Судом у кожному конкретному випадку, «в залежності від права, порушення якого стверджується, і серйозності втручання» [8, с. 94-95]. Наприклад, у справі «Dudchenko v. Russia» було встановлено, що національний суд обґрунтував надання дозволу на здійснення заходів прихованого контролю проти заявника протягом значного проміжку часу (180 днів) неможливістю отримати інформацію, необхідну для виявлення його незаконної діяльності шляхом відкритого розслідування, не пояснивши, як саме він прийшов до такого висновку. Отже, з позиції ЄСПЛ суд «не перевіряв, чи існує «обґрунтована підозра» проти заявника, і не

застосував тести «необхідності в демократичному суспільстві» та «пропорційності» [20].

Особлива охорона має надаватися спілкуванню адвоката з клієнтом. У справі «Michaud v. France» Суд підкреслив, що листування між адвокатом і клієнтом незалежно від його характеру (в тому числі й професійне), «має щодо конфіденційності привілейоване становище».

«...адвокати здійснюють у демократичному суспільстві основоположну місію – захист обвинувачених і підсудних. Зрозуміло, адвокат не може належно здійснювати цю основоположну місію, якщо він не може гарантувати тим, кого захищає, що їхнє спілкування залишиться конфіденційним. Тут йдеться про довірчі стосунки між ними, необхідні для здійснення цієї місії. Від цього залежить також, хоч і непрямо, але неухильно, повага до права підсудного на справедливий судовий розгляд, особливо щодо права кожного «обвинуваченого» не свідчити проти себе» [24].

ЄСПЛ розробив гарантії, які повинні бути встановлені в законодавстві для забезпечення захисту від зловживань при втручанні у спілкування адвоката з клієнтом. В законі «необхідно чітко визначити сферу юридичного професійного привілею та вказати, яким чином, за яких умов і через кого слід проводити розмежування між привілейованими та непривілейованими матеріалами»; при цьому обов'язково має бути забезпечений нагляд з боку незалежного судді [20]. Також окремо мають бути передбачені процедури поводження з отриманими внаслідок здійснення прихованого контролю матеріалами, що підпадають під поняття юридичного професійного привілею: процедура подання звітності незалежному наглядовому органу щодо розгляду таких випадків, умови, за яких вони можуть бути збережені та використані у кримінальному провадженні, порядок безпечного зберігання, розповсюдження таких матеріалів та їх подальшого знищення [20]. У справі «Dudchenko v. Russia» Суд встановив невідповідність російського законодавства вимозі якості закону, оскільки хоча воно й проголошувало захист професійної таємниці, проте «не містило жодних конкретних гарантій, що застосовуються до прослуховування повідомлень адвокатів; адвокати підпадають під дію тих самих правових положень про перехоплення

комунікацій, як і будь-хто інший»; закон не передбачає будь-яких положень яких слід дотримуватися у випадку коли при здійсненні заходів спостереження випадково перехоплюється розмова підозрюваного із захисником [20].

Гарантії таємниці спілкування передбачені й для осіб, які утримуються під вартою або перебувають в установах виконання покарань за злочини. Хоча Суд враховує особливе становище цих осіб, зумовлене посиленнями безпековими заходами щодо них, та не заперечує допустимості здійснення втручання у листування ув'язнених, проте це не означає, що держави наділені необмеженим розсудом у цій сфері [25]. До обмежувальних заходів так само ставляться вимоги «згідно з законом», «відповідність законній меті» та «необхідність у демократичному суспільстві». У справі «Calogero Diana v. Italy» Суд встановив, що перегляд кореспонденції заявника тюремною адміністрацією не здійснювався згідно з законом, оскільки законодавство надавало владі надто широкі дискреційні повноваження; в ньому визначалася лише категорія осіб, чия кореспонденція може бути піддана огляду, та компетентний суд; поза увагою були залишені питання тривалості заходу чи його підстав [26].

У справі «Беляєв та Дігтяр проти України» Суд також дійшов висновку про те, що тодішнє законодавство не надавало достатніх гарантій захисту листування ув'язнених від свавільного втручання. Зокрема, воно дозволяло переглядати працівникам установ виконання покарань усі листи, що відсилалися ув'язненими особами, за винятком листів Уповноваженому Верховної Ради з прав людини або прокурору, та містило інші недоліки:

«Законодавство не проводило будь-якого розмежування щодо інших категорій осіб, з якими могли листуватися ув'язнені - такими як, наприклад, правоохоронні та інші державні органи, конвенційні та інші міжнародні органи, родичі, захисник та ін. Законодавство не конкретизувало спосіб здійснення перегляду кореспонденції. Зокрема, воно не передбачало будь-якої участі ув'язнених осіб на будь-якій стадії процесу перегляду листів або їхнього залучення до нього. Воно також не визначало, чи мала ув'язнена особа право на інформування її про будь-які зміни, внесені у зміст її вихідної кореспонденції. Більш того,

перегляд був автоматичним, не був обмежений у строках та не вимагав будь-якого вмотивованого рішення, яке б надавало підстави для заходів з перегляду кореспонденції та/або встановлювало строки їхнього виконання. Насамкінець, не існувало конкретного засобу юридичного захисту, який надавав би ув'язненій особі змогу оскаржити вищезазначений захід та отримати адекватне відшкодування» [27].

У справі «Довженко проти України» Суд встановив, що «національне законодавство не визначало з достатньою чіткістю межі та способи здійснення дискреційних повноважень державних органів щодо надання дозволу на відправлення кореспонденції затриманих». Заявник, який перебував під вартою, для відправлення кореспонденції мав отримати дозвіл, проте більше шести місяців його клопотання про надання дозволу ігнорувалося компетентним органом, оскільки законодавство не зобов'язувало орган приймати таке рішення, наводити причини для прийняття рішення або надавати копію рішення, й у заявника не було правових засобів для оскарження дії чи бездіяльності відповідного органу [28].

У справі «Jankauskas v. Lithuania» заявник скаржився на те, що під час його перебування у слідчому ізоляторі абсолютно вся його кореспонденція підлягала перлюстрації за його відсутності. Суд визнав, що втручання у спілкування заявника мало правову підставу, однак не відповідало вимозі необхідності у демократичному суспільстві. Надане Урядом пояснення, що полягало у побоюванні втечі заявника або впливу на суд, могло мати значення для виправдання його тримання під вартою або навіть певної форми втручання в частину його кореспонденції, наприклад, перевірку певної кореспонденції неюридичного характеру або його листування з особами небезпечного характеру. Однак саме по собі це занепокоєння не могло бути достатнім для надання повноважень адміністрації здійснювати невибірково, регулярну перевірку всієї кореспонденції заявника, особливо тієї, яка адресувалася його адвокату (конфіденційність якої повинна поважатися згідно з Конвенцією), чи органам державної влади, у якій він міг скаржитися на умови тримання під вартою або подавати інші заяви, не пов'язані з кримінальною справою проти нього [29].

1.2. Теоретико-правові аспекти таємниці спілкування в Україні.

Право людини на таємницю її розмов, листів та інших видів комунікацій отримало особливий захист в українському законодавстві. Про це свідчить перш за все його наявність у переліку основних прав, охоронюваних на конституційному рівні: відповідно до ст. 31 Конституції України кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції [1]. З тлумачення конституційної норми випливає, що вона має універсальний характер: її дія поширюється як на громадян України, так і на іноземців та осіб без громадянства [30, с. 14]. На це вказують і положення ст. 3 Закону України «Про правовий статус іноземців та осіб без громадянства», згідно з якою 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; іноземці та особи без громадянства, які перебувають під юрисдикцією України, незалежно від законності їх перебування, мають право на визнання їх правосуб'єктності та основних прав і свобод людини [31]. Конституційні гарантії права на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції передбачають «заборону втручання в здійснення цього права з боку держави, її органів, посадових і будь-яких інших осіб та наявність правових механізмів і гарантій захисту від будь-яких посягань» [30, с. 14]. Проте воно не належить до абсолютних. Враховуючи суспільний інтерес у боротьбі зі злочинністю і водночас необхідність забезпечення високих стандартів захисту прав людини й уникнення зловживань, у Конституції України було передбачено можливість встановлення обмежень у реалізації права, однак винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинам чи з'ясувати

істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо.

Правові положення щодо реалізації та захисту таємниці листування, телефонних розмов, телеграфної та іншої кореспонденції закріплені й у інших нормативно-правових актах. Так, відповідно до ст. 306 Цивільного кодексу України фізична особа має право на таємницю листування, телеграм, телефонних розмов, телеграфних повідомлень та інших видів кореспонденції. У цій же статті врегульовано режим доступу до приватної кореспонденції. Листи, телеграми тощо є власністю адресата. 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. У разі смерті фізичної особи, яка направила кореспонденцію, і адресата використання кореспонденції, зокрема шляхом її опублікування, можливе лише за згодою фізичних осіб, визначених ч. 4 ст. 303 цього Кодексу. У разі смерті фізичної особи, яка направила кореспонденцію, і адресата, а також у разі смерті фізичних осіб, визначених ч. 4 ст. 303 цього Кодексу, кореспонденція, яка має наукову, художню, історичну цінність, може бути опублікована в порядку, встановленому законом. Кореспонденція, яка стосується фізичної особи, може бути долучена до судової справи лише у разі, якщо в ній містяться докази, що мають значення для вирішення справи. Інформація, яка міститься в такій кореспонденції, не підлягає розголошенню. Порушення таємниці кореспонденції може бути дозволено судом у випадках, встановлених законом, з метою запобігання кримінальному правопорушенню чи під час кримінального провадження, якщо іншими способами одержати інформацію неможливо [32]. За незаконне втручання в таємницю листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер передбачена кримінальна відповідальність за ст. 163 Кримінального кодексу України [33].

У ст. 14 Кримінального процесуального кодексу України запроваджено дещо інший підхід до розуміння сутності конституційного права на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції. Даною нормою вводиться поняття таємниці спілкування як однієї із загальних засад кримінального провадження, згідно з якою кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції, інших форм спілкування. Таким чином у Кримінальному процесуальному кодексі України листування, телефонні розмови, телеграфну та іншу кореспонденцію віднесено до форм спілкування, при цьому правова охорона поширюється й на інші форми, на відміну від Конституції України. Також у Кримінальному процесуальному кодексі України більш конкретизовані підстави для порушення права на таємницю 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. Інформація, отримана внаслідок втручання у спілкування, не може бути використана інакше як для вирішення завдань кримінального провадження [34].

Задля забезпечення належного правозастосування під час кримінального провадження необхідно з'ясувати, що саме слід відносити до об'єктів захисту таємницею спілкування. Потребують роз'яснення поняття «листування», «телефонні розмови», «телеграфна кореспонденція», «інші види кореспонденції», а також питання, що охоплюється поняттям «кореспонденція» та «інші форми спілкування». Отже, спробуємо проаналізувати основні підходи до їх визначення.

Перш за все потрібно зазначити, що в українському законодавстві відсутнє визначення поняття «кореспонденція». Згадується лише про письмову кореспонденцію у ст. 1 Закону України «Про поштовий зв'язок», відповідно до якої до письмової кореспонденції належать окремі різновиди

поштових відправлень, такі як:

- прості та рекомендовані листи. Листом є поштове відправлення у вигляді поштового конверта з вкладенням письмового повідомлення або документа, розміри і масу якого встановлено відповідно до законодавства України;
- поштові картки – поштові відправлення у вигляді стандартного бланка, що містять відкрите письмове повідомлення;
- бандеролі – поштові відправлення з друкованими виданнями, діловими паперами, предметами культурно-побутового та іншого призначення, розміри, маса і порядок упакування яких встановлені відповідно до законодавства України;
- секограми – письмові повідомлення, написані секографічним способом, друковані видання для сліпих, кліше із знаками секографії, що подаються у відкритому вигляді, а також звукові записи та спеціальний папір, призначені виключно для сліпих, за умови, що вони відправляються офіційно визнаними установами для сліпих або на їх адресу;
- дрібні пакети – міжнародні рекомендовані поштові відправлення із зразками товарів, дрібними предметами подарункового та іншого характеру, розміри, маса і порядок упакування яких встановлені відповідно до законодавства України [35].

Якщо звернутися за роз'ясненням до Словника української мови, то отримаємо декілька тлумачень: листування між окремими особами або установами; сукупність поштових відправлень (листів, телеграм тощо); окреме поштове відправлення (лист, телеграма тощо); замітка, допис, повідомлення, надіслані кореспондентом (у 2 знач.) до газети, журналу тощо [36]. Тобто за Словником поняттям «кореспонденція» не охоплюються телефонні розмови, інші сучасні види зв'язку. У наукових колах натомість пропонується розширене тлумачення. Наприклад, В.В. Назаров зазначає, що

«поняттям «кореспонденція» охоплюється не лише письмова кореспонденція (прості та рекомендовані листи, поштові

картки, бандеролі, секограми, а також дрібні пакети, мішки “М”), але й усі інші види кореспонденції (телеграми, телефонні розмови, телеграфні повідомлення, повідомлення електронною поштою, пейджером, SMS та MMS-повідомлення тощо» [37, с. 119].

М.Є. Шумило та В.С. Рудей, посилаючись на практику ЄСПЛ, відстоюють позицію, що «термін «кореспонденція» охоплює всі перелічені в ст. 31 Конституції України способи передачі інформації. Поняття «листування», «телефонні розмови», та «телеграфні повідомлення» у співвідношенні з поняттям «кореспонденція» є конкретизуючими». Крім того, науковці наголошують на тому, що формулювання «інші види кореспонденції» у законодавчих нормах вказує на невичерпність форм комунікації між людьми, що підпадають під правову охорону, і дозволяє враховувати нові засоби зв'язку як різновиди кореспонденції. На їх думку, до інших видів кореспонденції слід відносити

«будь-яку кореспонденцію, що не є листуванням, телефонними розмовами і телеграфними повідомленнями та передається з використанням радіозв'язку, електричного, радіорелейного, радіотелефонного, височастотного і космічного зв'язку (технічні можливості яких дозволяють передавати на відстані інформацію проводовими лініями, через ефір або в комбінації усну мову людини) та відправлена будь-яким іншим способом».

Як приклади вчені наводять електронні поштові повідомлення (e-mail), пейджинг, повідомлення, що надсилаються за допомогою ICQ або під час спілкування в чатах, телефонограми, телетайп, факсиміле, телекс, SMS та MMS повідомлення, голосову пошту [30, с. 23-26].

Д.Ю. Кондратов пропонує більш узагальнене визначення кореспонденції, зводячи її до форм спілкування, яке здійснюється за допомогою будь-яких засобів зв'язку:

«інформація, що становить таємницю кореспонденції, повинна міститися в листуванні, телефонних розмовах, телеграфних або інших повідомленнях осіб. Інакше кажучи, обов'язковою ознакою такої інформації є спосіб її передачі – вона вже була передана чи лише передається будь-якими засобами зв'язку (поштою, телефоном, телеграфом, за допомогою комп'ютера тощо)» [38, с. 102].

Л.В. Ємчук у своєму дисертаційному дослідженні також досить широко тлумачить поняття «кореспонденція», вказуючи, 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» [39, с. 56-57].

Незважаючи на термінологічні прогалини в українському законодавстві, в українських судах виробилася правозастосовна практика, що враховує як кореспонденцію спілкування за допомогою сучасних різноманітних засобів зв'язку. Наприклад, вироком Першотравневого районного суду м. Чернівці від 29 серпня 2008 р. у справі № 1-235/2008 громадянина ОСОБА_1 було засуджено за ст. 163 Кримінального кодексу України за порушення таємниці кореспонденції, що передається через комп'ютер, яке виразилося у ознайомленні зі змістом розмов потерпілих з друзями та знайомими, що здійснювалися за допомогою комп'ютерних програм `ja3c.exe`, `miranda32.exe` і `ICQ.exe` (програм обміну миттєвих текстових повідомлень), а також сайту «ОДНОКЛАСНИКИ», яке було вчинене за допомогою шкідливого програмного засобу «Trojan-Spy.Win32.Ardamax.n», що передавав відповідну інформацію до електронної скриньки правопорушника [40]. Франківський районний суд м. Львова у вироку від 11.10.2021 р. у справі № 465/5121/20 кваліфікував як порушення таємниці кореспонденції, що передається через комп'ютер, незаконне ознайомлення з кореспонденцією потерпілої, яка містилася у її обліковому записі в комп'ютерній мережі «i.ua», та становила її особисту таємницю [41].

Термін «листування» згідно зі Словником української мови має такі значення: дія за значенням листуватися (обмінюватися листами, писати один одному листи); зібрання листів, написаних і одержаних ким-небудь [42]. Серед науковців висловлювалися різні думки стосовно роз'яснення поняття «листування» в контексті кримінального процесу. З точки зору С.Я. Лихової, М.І. Мельника і М.І. Хавронюка «листування – це приватна кореспонденція,

що передається поштовим зв'язком (листи, телеграми, інші письмові відправлення, бандеролі тощо) або електронною поштою (через комп'ютер)». На думку В.М. Тертишника листуванням є різні види поштових відправлень (листи, телеграми, посилки, бандеролі тощо) [30, с. 18-19]. І.І. Савляк також визначає листування як «обмін поштовими відправленнями, що передаються поштовим зв'язком» [43, с. 26]. В.В. Сташис і В.Я. Тацій пропонують наступну дефініцію: «будь-які види кореспонденції: листи, посилки, бандеролі тощо, тобто ті послуги, що надаються установами зв'язку громадянам або юридичним особам» [30, с. 19]. На нашу думку, запропоновані варіанти є надто розширеними з огляду на наступне. Відповідно до ст. 6 Закону України «Про поштовий зв'язок» Конституцією та законами України гарантується таємниця поштових відправлень, у тому числі листування та іншої письмової кореспонденції, електронних повідомлень, що пересилаються (передаються) засобами зв'язку. З цього випливає, що поняттям «листування» охоплюються не всі види поштових відправлень, воно виокремлене як один із різновидів письмової кореспонденції. Тому найбільш прийнятною з точки зору відповідності чинному законодавству виглядає позиція М.Є. Шумило та В.С. Рудей, які надають наближене до словникового визначення листування: «написання одне одному листів та обмін ними», тобто листуванням є саме прості та рекомендовані листи, що передаються за допомогою засобів поштового зв'язку [30, с. 19].

Залишається недостатньо визначеним, чи охоплюються поняттям «листування» повідомлення, відправлені за допомогою мережі Інтернет (приміром, через електронну пошту або соціальні мережі). У згаданій вище законодавчій нормі поряд із таємницею листування окремо передбачена таємниця електронних повідомлень, що пересилаються (передаються) засобами зв'язку. Проте слід зауважити, що цим Законом визначаються правові основи діяльності у сфері надання послуг поштового зв'язку. Відповідно до п. 20 Правил надання послуг поштового зв'язку передбачено

послуги з пересилання відправлень електронної пошти, що надаються операторами поштового зв'язку за наявності відповідних технічних засобів. Відправленням електронної пошти є повідомлення, що подається для пересилання на паперовому або електронному носії інформації, передається з використанням інформаційно-комунікаційних технологій і доставляється/вручається одержувачу відтвореним на паперовому або електронному носії інформації. Відправлення електронної пошти, відтворене на паперовому носії інформації, доставляється/вручається одержувачу упакованим як письмова кореспонденція [44]. Тобто, під електронними повідомленнями в Законі маються на увазі лише ті, які пересилаються за допомогою операторів поштового зв'язку. У судовій практиці простежується підхід, за яким електронні повідомлення, що надсилаються користувачами мережі Інтернет за допомогою різних програмних засобів без посередництва операторів поштового зв'язку визначаються як особисте листування. Наприклад, Луцьким міськрайонним судом Волинської області у вироку від 17.02.2015 р. у справі № 161/1717/15-к було кваліфіковано як порушення таємниці листування, що передається через комп'ютер, незаконне отримання доступу до листів, які зберігалися в електронній поштовій скриньці потерпілого, та ознайомлення з їх змістом [45]. До такого ж висновку прийшов Рівненський міський суд Рівненської області у вироку від 13.09.2019 р. у справі № 569/12334/19, яка стосувалася несанкціонованого втручання в роботу електронного поштового серверу без згоди власника, внаслідок чого правопорушник отримав змогу ознайомитися з електронним листуванням потерпілої [46]. Відтак, можемо зробити висновок, що поняття «листування» включає в себе як поштові листи, так і електронне листування.

Телефонними розмовами є «розмови між особами, що відбуваються за допомогою будь-якого телефонного зв'язку, що здійснюється за допомогою проводових чи електромагнітних систем тощо» [30, с. 19]. Норми, що регламентують захист інформації, що становить таємницю телефонних розмов, містяться у Правилах надання та отримання телекомунікаційних

послуг. У відповідності до пп. 22 п. 39 Правил оператори, провайдери зобов'язані вживати відповідно до законодавства заходів із забезпечення таємниці телефонних розмов, іншої інформації, що передається телекомунікаційними мережами, а також із захисту відомостей про споживача, отриманих під час укладання договору, надані чи замовлені ним послуги, іншої інформації з обмеженим доступом. Як зазначено в п. 42 Правил, оператор, провайдер повинен відповідно до законодавства забезпечувати збереження відомостей про абонента, отриманих під час укладання договору, а також про надання послуг, у тому числі факт їх отримання, обсяг, зміст, маршрути передачі інформації тощо, і несе відповідальність за їх схоронність [47].

Іншим нормативно-правовим актом, що встановлює детальні вимоги стосовно захисту інформації, отриманої в ході надання телекомунікаційних послуг (інша назва – електронні комунікаційні послуги) є Закон України «Про електронні комунікації». Згідно зі ст. 119 вказаного Закону постачальники електронних комунікаційних послуг повинні забезпечувати і нести відповідальність за схоронність даних щодо кінцевого користувача, отриманих при укладенні договору про надання електронних комунікаційних послуг та наданні електронних комунікаційних послуг, 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, до яких відносяться будь-які дані, що обробляються постачальником електронних комунікаційних послуг при наданні послуг електронних комунікацій, у тому числі щодо розташування

термінального обладнання. Ця вимога не поширюється на випадок передачі даних про місцезнаходження абонента, що здійснює виклик до служби екстреної допомоги за номером 112;

б) 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.

Відповідно до ч. 1 ст. 121 Закону України «Про електронні комунікації» доступ до вказаної інформації може здійснюватися виключно на підставі рішення суду, слідчого судді у випадках та порядку, передбачених законом [48].

З наведеного вище можемо зробити висновок, що таємницею телефонних розмов захищаються не лише зміст спілкування між особами, а й відомості щодо факту проведення телефонної розмови, дані, які дозволяють ідентифікувати абонентів, їх місцезнаходження тощо. Зокрема, у судовій практиці як порушення таємниці телефонних розмов кваліфікується незаконне збирання та передача відомостей про зв'язок абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту (вихідних та вхідних з'єднань, SMS, MMS тощо), маршрутів передавання, ідентифікаційних ознак кінцевого обладнання телекомунікацій (абонентського номеру SIM-карти, IMEI, MAC-адрес, IP-адрес тощо), яке перебувало у зоні дії певних базових станцій у певний час [49].

Телеграфна кореспонденція визначається як «повідомлення, що відправляються телеграфом – системою зв'язку для передачі повідомлень на відстані за допомогою електричної енергії дротами або через радіо» [с. 23, 30]. Надання послуг телеграфного зв'язку врегульовано наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 22.04.2014 року № 195, а також Правилами надання та отримання телекомунікаційних послуг [50]. Однак з 01.03.2018 року ПАТ «Укртелеком», яке надавало послуги телеграфного зв'язку населенню, припинило прийом та відправку телеграм у зв'язку з нерентабельністю,

відсутністю підтримки старого обладнання з боку виробників та низьким попитом [51]. Через це законодавчі положення щодо захисту таємниці телеграфної кореспонденції видаються неактуальними, бо фактично телеграфний зв'язок більше не використовується для передачі приватних повідомлень.

Під іншими формами спілкування науковці пропонують вважати «безпосереднє спілкування осіб (не опосередковане технічними чи іншими засобами), спілкування за допомогою телекомунікаційних засобів (електронної пошти, ICQ тощо)» або ж повідомлення, що здійснюються за допомогою сучасних форм зв'язку – телефаксом, пейджингом, за допомогою інтернет-месенджерів, факсиміле, IP-телефонії та іншими способами [52, с. 41,]. Потрібно наголосити, що в ч. 3 ст. 258 Кримінального процесуального кодексу України спілкування визначається як передання інформації у будь-якій формі від однієї особи до іншої безпосередньо або за допомогою засобів зв'язку будь-якого типу. В даній частині роботи нами було з'ясовано, що поняття «кореспонденція» як у теоретичних дослідженнях, так і у судовій практиці охоплює практично будь-які форми спілкування, що здійснюються за допомогою засобів зв'язку (поштового, телефонного, електронного тощо). Тому на нашу думку, під іншими формами спілкування слід розуміти саме безпосереднє спілкування.

Дослідивши термінологічні засади таємниці спілкування, можемо підсумувати, що в українському законодавстві з недостатньою чіткістю визначено її обсяг та наявна неузгодженість понятійного апарату. На нормативному рівні відсутнє визначення понять «кореспонденція», «листування», «телефонні розмови», «телеграфна кореспонденція», «інші види кореспонденції». На відміну від Кримінального процесуального кодексу України, у Конституції України та інших правових актах не гарантується захист інших форм спілкування. З нашої точки зору для забезпечення дотримання принципу правової визначеності необхідно внести зміни до законодавчих актів, а саме роз'яснити зміст кореспонденції та її різновидів з

врахуванням наукових напрацювань, та закріпити гарантії інших форм спілкування. Або можна застосувати більш узагальнений підхід і, взявши за основу дефініцію з ч. 3 ст. 258 Кримінального процесуального кодексу України, закріпити гарантії таємниці спілкування, що передбачають захист інформації, що передається у будь-якій формі від однієї особи до іншої безпосередньо або за допомогою засобів зв'язку будь-якого типу.

Варто зауважити, що таємницею спілкування захищається приватне спілкування. Згідно з ч. 3 ст. 258 Кримінального процесуального кодексу України 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. Під фізичними умовами приватності розуміють «місце, час і форма здійснення спілкування, обрані його учасниками; заходи збереження інформації та її захисту від втручання інших осіб, які вживаються учасниками спілкування (кодування інформації тощо)». До юридичних умов відносять нормативно закріплені гарантії невтручання у таємницю спілкування, а також у разі здійснення спілкування за допомогою засобів зв'язку – «наявність угоди між учасником спілкування, який використовує послуги такого зв'язку, та юридичною особою, яка їх надає», в якій закріплений обов'язок постачальника послуги забезпечувати конфіденційність даних [53, с. 168].

Науковці висловлюють різні думки щодо обсягу приватності спілкування. О.А. Білічак зазначає, що приватне спілкування охоплює «особисті, неофіційні зв'язки, не ділового характеру, що існують поза державною службою», тому не становитимуть втручання у приватне спілкування заходи спостереження за службовцями органів державної влади та місцевого самоврядування [54, с. 100]. Така позиція базується на рішенні Конституційного Суду України від 20.01.2012 року № 2-рп/2012, у якому особисте життя особи розтлумачено як «її поведінка у сфері особистісних, сімейних, побутових, інтимних, товариських, професійних, ділових та інших

стосунків поза межами суспільної діяльності, яка здійснюється, зокрема, під час виконання особою функцій держави або органів місцевого самоврядування» [55]. Натомість А.Б. Ткачик наголошує, що виходячи з практики ЄСПЛ та визначення приватного спілкування за Кримінальним процесуальним кодексом України, «приватність спілкування повинна забезпечуватися у всіх випадках коли особи вважають, що їх спілкування не може бути відоме стороннім особам» [52, с. 36]. Ми погоджуємося з тим, що не можна поширити поняття «приватності» на робочу кореспонденцію у органах влади та приватних компаніях. Проте слід зважати на висловлені ЄСПЛ зауваження щодо випадків, коли особа може мати розумні очікування щодо приватності її спілкування на робочому місці. Працівник має бути чітко проінформований, чи допускається використання робочих сервісів у особистих цілях, про можливість спостереження, його підстави, характер і наслідки.

Національна судова практика з даного питання перебуває у стані формування. Наявна лише одна справа за № 332/1189/18, яка стосується втручання у спілкування на робочому місці. Суди першої та апеляційної інстанції дійшли висновку про відсутність порушення таємниці спілкування, пославшись на те, що «втручання здійснювалось не в особисте листування осіб і не в їх приватні електронні пошти, а щодо корпоративної пошти, яка є власністю підприємства і вся службова інформація в листуванні не є приватною, про що всі працівники підприємства попереджені та про що надали письмову згоду». Однак Верховний Суд у постанові від 23.11.2021 року направив справу на новий розгляд у суді апеляційної інстанції у зв'язку з неврахуванням показань свідків, що вказували на відсутність дозволу на негласне отримання інформації з їх робочих комп'ютерів та електронних скриньок, а також на втручання у їх особисте листування, що здійснювалося з робочих електронних скриньок [56].

У законодавстві окреслено сферу професійного привілею, який надає вищий ступінь конфіденційності спілкуванню. Відповідно до ч. 5 ст. 258

КПК України втручання у приватне спілкування захисника, священнослужителя з підозрюваним, обвинуваченим, засудженим, виправданим заборонене. Хоча у даній нормі не згадуються інші учасники кримінального провадження, проте за змістом інших положень закону можемо зазначити, що особливі гарантії таємниці спілкування з адвокатом поширюються й на них. Так, згідно зі ст. 161 КПК України заборонено доступ до речей і документів, що являють собою листування або інші форми обміну інформацією між захисником та його клієнтом або будь-якою особою, яка представляє його клієнта, у зв'язку з наданням правової допомоги, та об'єкти, які додані до такого листування або інших форм обміну інформацією. В п. 9 ч. 1 ст. 23 Закону України «Про адвокатуру та адвокатську діяльність» зазначено, що забороняється втручання у приватне спілкування адвоката з клієнтом [57]. Стосовно спілкування із священнослужителем варто уточнити, що під ним мається на увазі його спілкування як представника церкви чи церковної конфесії з приводу задоволення релігійних потреб з підозрюваним, обвинуваченим, засудженим чи виправданим, який ідентифікує себе як віруючий, є парафіянином даної церкви чи церковної конфесії [58, с. 296]. Священнослужитель повинен мати легітимний статус, що підтверджується його належністю до релігійної організації, яка зареєстрована в установленому законом порядку [43, с. 115]. Співставивши аналізовані правові норми зі стандартами ЄСПЛ, нами було виявлено, що істотним недоліком законодавчих положень є відсутність визначеного порядку, якого слід дотримуватися в разі випадкового перехоплення спілкування особи з захисником чи священнослужителем в ході здійснення втручання у приватне спілкування під час досудового розслідування. Ми підтримуємо позицію тих науковців, які наголошують на необхідності доповнення ст. 258 КПК України вказівкою на неможливість використання отриманих в ході такого втручання відомостей про спілкування особи із захисником чи священнослужителем та їх негайне знищення [43, с. 115].

Правове регулювання таємниці спілкування осіб, які знаходяться в установах попереднього ув'язнення або виконання покарань, має деякі особливості у порівнянні з іншими категоріями осіб. Відповідно до ст. 63 Конституції України засуджений користується всіма правами людини і громадянина, за винятком обмежень, які визначені законом і встановлені вироком суду. Істотні обмеження таємниці спілкування встановлені для засуджених до позбавлення волі. Згідно зі ст. 113 Кримінально-виконавчого кодексу засудженим дозволяється одержувати і відправляти листи і телеграми за свій рахунок без обмеження їх кількості. Листування між перебуваючими в місцях позбавлення волі засудженими, які не є родичами, допускається тільки з дозволу адміністрації колонії. Кореспонденція, яку одержують і надсилають засуджені до відбування покарання у виправних колоніях мінімального рівня безпеки із загальними умовами тримання, середнього та максимального рівня безпеки, підлягає перегляду, за винятком тієї, що адресується Уповноваженому Верховної Ради України з прав людини, Європейському суду з прав людини, а також іншим відповідним органам міжнародних організацій, членом або учасником яких є Україна, уповноваженим особам таких міжнародних організацій, до суду та прокуророві. Кореспонденція, яку засуджені одержують від зазначених органів та осіб, перегляду не підлягає. Також не підлягає перегляду кореспонденція засудженого із захисником у кримінальному провадженні, що здійснює свої повноваження відповідно до КПК України [59]. Відповідно до Правил внутрішнього розпорядку установ виконання покарань перегляд кореспонденції може здійснюватися лише з письмового дозволу начальника установи виконання покарань на підставі рапорту (клопотання) працівника оперативного підрозділу установи з обов'язковим встановленням строку перегляду кореспонденції [60]. Можемо відзначити, що у оновленому законодавстві були враховані зауваження ЄСПЛ щодо необхідності забезпечення правових гарантій захисту таємниці кореспонденції засуджених.

Значно гіршою виглядає ситуація з забезпеченням таємниці спілкування осіб, що перебувають під вартою. Їх вина у вчиненні правопорушення ще не доведена обвинувальним вироком суду, а тому відповідно до ст. 17 КПК України поводження з такими особами має відповідати поводженню з невинуватою особою. Крім того, обмеження права на таємницю спілкування щодо такої категорії осіб не відповідає ст. 31 Конституції України. Проте у ст. 13 Закону України «Про попереднє ув'язнення» все ще передбачена вимога отримання письмового дозволу особи або органу, які здійснюють кримінальне провадження, на листування з родичами та іншими громадянами, а також підприємствами, установами, організаціями. При цьому не визначена процедура надання дозволу: строків розгляду клопотання, підстав для відмови у його задоволенні, а також порядок оскарження дії або бездіяльності компетентного органу, на чому наголошував ЄСПЛ у справі «Довженко проти України». Вся кореспонденція осіб, взятих під варту, підлягає автоматичному перегляду, за винятком кореспонденції з Уповноваженим Верховної Ради України з прав людини, Європейським судом з прав людини, а також іншими відповідними органами міжнародних організацій, членом або учасником яких є Україна, уповноваженими особами таких міжнародних організацій, прокурором та захисником [61]. Ми вважаємо, що положення Закону України «Про попереднє ув'язнення» потрібно привести у відповідність до Конституції України та стандартів ЄСПЛ та забезпечити можливість реалізації особами, що перебувають під вартою, права на таємницю спілкування.

Таємниця спілкування як складова права на повагу до приватного життя закріплена в низці ключових міжнародно-правових договорів, які проголошують основні права людини. Найбільш повно її зміст розкрито у прецедентній практиці Європейського Суду з прав людини. Встановлюючи у

кожній конкретній справі наявність або відсутність порушення права на таємницю кореспонденції, Суд застосовує декілька тестів:

- тест на належність предмета спору до сфери дії ст. 8 Конвенції про захист прав людини і основоположних свобод, а саме, чи відбулося втручання у приватну кореспонденцію. Поняття «кореспонденція» не є сталим і постійно доповнюється новим змістом, враховуючи всі сучасні засоби зв'язку. Обсяг приватності не обмежується виключно колом дружніх особистих зв'язків та може охоплювати й професійну активність особи, в залежності від того, чи мала вона розумні очікування приватності її комунікацій;

- тест «згідно з законом», що передбачає наявність закону, що регулює питання втручання у приватне спілкування, і має відповідати вимогам доступності та якості;

- тест «законної мети», який означає перевірку здійснення заходів відповідно до цілей, вказаних у ст. 8 Конвенції;

- тест «необхідності у демократичному суспільстві», яким встановлюється, чи було пропорційним здійснене втручання у спілкування меті, яку воно переслідувало.

Судом передбачена особлива охорона спілкування окремих категорій осіб. Не заперечуючи проти допустимості втручання у спілкування адвоката з клієнтом, ЄСПЛ водночас вимагає забезпечення належних гарантій захисту від свавілля, які мають з достатньою чіткістю визначати межі втручання у спілкування адвоката. Питання обмеження кореспонденції засуджених Суд залишає на розсуд держав, при цьому наголошуючи на неприпустимості повної заборони спілкування ув'язнених із зовнішнім світом, та необхідності забезпечити конфіденційність перемовин з адвокатом, органами державної влади, ЄСПЛ та іншими міжнародними організаціями.

В українському законодавстві були відображені основні міжнародні стандарти захисту таємниці спілкування, проте воно не позбавлене недоліків. Наявна термінологічна неузгодженість й недостатня визначеність щодо

понять «кореспонденція», «листування», «телефонні розмови», «телеграфна кореспонденція», «інша кореспонденція», «інші форми спілкування». Також закон містить недостатньо гарантій захисту спілкування особи з захисником та священнослужителем. Законодавчі положення щодо кореспонденції осіб, які тримаються під вартою не відповідають практиці ЄСПЛ та суперечать Конституції України, оскільки встановлюють непропорційне втручання у їх конституційне право на таємницю спілкування й не відповідають принципу правової визначеності. Отже, правові норми щодо таємниці спілкування потребують вдосконалення з боку законодавця.

РОЗДІЛ 2

ОХОРОНА ТАЄМНИЦІ СПІЛКУВАННЯ ПІД ЧАС КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ

2.1. Охорона таємниці спілкування під час здійснення тимчасового доступу до речей і документів.

Серед заходів забезпечення кримінального провадження, передбачених КПК України, особливий інтерес у контексті магістерського дослідження становить тимчасовий доступ до речей і документів. Відповідно до ст. 159 КПК України 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). При цьому кодексом виокремлена особлива категорія речей і документів, що містять охоронювану законом таємницю, доступ до яких можливий лише у разі, якщо обставини, які передбачається довести за допомогою цих речей і документів, неможливо довести іншими способами. До речей і документів, що містять охоронювану законом таємницю, згідно з переліком, наведеним у ст. 162 КПК України, належать, зокрема, особисте листування особи та інші записи особистого характеру, а також 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. Однак за змістом ст. 14 і ст. 258 КПК України втручання в таємницю спілкування можливе лише шляхом проведення негласних слідчих (розшукових) дій. У зв'язку з цим постає питання щодо обсягу відомостей, які можуть бути отримані в ході здійснення тимчасового доступу до таких речей і документів, та відповідно його розмежування з НСРД, тому слід детально проаналізувати особливості проведення даної процесуальної дії.

Тимчасовий доступ до речей і документів здійснюється на підставі

ухвали слідчого судді, суду. Для цього сторони кримінального провадження мають звернутися з відповідним клопотанням до слідчого судді, суду першої інстанції (слідчий має право звернутися з клопотанням за погодженням з прокурором). Згідно зі ст. 160 КПК України у клопотанні, окрім загальних відомостей про кримінальне правопорушення, у зв'язку з яким подається клопотання (короткий виклад обставин про кримінальне правопорушення, правова кваліфікація кримінального правопорушення із зазначенням статті (частини статті) закону України про кримінальну відповідальність) повинні бути зазначені речі та документи, тимчасовий доступ до яких планується отримати. На практиці виникають складнощі при визначенні речей і документів, до яких може бути надано доступ, пов'язані з різним тлумаченням судами положень закону. Так, наприклад ухвалою Херсонського міського суду Херсонської області від 31.10.2018 року у справі № 766/7213/18 було надано дозвіл на тимчасовий доступ до речей і документів, які містять охоронювану законом таємницю, шляхом зняття копій інформації, а саме інформації графічного та текстового змісту, яка міститься у вхідних та вихідних повідомленнях, інтернет-переписках у мобільних месенджерах, а також в інших мобільних програмах, наявних на мобільному телефоні [62]. Однак Шаргородським районним судом Вінницької області ухвалою від 03.03.2020 року у справі № 152/239/20 було відмовлено у тимчасовому доступі до інформації, що міститься у листуванні з використанням електронної пошти, СМС повідомлень, змісту спілкування (листування) в програмному забезпеченні, що встановлене в мобільному телефоні та забезпечувало можливість передачі даних (Viber, Telegram, WhatsApp, Gmail Google, фото), оскільки на думку слідчого судді надання доступу до особистого листування особи у месенджері мобільного телефону належить до негласних слідчих дій, якими здійснюється втручання у приватне спілкування [63]. Серед науковців також висловлюються різні думки з даного питання. С.І. Перепелиця вказує, що

«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».

З огляду на це, на його думку, задля забезпечення захисту права особи на таємницю спілкування необхідним є виключення п. 6 ст. 162 КПК України [64, с. 75-76].

З точки зору інших дослідників у випадку вирішення питання про надання тимчасового доступу до особистого листування у електронних сервісах отримання інформації має обмежуватися даними, які дають змогу ідентифікувати користувача облікового запису, дату та час листування за період, пов'язаний зі вчиненням кримінального правопорушення, але без розкриття змісту повідомлень [65].

Натомість, Т.О. Кузубова та О.О. Юхно у своєму монографічному дослідженні зазначають, що шляхом тимчасового доступу до особистого листування сторони кримінального провадження можуть ознайомитися з приватною кореспонденцією, але лише з тими листами, які вже написані та/або одержані та зберігаються у особи, яка надає до них доступ [66, с. 80]. Схожої позиції притримується й С. Тагієв, який, розглядаючи питання розмежування тимчасового доступу до інформації, що надходить у телекомунікаційні мережі, з НСРД, зауважує, що така інформація поділяється на динамічну та статичну. До динамічної належить інформація, «яка передається через мережу та не фіксується, не зберігається в пам'яті програмно-комплексного обладнання операторів і провайдерів телекомунікацій (наприклад, зміст розмов)» [67, с. 17]. Постачальники електронних комунікаційних послуг не записують та не зберігають розмови абонентів. Однак відповідно до положень ч. 2 і 3 ст. 121 Закону України «Про електронні комунікації» вони повинні забезпечити можливість підключення технічних засобів для зняття інформації з електронних комунікаційних мереж, тобто за наявності судового дозволу на втручання у приватне спілкування на них покладається обов'язок забезпечити можливість

перехоплення органами досудового розслідування інформації, що надходитиме в мережу у період часу, визначений у судовому рішенні. До статичної належить «інформація про споживача та про телекомунікаційні послуги, яка на відміну від динамічної знаходиться (накопичується, змінюється та знищується) у операторів і провайдерів телекомунікацій протягом певного часу», а саме дані про зв'язок, абонента, надання телекомунікаційних послуг, передбачені п. 7 ч. 1 ст. 162 КПК України, а також документи, повідомлення, що вже надійшли до особи і зберігаються в неї та зі змістом яких вона була ознайомена. Відповідно, доступ до динамічної інформації може бути наданий лише під час здійснення НСРД, тоді як статичну інформацію можна отримати в порядку тимчасового доступу до речей і документів [67, с. 18; с.21].

Також у п. 17 Інформаційного листа Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ від 05.04.2013 року № 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» наголошується на тому, що 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. У статтях 159, 162 КПК передбачено отримання слідчим (прокурором) інформації про зв'язок, що відбувся в минулому (постфактум), у тому числі про місцезнаходження радіоелектронного засобу у певний день та час, водночас визначена у ст. 268 КПК негласна слідча (розшукова) дія – установлення місцезнаходження

радіоелектронного засобу – передбачає локалізацію (моніторинг) місцезнаходження радіоелектронного засобу в режимі реального часу (тобто дає змогу отримати інформацію про те, де перебуває відповідний засіб на момент спостереження за ним, визначити маршрут його перебування) [68].

Таким чином, тимчасовий доступ до речей і документів має такі основні відмінності від НСРД, що становлять втручання у приватне спілкування. По-перше, як зазначено у ч. 4 ст. 258 КПК України втручанням у приватне спілкування є доступ до змісту спілкування за умов, якщо учасники спілкування мають достатні підстави вважати, що спілкування є приватним. Отже, НСРД, що становлять втручання у приватне спілкування, завжди мають таємний характер, тобто здійснюються без відома особи, щодо якої вони застосовуються. Натомість тимчасовий доступ до речей і документів може передбачати повідомлення особи про необхідність надати для ознайомлення речі та документи, що перебувають у її володінні, особливо у випадку надання доступу до особистого листування. По-друге, при проведенні НСРД підлягає перехопленню спілкування, що здійснюватиметься особою в режимі реального часу за період, вказаний в ухвалі слідчого судді, тоді як тимчасовий доступ можливий лише до відомостей про зв'язок, що мав місце у минулому. Також відповідно до ч. 1 ст. 159 КПК України тимчасовий доступ до електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку здійснюється шляхом зняття копії інформації, що міститься в таких електронних інформаційних системах, комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку, без їх вилучення. Водночас, на нашу думку, для забезпечення єдності у правозастосуванні слід доповнити положення Глави 15 КПК України в частині уточнення обсягу інформації, яка може бути отримана в ході здійснення тимчасового доступу до речей і документів.

У клопотанні слід чітко конкретизувати речі та документи, доступ до яких планується отримати. Згідно з положеннями п. 16 згаданого вище

Листа, у клопотанні про надання тимчасового доступу до документів, що знаходяться у оператора (провайдера) телекомунікацій, слід вказати наступні дані: 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.

У клопотанні про надання тимчасового доступу до особистого листування особи та інших записів особистого характеру, відповідно, слід вказувати носій інформації (якщо це електронна інформаційна система, комп'ютерна система або мобільний термінал системи зв'язку – їх конкретні характеристики, зокрема, модель обладнання, серійний номер, програмні засоби у яких містяться особисте листування та інші записи тощо), інформацію про володільця носія, відомості про обставини вчинення кримінального правопорушення, які передбачається отримати, часові рамки інформації. Так, ухвалою слідчого судді Старокостянтинівського районного суду Хмельницької області від 27.11.2020 року у справі № 683/2766/20 було задоволено клопотання про надання тимчасового доступу до «особистого листування та інших записів особистого характеру, наявних у встановленому програмному забезпеченні у виді месенджерів та пам'яті мобільних телефонів марки "Nokia" IMEI: НОМЕР_2 з сім-карткою мобільного оператора ПрАТ "ІНФОРМАЦІЯ_4 " і номером телефону: НОМЕР_3 та мобільного телефону

марки "RedmiNote 8 Pro" IMEI 1: HOMER_4, IMEI 2: HOMER_5 з чохлам чорного кольору у вигляді книжки з сім-карткою мобільного оператора ПрАТ "ІНФОРМАЦІЯ_5" і номером телефону: HOMER_6 власником та користувачем якого є ОСОБА_4, ІНФОРМАЦІЯ_3, уродженець м. Ленінабад Таджикистан, українець, громадянин України, з незакінченою середньою спеціальною освітою, депутатом не обирався, на утриманні неповнолітніх дітей не має, не працює, не зареєстрований, фактично проживає по АДРЕСА_1, раніше не судимий, з метою отримання інформації про обставини вчинення злочинів ОСОБА_4, а саме відомостей, які встановлені у програмному забезпеченні у виді месенджерів та пам'яті мобільного телефону, зокрема про збут останнім наркотичних засобів, інформації про постачальників наркотичних речовин, інших відомостей, які мають значення для досудового розслідування вказаного кримінального провадження, з можливістю копіювання інформації в електронному вигляді на цифровому носії та проведення огляду такої інформації, у період часу з 00 год. 00 хв. 01.01.2020 р. до 00 год. 00 хв. 27.11.2020 р.» [69].

Також у клопотанні слід вказати підстави вважати, що речі і документи перебувають або можуть перебувати у володінні відповідної фізичної або юридичної особи, значення речей і документів для встановлення обставин у кримінальному провадженні, можливість використання як доказів відомостей, що містяться в речах і документах, та неможливість іншими способами довести обставини, які передбачається довести за допомогою цих речей і документів, та обґрунтування необхідності вилучення речей і документів, якщо відповідне питання порушується стороною кримінального провадження. Проте органи досудового розслідування не завжди дотримуються вказаних вимог закону, внаслідок чого слідчі судді відмовляють у задоволенні клопотань. Наприклад, в ухвалі Сватівського районного суду Луганської області від 30.10.2018 року у справі № 426/21771/18 слідчим суддею було відмовлено у наданні тимчасового доступу до інформації, яка знаходиться в операторів та провайдерів

телекомунікацій, оскільки «слідчий не навів докази на підтвердження того, що особа могла користуватися під час вчинення злочину послугами мобільного зв'язку; крім того, інформація про кількість користувачів телекомунікаційних послуг, до інформації яких слідчий у разі задоволення клопотання отримає доступ, не надана, невідомо розмір площі, на якій за допомогою вказаних у клопотанні антен базових станцій здійснюється обслуговування абонентів; клопотання не містить обґрунтування того, яким чином інформація про усіх абонентів мобільного зв'язку, які перебували на невизначеній території у населеному районі, може бути використана у справі як доказ, не зазначено, як визначатимуть причетних до злочину осіб з усього масиву інформації про номери телефонів абонентів та їх зв'язки без точної прив'язки до місця вчинення злочину або до інших ознак, які можуть мати значення для розкриття злочину». Також слідчим не було доведено неможливість іншим способом довести обставини, які передбачалось довести за допомогою запитуваної інформації, та що потреби досудового розслідування виправдовували такий ступінь втручання у права і свободи осіб [70]. Ще одним прикладом відмови слідчого судді у задоволенні клопотання через його неналежне обґрунтування є ухвала Богодухівського районного суду Харківської області від 13.11.2018 року у справі № 613/1508/18, у якій слідчий суддя зазначив, що «сторона обвинувачення не довела наявності достатніх підстав вважати, що вказана в клопотанні інформація, яка знаходиться у оператора ПрАТ "ВФ Україна" сама по собі або в сукупності з іншими речами і документами кримінального провадження, у зв'язку з яким подається клопотання, має суттєве значення для встановлення важливих обставин у кримінальному провадженні... Також, слідчим не доведено того, що вказана в клопотанні інформація може бути використана як докази та що іншим способом неможливо довести обставини, які передбачається довести за допомогою цієї інформації. Наявні матеріали не містять жодних належних та допустимих відомостей на підтвердження існування вказаного в клопотанні мобільного номеру, його з'єднання з

номером потерпілого та причетності особи, яка ним користується до обставин скоєного злочину матеріалами клопотання також не підтверджено» [71].

Також нерідко органи досудового розслідування подають клопотання про тимчасовий доступ до речей і документів, які вже були отримані ними в ході проведення обшуку. Судова практика йде шляхом відмови у задоволенні таких клопотань, мотивуючи це тим що предмети вже перебувають на законних підставах у володінні органу досудового розслідування [72].

Слід зважати на те, що відповідно до ст. 161 КПК України забороняється доступ до листування або інші форми обміну інформацією між захисником та його клієнтом або будь-якою особою, яка представляє його клієнта, у зв'язку з наданням правової допомоги, та об'єктів, які додані до такого листування або інших форм обміну інформацією.

Відповідно до ст. 163 КПК України після отримання клопотання про тимчасовий доступ до речей і документів слідчий суддя, суд здійснює судовий виклик особи, у володінні якої знаходяться такі речі і документи, якщо тільки сторона кримінального провадження, яка звернулася з клопотанням, не доведе наявності достатніх підстав вважати, що існує реальна загроза зміни або знищення речей чи документів. Слідчий суддя, суд розглядає клопотання за участю сторони кримінального провадження, яка подала клопотання, та особи, у володінні якої знаходяться речі і документи; однак неприбуття за судовим викликом особи, у володінні якої знаходяться речі і документи, без поважних причин або неповідомлення нею про причини неприбуття не є перешкодою для розгляду клопотання. Кодексом не встановлено строк розгляду клопотання про тимчасовий доступ до речей і документів. У п. 8 Листа зазначено, що клопотання розглядається не пізніше трьох днів із дня його надходження до суду; у разі якщо особа, яка подала клопотання, обґрунтує у ньому наявність реальної загрози зміни або знищення речей і документів, слідчий суддя має невідкладно розглянути зазначене клопотання. Зважаючи на рекомендаційний характер зазначеного

документа, на практиці суди можуть не дотримуватися вказаного положення, і навіть затягувати з розглядом, що може негативно позначитися на якості досудового розслідування злочинів. Тому з нашої точки зору доцільним є доповнення ст. 163 КПК України вказівкою на строк розгляду клопотання, взявши за основу п. 8 Листа або ж встановивши інші розумні строки.

За результатами розгляду клопотання слідчий суддя, суд постановляє ухвалу, строк дії якої не може перевищувати два місяці з дня її постановлення. На особу, яка зазначена в ухвалі як володілець речей чи документів, покладається обов'язок надати тимчасовий доступ до зазначених в ухвалі речей і документів особі, зазначеній у відповідній ухвалі слідчого судді, суду. У разі невиконання ухвали про тимчасовий доступ до речей і документів слідчий суддя, суд за клопотанням сторони кримінального провадження, якій надано право на доступ до речей і документів на підставі ухвали, має право постановити ухвалу про дозвіл на проведення обшуку згідно з положеннями цього Кодексу з метою відшукування та вилучення зазначених речей і документів.

2.2. Охорона таємниці спілкування під час проведення негласних слідчих (розшукових) дій.

Під час кримінального провадження порушення таємниці спілкування можливе лише в ході здійснення НСРД, що являють собою втручання у приватне спілкування. Згідно зі ст. 258 КПК України різновидами втручання у приватне спілкування є аудіо-, відеоконтроль особи, арешт, огляд і виїмка кореспонденції, зняття інформації з електронних комунікаційних мереж та зняття інформації з електронних інформаційних систем. Загальні підстави для проведення таких заходів регламентовані у ст. 246 КПК України, відповідно до якої НСРД проводяться у випадках, якщо відомості про кримінальне правопорушення та особу, яка його вчинила, неможливо отримати в інший спосіб. Втручання у приватне спілкування проводиться

виключно у кримінальному провадженні щодо тяжких або особливо тяжких злочинів на підставі ухвали слідчого судді. Для отримання дозволу на втручання у приватне спілкування прокурор або слідчий за погодженням з прокурором має подати відповідне клопотання, при цьому необхідність отримання дозволу передбачена в усіх випадках, коли будь-яке слідча (розшукова) дія включатиме таке втручання.

Клопотання розглядається 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. Кодексом встановлено достатньо короткий строк розгляду клопотання у 6 годин, вочевидь з метою забезпечення оперативного досудового розслідування злочинів. На слідчого, прокурора покладається обов'язок належно мотивувати необхідність такого істотного втручання у конституційне право особи, а саме має бути доведено вчинення кримінального правопорушення відповідного ступеня тяжкості, наведено обставини, що дають підстави підозрювати особу у вчиненні кримінального правопорушення, обґрунтовано неможливість отримання відомостей про кримінальне правопорушення та особу, яка його вчинила, в інший спосіб, а також можливість отримання в ході проведення НСРД 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. Крім того, клопотання має відповідати й формальним вимогам, зокрема містити загальну інформацію щодо кримінального провадження, відомості про особу (осіб), місце або річ, щодо яких необхідно провести НСРД, вид НСРД та обґрунтування строку її проведення, відомості залежно від виду негласної слідчої дії про ідентифікаційні ознаки, які дозволять унікально ідентифікувати абонента спостереження, електронну комунікаційну мережу, кінцеве (термінальне) обладнання тощо.

Недотримання перелічених вимог призводить до відмови слідчого судді у наданні дозволу на здійснення втручання у приватне спілкування. Так, ухвалою Харківського апеляційного суду від 06.12.2018 року у справі № 818/2677т/18 слідчий суддя відмовив у наданні дозволу на зняття інформації з транспортних телекомунікаційних мереж, посилаючись на недоведеність неможливості отримання відомостей про злочин та особу в інший спосіб, відсутність конкретизації обставин, з метою встановлення яких пропонувалося провести НСРД та відсутність пояснення, чому це не можна було зробити іншими засобами кримінального провадження; також у клопотанні не було вказано особу, щодо якої мала бути застосована НСРД [73]. Водночас, відповідно до ч. 5 ст. 248 КПК України відмова у задоволенні клопотання не позбавляє сторону обвинувачення права повторно звернутися з новим клопотанням про надання дозволу на проведення НСРД.

Однак аналіз судової практики надання дозволів на здійснення втручання у приватне спілкування свідчить про те, що й самі слідчі судді не завжди дотримуються вимог Кодексу, встановлених для ухвалення судових рішень, зокрема, ними задовольняються клопотання без належного обґрунтування необхідності проведення НСРД. Прикладом цього можна навести ухвалу Запорізького апеляційного суду від 24.03.2020 року у справі № 4807/1263/20, у якій слідчий суддя надав дозвіл на зняття інформації з транспортних телекомунікаційних мереж, а саме з мобільних номерів особи, не аргументувавши, яке саме доказове значення може мати інформація, здобута при проведенні НСРД, а також чи дійсно неможливо здобути відомості щодо обставин злочину шляхом проведення інших процесуальних дій, що передбачають менший ступінь втручання у права особи [74]. Такі дії слідчих суддів є неприпустимими, адже на них законом покладена функція здійснення судового контролю за діяльністю органів досудового розслідування, який виступає одним із запобіжників порушення прав і свобод людини під час кримінального провадження, та передбачає належну перевірку наявності підстав для втручання у приватне спілкування.

У КПК України встановлено обмеження строку проведення НСРД: за загальним правилом він не може перевищувати два місяці. Проте за наявності для цього підстав слідчий, прокурор можуть звернутися до слідчого судді за дозволом на повторне проведення НСРД. Загальний строк протягом якого в одному кримінальному провадженні може тривати проведення НСРД, що являє собою втручання у приватне спілкування, не може перевищувати максимальні строки досудового розслідування, передбачені ст. 219 цього Кодексу (вісімнадцять місяців). У разі якщо така НСРД проводиться з метою встановлення місцезнаходження особи, яка переховується від органів досудового розслідування, слідчого судді чи суду, та оголошена в розшук, вона може тривати до встановлення місцезнаходження розшукуваної особи. Також Кодекс містить вимогу прийняття рішення прокурором про припинення проведення НСРД як тільки в цьому відпаде необхідність.

Досліджуючи питання можливості здійснення втручання у приватне спілкування до постановлення ухвали слідчого судді, необхідно зазначити, що згідно зі ст. 250 КПК України такі дії допускаються лише у випадках, передбачених цим Кодексом. Така можливість прямо передбачена лише у ст. 268 і 269 КПК України, що регулюють проведення НСРД, якій не є втручанням у приватне спілкування. Також у п. 1.15 Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні вказано, що до постановлення ухвали слідчого судді дозволяється проводити лише НСРД, передбачені ст. 268 і 269 КПК України [75]. Отже, НСРД, що належать до втручання у приватне спілкування, не можуть бути проведені до постановлення ухвали слідчого судді.

Відповідно до п. 3.1 Інструкції організація проведення НСРД покладається на слідчого, який може проводити їх самостійно, спільно з уповноваженими підрозділами, залучати до їх проведення інших осіб, а також доручати їх проведення уповноваженим оперативним підрозділам. Хід

та результати НСРД підлягають фіксації; за результатами проведення НСРД складається протокол, до якого в разі необхідності долучаються додатки. Враховуючи особливий характер даної процесуальної дії, що полягає в необхідності забезпечення режиму таємності, відомості про її проведення підлягають засекречуванню, а особи, яким стала відома така інформація, попереджаються про кримінальну відповідальність за її розголошення. Матеріали, одержані в ході проведення НСРД, які не будуть використані в цілях досудового розслідування злочину, підлягають негайному знищенню за рішенням прокурора. В той же час КПК України містить приписи щодо обов'язку письмового повідомлення прокурором чи слідчим за його дорученням осіб, конституційні права яких були тимчасово обмежені під час проведення НСРД, та підозрюваного і його захисника про таке обмеження, в тому числі і у випадку знищення матеріалів. Конкретний час повідомлення визначається із урахуванням наявності чи відсутності загроз для досягнення мети досудового розслідування, суспільної безпеки, життя або здоров'я осіб, які причетні до проведення НСРД. Відповідне повідомлення про факт і результати НСРД повинне бути здійснене протягом дванадцяти місяців з дня припинення таких дій, але не пізніше звернення до суду з обвинувальним актом.

На перший погляд, зазначені положення видаються такими, що відповідають стандартам ЄСПЛ у сфері охорони таємниці спілкування у кримінальному провадженні. Проте у законодавстві відсутні детальні вимоги щодо змісту такого повідомлення, що надає стороні обвинувачення можливість на власний розсуд визначати обсяг інформації, що підлягає розкриттю. При цьому якщо відомості, отримані в результаті проведення НСРД, планується використати у кримінальному провадженні, то у сторони захисту наявна можливість ознайомитися з ними в порядку відкриття сторонами матеріалів досудового розслідування, передбаченому ст. 290 КПК України, і у випадку недотримання стороною обвинувачення такої вимоги за правовим висновком Верховного Суду України такі відомості можуть бути

визнані недопустимими як докази [76]. В ситуації зі знищенням матеріалів про проведення НСРД особа може бути позбавлена належного інформування про втручання у її приватне спілкування, отримавши лише коротку відписку з загальними даними щодо факту та результатів застосованої до неї НСРД.

Ще одну проблему становить відсутність ефективного правового засобу захисту у випадку незаконного втручання органами досудового розслідування у приватне спілкування. За змістом ст. 309 КПК України ухвала слідчого судді про дозвіл на проведення НСРД не підлягає оскарженню в апеляційному порядку. Як вказав Верховний Суд у постанові від 31.05.2021 року у справі № 646/3986/19, «перевірці в апеляційній інстанції підлягають лише ухвали слідчого судді, які пов'язані з можливістю істотного обмеження прав, свобод та інтересів особи або мають вирішальне значення для руху досудового розслідування чи кримінального провадження в цілому» [77]. Але таке обмеження законодавцем переліку ухвал слідчого судді, що можуть бути оскаржені, виглядає не досить обґрунтованим, адже під час проведення НСРД має місце суттєве обмеження конституційних прав і свобод людини, зокрема, під час втручання у приватне спілкування. КПК України передбачає можливість подання заперечень проти ухвал слідчого судді, що не підлягають оскарженню, під час підготовчого провадження в суді. Проте Кодексом чітко не врегульовано порядок та наслідки подання таких заперечень.

Розглянемо тепер особливості проведення кожного з різновидів втручання у приватне спілкування. За змістом ст. 260 КПК України та п. 1.11.2 Інструкції аудіо-, відеоконтроль особи полягає у негласній фіксації та обробці із використанням технічних засобів розмов особи або інших звуків, рухів, дій, пов'язаних з її діяльністю або місцем перебування тощо, за наявності достатніх підстав вважати, що вони можуть містити відомості, які мають значення для досудового розслідування. Виходячи з аналізу судової практики аудіо-, відеоконтроль особи може застосовуватися для збору інформації про обставини вчинення злочинного діяння, злочинні зв'язки,

встановлення місцезнаходження особи та речових доказів, зокрема у випадку конспіративного (таємного) характеру діяльності злочинця, що унеможлиблює отримання необхідних даних іншим способом [78; 79].

Аудіоконтроль особи полягає у «прослуховуванні та фіксації розмов такої особи», та може здійснюватися у двох формах: епізодично, тобто під час якихось конкретних подій: відвідування особою певних місць, зустрічей, або безперервно, «на проміжок часу, що визначений у рішенні слідчого судді», як правило цілодобово. Відеоконтроль особи являє собою «візуальне спостереження за діями особи шляхом відеозапису та аудіофіксації у будь-якому місці її перебування» [80, с. 210]. У Кодексі чітко не вказано, де саме може здійснюватися аудіо-, відеоконтроль особи. У наукових джерелах зазначається, що це може бути будь-яке місце, як приватне володіння особи, так і громадські місця, транспорт тощо [43, с. 75]. Слідчі судді у окремих випадках задовольняють клопотання про надання дозволу на здійснення аудіо-, відеоконтролю особи одночасно в публічно доступних місцях і публічно недоступних місцях [79]. При цьому у випадку здійснення даної НСРД у публічно недоступному місці (тобто такому, до якого неможливо увійти або в якому неможливо перебувати на правових підставах без отримання на це згоди власника, користувача або уповноважених ними осіб) попередньо має проводитися інша НСРД, передбачена ст. 270 КПК України – обстеження публічно недоступних місць, житла чи іншого володіння особи, з метою встановлення технічних засобів аудіо-, відеоконтролю. На думку І.І. Маскалюк, для отримання дозволу на проведення кожної із зазначених НСРД слідчий, прокурор мають складати окремі клопотання, за результатами розгляду яких також мають бути постановлені окремі рішення [80, с. 213]. Натомість в п. 6 Інформаційного листа Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ від 29.01.2013 року «Про окремі питання здійснення слідчим суддею суду апеляційної інстанції судового контролю за дотриманням прав, свобод та інтересів осіб у кримінальному провадженні» вказується, що слідчі судді мають враховувати,

що однорідні питання, які необхідно з'ясувати в рамках одного кримінального провадження шляхом проведення НСРД одного або різних видів, пов'язаних між собою (при цьому необхідність з'ясування таких питань обґрунтовується однаковими обставинами), можуть ініціюватися слідчим (прокурором) у рамках одного клопотання та вирішуватися слідчим суддею однією ухвалою. Наприклад, в одному документі може міститися клопотання про дозвіл на здійснення аудіо-, відеоконтролю особи (ст. 260 КПК) та обстеження публічно недоступних місць, житла чи іншого володіння особи (ст. 267 КПК) із метою встановлення технічних засобів аудіо-, відеоконтролю особи [81, с. 290]. На наш погляд, підхід, викладений у Листі, є більш виправданим, оскільки це сприятиме економії часу й відповідно дотриманню засади розумності строків кримінального провадження без шкоди для прав та інтересів осіб, на яких може вплинути ухвалене рішення. Проте слідчі судді переважно вирішують питання проведення аудіо-, відеоконтролю особи окремою ухвалою, а в ряді випадків слідчий, прокурор навіть не подають клопотання щодо проведення обстеження публічно недоступних місць, житла чи іншого володіння особи.

Наступною НСРД є арешт, огляд і виїмка кореспонденції, передбачена ст. 261 і 162 КПК України. Накладення арешту на кореспонденцію здійснюється за наявності достатніх підстав вважати, що поштово-телеграфна кореспонденція певної особи іншим особам або інших осіб їй може містити відомості про обставини, які мають значення для досудового розслідування, або речі і документи, що мають істотне значення для досудового розслідування. Метою проведення даної НСРД може бути:

«отримання інформації доказового характеру про злочин, його учасників, місце приховання знарядь й об'єктів злочинної діяльності; тимчасове припинення листування між певною особою та іншими особами для припинення злочинних зв'язків між ними; розшук підозрюваного, що переховується; забезпечення накладення арешту на майно певної особи, зокрема підозрюваного (грошові перекази, посилки тощо)» [82, с. 65].

Накладення арешту можливе лише до різновидів кореспонденції, що

передається поштово-телеграфним зв'язком, а саме листи усіх видів, бандеролі, посилки, поштові контейнери, перекази, телеграми, інші матеріальні носії передання інформації між особами. Враховуючи те, що наразі для спілкування більшою мірою використовуються мобільний зв'язок та електронні засоби комунікацій, найбільш ефективним накладення арешту на кореспонденцію вбачається для пошуку речових доказів, зокрема при розслідуванні злочинів, пов'язаних з незаконним обігом різних предметів (наприклад, наркотичних речовин).

Згідно з п. 1.11.3 Інструкції накладення арешту полягає у забороні установам зв'язку та фінансовим установам вручення кореспонденції адресату без відповідної вказівки слідчого, прокурора. Як і щодо аудіо-, відеоконтролю особи, Кодекс не передбачає детальних вимог до змісту клопотання про надання дозволу на арешт кореспонденції. Ми погоджуємося з пропозицією науковців додатково вказувати у клопотанні «конкретну установу зв'язку, якій доручено здійснювати контроль і затримувати кореспонденцію, та порядок невідкладного інформування установою слідчого про затримання кореспонденції» [83, с. 233].

Накладення арешту на кореспонденцію надає право слідчому здійснювати огляд і виїмку кореспонденції. У наукових колах тривають дискусії щодо того, чи є арешт, огляд і виїмка кореспонденції різними НСРД. Деякі дослідники вважають, що вони є взаємопов'язаними, але різними НСРД. Д.Б. Сергєєва розглядає їх як етапи однієї НСРД, порядок проведення якої закріплено у декількох статтях КПК України [43, с. 81]. З позиції В.І. Галагана огляд та виїмка кореспонденції входять до структури накладення арешту на кореспонденцію як процесуальної дії. Водночас накладення арешту, огляд та виїмка кореспонденції є трьома послідовними етапами проведення НСРД. В ході її проведення слідчий може обмежитися лише першим етапом (якщо кореспонденція не надійшла до установи зв'язку), першим та другим (якщо внаслідок огляду виявлено, що перехоплена кореспонденція не містить даних, що мають значення для кримінального

провадження) або охопити всі три етапи [82, с. 56, 63]. На нашу думку, саме другий підхід до визначення арешту, огляду і виїмки кореспонденції як етапів проведення однієї НСРД є правильним з огляду на їх тісну взаємопов'язаність та взаємообумовленість, а також те, що це прямо передбачено у ст. 258 КПК України. Проте серед слідчих суддів трапляється різне розуміння кримінально-процесуального закону, прикладом чого є ухвала Сумського апеляційного суду від 07.02.2019 року у справі № 4816/199/19, в якій арешт, огляд і виїмка кореспонденції вказані як окремі НСРД [84].

Огляд затриманої кореспонденції проводиться слідчим в установі зв'язку, якій доручено здійснювати контроль і затримувати цю кореспонденцію, за участю представника цієї установи, а за необхідності слідчий також може залучити до огляду спеціаліста. Під час огляду слідчий вивчає кореспонденцію на предмет наявності у ній відомостей, що мають значення для досудового розслідування. В разі виявлення у ній речей (речовин), документів, що мають значення для досудового розслідування, слідчий у межах, визначених ухвалою слідчого судді, здійснює виїмку відповідної кореспонденції або обмежується зняттям копій чи отриманням зразків з відповідних відправлень. Зняття копій чи отримання зразків здійснюється з метою збереження конфіденційності накладення арешту на кореспонденцію. У разі необхідності особою, яка проводить огляд поштово-телеграфної кореспонденції, може бути прийняте рішення про нанесення на виявлені речі і документи спеціальних позначок, обладнання їх технічними засобами контролю, заміну речей і речовин, що становлять загрозу для оточуючих чи заборонені у вільному обігу, на їх безпечні аналоги. Якщо під час огляду кореспонденції не було виявлено речі або документи, що мають значення для досудового розслідування, то слідчий дає вказівку про вручення оглянутої кореспонденції адресату. Керівники та працівники установ зв'язку зобов'язані сприяти проведенню НСРД і не розголошувати факт її проведення чи отриману інформацію.

У ст. 263 і 264 КПК України регламентований порядок проведення таких НСРД, як зняття інформації з електронних комунікаційних мереж та зняття інформації з електронних інформаційних систем. 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. Зняття інформації з електронних комунікаційних мереж полягає у проведенні із застосуванням відповідних технічних засобів спостереження, відбору та фіксації змісту інформації, яка передається особою та має значення для досудового розслідування, а також одержанні, перетворенні і фіксації різних видів сигналів, що передаються каналами зв'язку. В п. 1.11.5.1 Інструкції виокремлено дві форми проведення даної НСРД:

1) 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;

2) 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.

З положень ч. 2 ст. 263 КПК України випливає, що перш ніж провести дану слідчу дію необхідно ідентифікувати абонента спостереження, електронну комунікаційну мережу та кінцеве обладнання. Вказані дані

можуть бути отримані шляхом тимчасового доступу до речей і документів, які знаходяться в операторів і провайдерів телекомунікацій або у інший спосіб. Однак дещо проблемним є питання ідентифікації абонента спостереження у випадку втручання у приватне спілкування, що здійснюється за допомогою мобільного телефону. З цього приводу М.А.Самбор зазначає, що

«ідентифікаційна телекомунікаційна картка, яка використовується для ідентифікації кінцевого обладнання абонента в телекомунікаційній мережі (SIM-картка, USIM-картка, R-UIM-картка тощо), не дає можливості ідентифікувати абонента – фізичну особу, яка користується такою картою, адже на сьогоднішній день в Україні немає законодавчої вимоги щодо укладення договору про надання послуг рухомого (мобільного) зв'язку у письмовій формі, що гарантуватиме ідентифікацію абонента. Крім того, законодавством України не врегульовано вторинний ринок, на якому здійснюється реалізація ідентифікаційних телекомунікаційних карток, зокрема тому, що договори про надання послуг рухомого (мобільного) зв'язку не підлягають обов'язковій державній реєстрації. IMEI (міжнародний ідентифікаційний номер мобільного терміналу) фактично також ідентифікує кінцеве обладнання, а саме мобільний термінал».

Встановити зв'язок між абонентом і кінцевим обладнанням можливо й іншим шляхом (наприклад, проведення допиту потерпілого, свідків). Проте з точки зору дослідника, це підвищує ризики неправомірного втручання у приватне спілкування, тому що «відсутні документальні підтвердження факту користування конкретною особою кінцевим обладнанням (мобільним телефоном)»; фактично користуватися телефоном може не лише підозрюваний, а й будь-які інші особи. Він приходить до висновку, що необхідно внести відповідні зміни до законодавства та призупинити здійснення даної НСРД [85, с. 76-79]. На наш погляд, з такою позицією складно погодитися. У багатьох державах реєстрація та використання SIM-карт для телефону здійснюється виключно за наявності документів, що посвідчують особу. Водночас у окремих європейських державах відмовилися від запозичення такої практики, мотивуючи це відсутністю нових переваг у боротьбі зі злочинністю. В Україні немає однозначної позиції стосовно

доцільності зміни порядку надання електронних комунікаційних послуг через те, що запровадження обов'язкової документальної прив'язки кожного мобільного номеру до конкретної особи з одного боку спрощує ідентифікацію абонента, а з іншого боку цим самим створює широке поле для зловживань правоохоронними органами своїми повноваженнями, особливо у світлі незавершеності їх реформування, і може призвести до незаконного втручання у приватне життя громадян. Спроби запровадити продаж SIM-карток за паспортами завершувалися відкликанням законопроекту [86]. Очевидно, що у випадку внесення змін до законодавства постане проблема реєстрації SIM-карток, що вже використовуються громадянами. Також за останні кілька років правоохоронними органами вироблена практика проведення зняття інформації з електронних комунікаційних мереж, і заборона здійснення даної НСРД призведе до негативних наслідків для ефективного здійснення досудового розслідування злочинів, тому потрібно шукати інші способи забезпечення захисту прав особи від незаконного втручання у приватне спілкування.

Ж.В. Удовенко також акцентує увагу на тому, що під час кримінального провадження можливими є ситуації, коли прослуховування розмов здійснюється «не лише стосовно осіб, щодо яких здійснюється кримінальне провадження, а й осіб, залучених до нього у іншому процесуальному статусі, зокрема... потерпілий, свідок, інші близькі родичі та члени сім'ї – за наявності погрози вчинення проти них злочинних дій». Ми підтримуємо її пропозицію щодо встановлення такої діяльності органів досудового розслідування шляхом доповнення ст. 263 КПК України ч. 5 у такій редакції: «За наявності загрози вчинення насильства або інших протиправних дій щодо потерпілого, свідка або їхніх близьких родичів чи членів сім'ї зняття інформації з транспортних телекомунікаційних мереж допускається за письмовою заявою цих осіб або за їхньою письмовою згодою, а без такої заяви або згоди – за ухвалою слідчого судді» [87, с. 124-125].

Зняття інформації з електронних інформаційних систем полягає у пошуку, виявленні та фіксації відомостей, що містяться в електронній інформаційній системі, або їх частин, доступі до електронної інформаційної системи або її частини, а також отриманні таких відомостей без відома її власника, володільця або утримувача, якщо є підстави вважати, що в електронній інформаційній системі або її частині наявна інформація, що має значення для досудового розслідування. У законодавстві відсутнє визначення поняття «електронна інформаційна система». У ст. 1 Закону України «Про захист інформації в інформаційно-комунікаційних системах» наявний термін «інформаційно-комунікаційна система», який означає сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле; інформаційна система відповідно визначена як організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів [88]. У наукових джерелах під електронною інформаційною системою пропонується розуміти:

«взаємозв'язок технічних засобів (комп'ютерів, серверів, апаратно-програмних комплексів, зовнішніх накопичувачів інформації, локальних комп'ютерних мереж та/або інших технічних засобів) з інформаційними технологіями, що реалізують інформаційні процеси та призначені для збору, зберігання, обробки, пошуку, розповсюдження, передачі та надання впорядкованої інформації (даних) в електронному вигляді... 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» [52, с. 135].

В п. 1.11.6 Інструкції зазначено, що дана НСРД передбачає одержання інформації, в тому числі із застосуванням технічних засобів, яка міститься в електронно-обчислювальних машинах (комп'ютер), автоматичних системах, комп'ютерній мережі. У судовій практиці також до електронних інформаційних систем відносять веб-сайти, електронну пошту, програмне забезпечення що міститься на мобільних телефонах, зокрема, месенджери [89]. У клопотанні додатково мають бути вказані ознаки, що дозволяють

ідентифікувати електронну інформаційну систему, в якій може здійснюватися втручання у приватне спілкування.

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. Під системою логічного захисту слід розуміти «використання імені користувача, пароллю, аудит системи, шифрування даних, захист від вірусів, резервне копіювання, використання джерел безперебійного живлення та створення відмовостійких систем», тобто вжиття особою заходів для запобігання неправомірному доступу до електронної інформаційної системи [43, с. 104]. В такому випадку інформація може бути отримана шляхом огляду предмета, з якого здійснюється доступ до електронної інформаційної системи: згідно правового висновку Верховного суду в постанові від 09.04.2020 року у справі № 727/6578/17 протокол огляду текстових повідомлень, які знаходилися у мобільному телефоні та доступ до яких не був пов'язаний із наданням володільцем відповідного серверу (оператором мобільного зв'язку) доступу до електронних інформаційних систем є допустимим доказом [90].

2.3. Іноземний досвід втручання у приватне спілкування.

У пошуках шляхів вирішення проблем правового регулювання того чи іншого питання та моделей імплементації міжнародно-правових стандартів у національне законодавство держави доцільним є дослідження нормативно-правової бази провідних держав світу. З огляду на належність України до континентальної правової системи нами було обрано для порівняльного аналізу країни, що належать до такої ж правової системи, а саме Німеччина, Естонія, Швейцарія.

2.3.1. Втручання у приватне спілкування за законодавством Федеративної Республіки Німеччина.

Процедура здійснення втручання у приватне спілкування регламентована Кримінальним процесуальним кодексом [91]. Згідно з розділом 100 допускається арешт поштових відправлень і телеграм, якщо конкретні факти свідчать про те, що вони були направлені підозрюваному або відправлені ним, і у них можуть міститися відомості, що мають значення для досудового розслідування. Рішення щодо проведення даної слідчої дії приймає суд або у виключних невідкладних випадках прокурор, при цьому на прокурора покладається обов'язок отримати дозвіл суду протягом трьох днів після прийняття рішення. На відміну від КПК України даним кодексом уповноважено суд на проведення огляду кореспонденції, але він може делегувати здійснення даного заходу прокурору. Кореспонденція, яка не була піддана перлюстрації, а також відправлення, що не містять інформації, яка має значення для досудового розслідування, підлягають негайному врученню адресату.

У розділах 100a-100c врегульовано заходи щодо перехоплення та запису приватного спілкування, а саме перехоплення телекомунікацій, таємний віддалений доступ до інформаційно-технологічних систем та аудіоконтроль особи у приватних приміщеннях). Загальними підставами їх проведення є обґрунтована підозра особи у вчиненні тяжкого чи особливо тяжкого злочину або скоєнні замаху чи готування до такого злочину (при цьому у нормах міститься перелік конкретних злочинів, при розслідуванні яких дозволяється здійснення такого втручання), та неможливість отримання відомостей щодо обставин вчиненого чи місцезнаходження особи у інший спосіб.

Рішення щодо перехоплення телекомунікацій може бути прийнято виключно судом за клопотанням прокурора. У невідкладних випадках рішення може бути прийняте прокурором, що не звільняє від обов'язку отримати ухвалу суду протягом трьох днів. Максимальний строк проведення

слідчої дії обмежується трьома місяцями з можливістю продовження не більш як на три місяці за наявності до того підстав. Такий захід може бути застосовано лише до підозрюваного або осіб, щодо яких є обґрунтована підозра у тому, що вони спілкуються з підозрюваним або підозрюваний користується їх засобами телефонного зв'язку. Віддалений доступ до інформаційно-технологічної системи та аудіоконтроль особи у приватних приміщеннях проводяться виключно за рішенням суду, ухваленим на підставі клопотання прокурора, на строк не більше одного місяця з можливістю продовження на такий же строк. Дані заходи застосовуються виключно щодо підозрюваного, за винятком: щодо віддаленого доступу до інформаційно-технологічної системи – якщо є підстави вважати що підозрюваний використовує інформаційно-технологічну систему іншої особи та втручання в інформаційно-технологічну систему підозрюваного саме по собі не призведе до встановлення обставин, що мають значення для кримінального провадження; щодо аудіоконтролю особи – якщо підозрюваний перебуває у приватному приміщенні іншої особи, та застосування такого заходу лише у володінні підозрюваного не надасть можливості отримати відомості, що мають значення для кримінального провадження. У рішенні щодо проведення зазначених слідчих дій серед іншого, мають бути обов'язково зазначені ідентифікаційні ознаки об'єктів, щодо яких надається доступ: номер телефону чи інший ідентифікатор з'єднання або кінцевого обладнання, найменування інформаційно-технологічної системи, конкретні приватні приміщення чи кімнати, що підлягають негласному нагляду.

Істотні відмінності у порівнянні з КПК України має порядок повідомлення особи щодо здійсненого щодо них втручання. Так, якщо відповідно до українського законодавства особа, щодо якої була проведена НСРД обов'язково має бути повідомлена щодо факту такого втручання у приватне спілкування, то за німецьким законодавством допускається відсутність сповіщення особи в разі, якщо застосований захід лише побічно

стосувався цієї особи і є підстави припускати, що дана особа не зацікавлена в повідомленні. Повідомлення має бути здійснене протягом дванадцяти місяців з дня припинення заходу, проте допускається відстрочка такого повідомлення за рішенням суду. Також кодекс допускає оскарження в суді законності рішення щодо проведення заходу: у повідомленні має бути зазначена можливість такого оскарження та строк подання скарги, який становить два тижні після повідомлення особи. Видалення даних, отриманих в ході проведення втручання у приватне спілкування, може здійснюватися виключно після завершення строку судового оскарження слідчої дії.

Отже, основні відмінності у правовому регулюванні охорони таємниці спілкування у законодавстві Німеччини та України полягають в тому, що за німецьким законодавством чіткіше врегульовано порядок аудіоконтролю особи, зокрема, встановлено підстави для встановлення засобів спостереження у приміщеннях, що не належать підозрюваному, та обов'язок зазначати в судовому рішенні конкретні приміщення, у яких буде відбуватися негласна слідча дія; також різниться порядок повідомлення особи про НСРД, зокрема німецьке законодавство допускає відсутність такого повідомлення взагалі; наявна можливість оскарження рішення щодо проведення втручання у приватне спілкування.

2.3.2. Втручання у приватне спілкування за законодавством Естонської Республіки.

Відповідно до Глави 3 Кримінального процесуального кодексу Естонії втручання у приватне спілкування віднесене до оперативно-розшукових заходів [92]. Прийняття рішення про здійснення втручання у приватне спілкування віднесено до компетенції слідчого судді, який ухвалює рішення на підставі вмотивованого клопотання прокурора; строк заходу становить не більше трьох місяців з можливістю продовження на строк до трьох місяців. Загальний строк застосування до особи оперативно-розшукових заходів не може перевищувати один рік.

Даним кодексом порівняно з КПК України детальніше врегульовано

порядок повідомлення особи про вжиті щодо неї заходи втручання у приватне спілкування. Згідно зі ст. 126-13 негайно після закінчення строку їх проведення має бути сповіщено особу, щодо якої вони проводилися, а також особу, недоторканність приватного життя якої була істотно порушена в ході їх проведення. Виняток становить лише наявність обставин, внаслідок яких повідомлення може суттєво зашкодити кримінальному провадженню, правам і свободам особи, гарантованим законом, або поставити у небезпеку іншу особу, а також поставити під загрозу таємний характер методів і тактики оперативно-розшукових заходів, засобу, що використовується при їх проведенні. В такому разі сповіщення особи має бути здійснене по закінченню досудового розслідування, але не пізніше ніж через рік після завершення строку дії оперативно-розшукового заходу. Якщо ж і по завершенню даного строку не відпали обставини, що були підставою для неінформування особи, то не пізніше ніж за 15 днів до спливу вказаного строку прокурор має ініціювати клопотання перед слідчим суддею про його продовження. Також при повідомленні особи встановлено обов'язок роз'яснення порядку оскарження проведення оперативно-розшукового заходу.

У ст. 126-16 кодексу передбачена можливість оскарження постанови про видачу дозволу на проведення оперативно-розшукового заходу шляхом подання приватної скарги в порядку, передбаченому Главою 15 даного кодексу. Окремо може бути оскаржено хід оперативно-розшукового заходу, неповідомлення особи про його проведення та неознайомлення її з матеріалами, зібраними в результаті проведення заходу, в порядку, передбаченому розділом 5 Глави 8 цього кодексу. Досить цікавими є положення ст. 126-15 кодексу, якими передбачено обов'язок Міністерства юстиції публікувати на власному веб-сайті звіт на основі статистичних даних, отриманих від оперативно-розшукових органів, прокуратур та судів, який має містити відомості про вид та кількість порушених оперативно-розшукових справ, кількість дозволів на проведення оперативно-розшукових

заходів по їх видам, кількість осіб, сповіщених про проведення оперативно-розшукового заходу, та кількість осіб, повідомлення яких відкладено на один рік згідно з вимогами кодексу, оскільки в Україні не передбачена на законодавчому рівні вимога ведення узагальнюючої статистики по проведеним НСРД.

Таким чином, ключовими відмінностями між Україною та Естонією у кримінальному процесуальному законі є детально врегульована процедура повідомлення особи про проведене втручання у таємницю спілкування у кримінальному провадженні з можливістю продовження строку відкладення повідомлення за наявності до того підстав, можливість оскарження заходу, здійсненого щодо особи, та вимога публікувати статистичні звіти щодо проведених оперативно-розшукових заходів.

2.3.3. Втручання у приватне спілкування за законодавством Швейцарської Конфедерації.

Підстави для втручання у приватне спілкування під час кримінального провадження визначені у ст. 269 Кримінального процесуального кодексу Швейцарської Конфедерації [93]. Згідно з нею, прокурор може організувати моніторинг пошти і телекомунікацій, якщо є обґрунтовано підозра щодо вчинення кримінального правопорушення, зазначеного в переліку у цій статті, тяжкість правопорушення виправдовує перехоплення і здобуття іншим шляхом відомостей про кримінальне правопорушення, що передбачається отримати за допомогою слідчої дії неможливо. При цьому моніторинг вимагає також дозволу спеціалізованого суду примусових заходів, який надається на строк не більше трьох місяців з можливістю продовження на такий же строк.

Втручання у приватне спілкування може застосовуватися щодо підозрюваного, а також третьої особи, якщо на основі конкретної інформації є достатні підстави вважати, що підозрюваний використовує поштову адресу або телекомунікаційну мережу такої особи, або третя особа отримує певні повідомлення від підозрюваного або передає повідомлення від

підозрюваного іншій особі. Кодекс також більш широко у порівнянні з КПК України окреслює сферу професійного привілею. Під час спостереження за особою, яка належить до однієї з професій, зазначених у ст. 170-173 кодексу (державні службовці, юристи, медичні працівники, журналісти тощо) суд повинен забезпечити відокремлення інформації, яка має значення для досудового розслідування, від професійної, щоб гарантувати, що жодна професійна таємниця не стане відомою органу кримінальної юстиції. Відокремлені дані мають бути негайно знищені та не можуть бути використані як докази. Це положення не застосовується якщо є обґрунтована підозра в тому, що особа, на яку поширюється професійна таємниця, є винною у вчиненні злочину, і є конкретні причини, що виправдовують пряме перехоплення комунікацій. Під час спостереження за іншими особами, відомості про спілкування з представниками зазначених професій мають бути так само відокремлені та знищені.

Прокурор має повідомити осіб, чиє спілкування було піддано перехопленню, про причину, строку та форму здійснення негласного заходу не пізніше моменту закінчення досудового розслідування. З дозволу суду повідомлення може бути відкладене, якщо отримані матеріали не використовуються як докази у судовому провадженні, та якщо це необхідно для захисту суспільних або приватних інтересів. Закон наділяє особу, щодо якої здійснювалося втручання, правом подати заперечення в порядку ст. 393-397 кодексу.

На підставі вищевикладеного можемо зазначити, що різниця у законодавстві України та Швейцарії в частині регулювання заходів втручання у приватне спілкування полягає в тому, що по-перше, нагляд за законністю під час здійснення заходів перехоплення здійснює спеціалізований суд; по-друге, наявний більший ступінь захисту професійної таємниці (поширюється на більшу кількість осіб, вказана вимога обов'язкового знищення відомостей, що стосуються професійної таємниці та випадки, коли вона не застосовується); по-третє, надається можливість

оскарження негласної слідчої дії та врегульована процедура такого оскарження.

У Кримінальному процесуальному кодексі України закріплена низка гарантій забезпечення права особи на таємницю спілкування, які передбачають наявність визначеного порядку втручання у приватне спілкування, яким закріплені підстави для такого втручання, повноваження органів досудового розслідування, судовий контроль за законністю заходів негласного стеження за особою та допустимі межі втручання у права особи. В цілому зазначені положення закону відповідають міжнародно-правовим стандартам охорони приватного спілкування людини під час кримінального провадження, проте воно не позбавлене недоліків, що виражаються у нечіткості розмежування заходів втручання у приватне спілкування та тимчасового доступу до особистого листування особи, недостатній врегульованості порядку повідомлення особи про здійснені щодо неї негласні слідчі (розшукові) дії та відсутності належної процедури оскарження таких заходів в судовому порядку, що призводить до неоднакового розуміння судами законодавчих норм та порушення прав людини.

ВИСНОВКИ

На підставі проведеного дослідження можна зробити наступні висновки. Таємниця спілкування належить до основних прав людини, передбачених міжнародно-правовими актами. При цьому у Конвенції про захист прав і основоположних свобод вона закріплена як складова більш ширшого права на повагу до приватного життя. Європейським судом з прав людини у своїй практиці вироблено основні підходи до визначення предмету охорони таємницею спілкування. Нею охоплюються практично будь-які різновиди спілкування, від кореспонденції, що передається поштово-телеграфним зв'язком, до спілкування за допомогою новітніх технологій. Охорона надається лише приватному спілкуванню, проте його межі є достатньо розпливчатими й за умов наявності розумних очікувань у особи щодо приватності спілкування воно може включати й професійну діяльність особи.

При перевірці дотримання Конвенції при здійсненні втручання у приватне спілкування під час кримінального провадження Суд перевіряє правомірність обмежень через застосування критеріїв здійснення згідно з законом, відповідно до мети, визначеної у Конвенції, та необхідності у демократичному суспільстві. Крізь аналіз практики Суду ми можемо виокремити такі ключові вимоги, що ставляться до правового регулювання втручання у приватне спілкування: наявність доступного й передбачуваного законодавства, яке має з достатньою чіткістю визначати підстави і порядок втручання, повноваження компетентних органів, зокрема, в ньому мають бути закріплені характер, масштаби і тривалість заходів, чітко визначені особи, до яких вони можуть бути застосовані (при цьому особливі гарантії повинні бути втілені для представників окремих професій, що пов'язано з потребою у збереженні професійної таємниці), процедури дослідження, використання та зберігання отриманої інформації, засоби захисту від її неправомірного використання, та ефективний судовий контроль за

втручанням на всіх етапах здійснення негласних заходів. Крім того, Судом передбачена також вимога сповіщення особи про застосовані щодо неї заходи спостереження та наявності можливості для їх оскарження. Втручання у приватне спілкування може бути здійснене виключно з метою захисту національної та громадської безпеки чи економічного добробуту країни, запобігання заворушенням чи злочинам, захисту здоров'я чи моралі або захисту прав і свобод інших осіб, та лише за наявності реальної суспільної потреби і пропорційності втручання меті його здійснення.

Проводячи паралелі з правовим регулюванням охорони таємниці спілкування в Україні, можемо зазначити, що право на таємницю спілкування набуло закріплення на найвищому (конституційному) рівні, а також гарантується у кримінальному провадженні. Водночас правові положення щодо захисту права на таємницю спілкування не позбавлені певних недоліків, зокрема, з недостатньою чіткістю визначено її обсяг, що виражається у відсутності нормативного визначення складових понять даного права «кореспонденція», «листування», «телефонні розмови», «телеграфна кореспонденція», «інші види кореспонденції», а також на відміну від Кримінального процесуального кодексу України у Конституції України не гарантується захист інших форм спілкування. Вказане може бути виправлене шляхом внесення відповідних змін до законодавства, а саме слід роз'яснити зміст кореспонденції та її різновидів з врахуванням наукових напрацювань, та закріпити гарантії інших форм спілкування, або ж застосувати інший підхід, передбачений у ч. 3 ст. 258 Кримінального процесуального кодексу України, закріпити гарантії таємниці спілкування, що передбачають захист інформації, що передається у будь-якій формі від однієї особи до іншої безпосередньо або за допомогою засобів зв'язку будь-якого типу. Крім того, у КПК України відсутній визначений порядок дій при перехопленні спілкування особи з носіями професійного привілею (захисником, священнослужителем). На нашу думку, такі положення мають бути доповнені вказівкою на знищення відомостей, отриманих в результаті

такого перехоплення, та неможливість їх використання у доказуванні; можливе врахування також швейцарського досвіду правового регулювання втручання у спілкування з представниками окремих професій.

У кримінальному процесуальному законі досить детально регламентовано порядок втручання у приватне спілкування. Воно може бути здійснене лише в ході проведення негласних слідчих (розшукових) дій, таких як аудіо-, відеоконтроль особи, арешт, огляд і виїмка кореспонденції, зняття інформації з електронних комунікаційних мереж та зняття інформації з електронних інформаційних систем. В цілому положення щодо проведення НСРД відповідають стандартам ЄСПЛ, що ставляться до такого втручання у право особи на таємницю спілкування. У законі визначено підстави, строки для здійснення заходів втручання, їх характер, та процедуру прийняття рішення слідчим суддею, на якого покладена функція судового контролю за діями органів досудового розслідування при перехопленні спілкування, вимоги до фіксації та зберігання матеріалів, отриманих при їх проведенні. Однак істотними недоліками КПК України є нечіткість вимог щодо змісту повідомлення особи про проведені щодо неї НСРД, та відсутність можливості оскаржити ухвалу слідчого судді про дозвіл на проведення втручання у приватне спілкування та дії правоохоронних органів. На наш погляд, необхідним є внесення змін до законодавства, які б деталізували процедуру повідомлення особи, а також надали можливість оскаржити в судовому порядку заходи втручання у приватне спілкування, з урахуванням висвітленого у роботі досвіду правового регулювання зазначених питань у інших державах.

Ще однією проблемою є недотримання органами досудового розслідування та слідчими суддями вимог КПК України на етапі ухвалення рішення про проведення НСРД, що проявляється у необґрунтованості клопотань та рішень, що приймаються на їх основі. Вказане можна пояснити їх великим навантаженням у роботі та бажанням пришвидшити здійснення кримінального провадження у справі, проте неприпустимим є вирішення

таких завдань за рахунок нехтування правами осіб, щодо яких здійснюється втручання у приватне спілкування. На нашу думку, законодавець має звернути увагу на проблему постановлення компетентними особами неправомірних рішень та вжити заходів щодо недопущення виникнення таких прецедентів, у тому числі шляхом збільшення кількості штатних працівників, покращення відбору кадрів та проведення заходів з підвищення їх кваліфікації, надання роз'яснень щодо застосування положень закону тощо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України : Закон України від 28.06.1996 р. № 254к/96-ВР.
URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>.
2. Про міжнародні договори України : Закон України від 29.06.2004 р. № 1906-IV. URL: <https://zakon.rada.gov.ua/laws/show/1906-15#Text>.
3. Загальна декларація прав людини від 10.12.1948 р.
URL: https://zakon.rada.gov.ua/laws/show/995_015#Text.
4. Міжнародний пакт про громадянські і політичні права від 16.12.1966 р.
URL: https://zakon.rada.gov.ua/laws/show/995_043#Text.
5. Конвенція про захист прав людини і основоположних свобод від 04.11.1950 р. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text.
6. Про виконання рішень та застосування практики Європейського суду з прав людини : Закон України від 23.02.2006 р. № 3477-IV.
URL: <https://zakon.rada.gov.ua/laws/show/3477-15#Text>.
7. Довідник із застосування статті 8 Європейської конвенції з прав людини. Рада Європи/Європейський суд з прав людини. 2018 р. 118 с.
URL: https://www.echr.coe.int/Documents/Guide_Art_8_UKR.pdf.
8. Стаття 8 Конвенції про захист прав людини і основоположних свобод: стандарти застосування при здійсненні правосуддя / Автори: Н. Ахтирська, В. Філатов, Т. Фулей, Х. Хембах. К.: Істина, 2011. 200с.
9. Case of Niemietz v. Germany. URL: [https://hudoc.echr.coe.int/eng#{%22fulltext%22:\[%22%22CASE%20OF%20NIEMIETZ%20v.%20GERMANY%22%22\],%22documentcollectionid%22:\[%22GRANDCHAMBER%22,%22CHAMBER%22\],%22itemid%22:\[%22001-104030%22\]}](https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22%22CASE%20OF%20NIEMIETZ%20v.%20GERMANY%22%22],%22documentcollectionid%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-104030%22]}).
10. Case of M.N. and Others v. San Marino. URL: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-155819%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-155819%22]}).
11. Справа «Хелфорд проти Сполученого Королівства». URL: <https://khpg.org/1363591929>.

12. Справа «Барбулеску проти Румунії». URL: <http://privacy.khpg.org/1604922584>.
13. Case of Copland v. The United Kingdom. URL: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-79996%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-79996%22]}).
14. Справа «Круслен проти Франції». URL: <http://eurocourt.in.ua/Article.asp?AIdx=432>.
15. Справа «Ювіг проти Франції». URL: <http://privacy.khpg.org/1604922590>.
16. Справа «Волохи проти України». URL: https://zakon.rada.gov.ua/laws/show/974_138#Text.
17. Справа «Роман Захаров проти Росії». URL: <http://privacy.khpg.org/1604922614>.
18. Справа «Кеннеді проти Сполученого Королівства». URL: <http://privacy.khpg.org/1604922638>.
19. Case of Malone v. The United Kingdom. URL: https://european-court.ru/uploads/ECHR_Malone_v_the_United_Kingdom_02_08_1984.pdf.
20. Case of Dudchenko v. Russia. URL: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-184557%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-184557%22]}).
21. Справа «Класс та інші проти Німеччини». URL: https://zakon.rada.gov.ua/laws/show/980_093#Text.
22. Справа «Сабо і Віші проти Угорщини». URL: <http://privacy.khpg.org/1604922643>.
23. Фулей Т.І. Застосування практики Європейського суду з прав людини при здійсненні правосуддя: Науково-методичний посібник для суддів. 2-ге вид. випр., допов. К., 2015. 208 с.
24. Case of Michaud v. France. URL: [https://hudoc.echr.coe.int/eng#{%22display%22:\[%220%22\],%22languageisocode%22:\[%22UKR%22\],%22appno%22:\[%2212323/11%22\],%22documentcollectionid%22:\[%22CHAMBER%22\],%22itemid%22:\[%22001-126862%22\]}](https://hudoc.echr.coe.int/eng#{%22display%22:[%220%22],%22languageisocode%22:[%22UKR%22],%22appno%22:[%2212323/11%22],%22documentcollectionid%22:[%22CHAMBER%22],%22itemid%22:[%22001-126862%22]}).

25. Case of Silver and Others v. The United Kingdom. URL: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-57577%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57577%22]}).
26. Case of Calogero Diana v. Italy. URL: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-58072%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58072%22]}).
27. Справа «Беляєв та Дігтяр проти України. URL: https://zakon.rada.gov.ua/laws/show/974_938#Text.
28. Справа «Довженко проти України». URL: https://zakon.rada.gov.ua/laws/show/974_845#Text.
29. Case of Jankauskas v. Lithuania. URL: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-68394%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-68394%22]}).
30. Шумило М. Є. Реалізація конституційного принципу таємниці листування, телефонних розмов, телеграфної та іншої кореспонденції у досудових стадіях кримінального процесу України : монографія. Х. : Бровін О.В., 2012. 208 с.
31. Про правовий статус іноземців та осіб без громадянства : Закон України від 22.09.2011 р. № 3773-VI. URL: <https://zakon.rada.gov.ua/laws/show/3773-17#Text>.
32. Цивільний кодекс України : Закон України від 16.01.2003 р. № 435-IV. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text>.
33. Кримінальний кодекс України : Закон України від 05.04.2001 р. № 2341-III. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>.
34. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 р. № 4651-VI. URL: <https://zakon.rada.gov.ua/laws/show/4651-17#Text>.
35. Про поштовий зв'язок : Закон України від 04.10.2001 р. № 2759-III. URL: <https://zakon.rada.gov.ua/laws/show/2759-14#Text>.
36. Кореспонденція : Словник української мови. URL: <http://sum.in.ua/s/korespondencija>.
37. Назаров В. В. Право особи на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції та його обмеження у

- кримінальному провадженні. *Вісник Академії адвокатури України*. 2009. №. 1. С. 119-125. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/vaau_2009_1_17.pdf.
38. Кондратов Д. Ю. Таємниця кореспонденції як предмет злочину, передбаченого статтею 163 Кримінального кодексу України. 2015. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/511/tayemnicya_korrespondenciya_yak_predmet_z.pdf?sequence=2&isAllowed=y.
39. Ємчук Л. В. Конституційно-правове регулювання особистого та сімейного життя людини і громадянина. Дис. кандидата юридичних наук. URL: <http://www.uzhnu.edu.ua/uk/infocentre/get/7948>. – 2015.
40. Вирок Першотравневого районного суду м. Чернівці від 29.08.2008 р. Справа № 1-235/2008. URL: <https://reyestr.court.gov.ua/Review/2394418>.
41. Вирок Франківського районного суду м. Львова від 11.10.2021 р. Справа № 465/5121/20. URL: <https://reyestr.court.gov.ua/Review/100341888>.
42. Листування : Словник української мови. URL: <http://sum.in.ua/s/lystuvannja>.
43. Савляк І. І. Таємниця спілкування як засада кримінального провадження: дис. ... канд. юрид. наук. Київ, 2018. 229 с. URL: http://elar.naiu.kiev.ua/bitstream/123456789/8137/1/Dis_savliak_06112018.pdf.
44. Про затвердження Правил надання послуг поштового зв'язку : Постанова Кабінету Міністрів України від 05.03.2009 р. № 270. URL: <https://zakon.rada.gov.ua/laws/show/270-2009-%D0%BF#Text>.
45. Вирок Луцького міськрайонного суду Волинської області від 17.02.2015 р. Справа № 161/1717/15-к. URL: <https://reyestr.court.gov.ua/Review/42727424>.
46. Вирок Рівненського міського суду Рівненської області від 13.09.2019 р. Справа № 569/12334/19. URL: <https://reyestr.court.gov.ua/Review/84251500>.

47. Про затвердження Правил надання та отримання телекомунікаційних послуг : Постанова Кабінету Міністрів України від 11.04.2012 р. № 295. URL: <https://zakon.rada.gov.ua/laws/show/295-2012-%D0%BF#Text>.
48. Про електронні комунікації : Закон України від 16.12.2020 р. № 1089-IX. URL: <https://zakon.rada.gov.ua/laws/show/1089-20#Text>.
49. Вирок Дніпровського районного суду м. Києва від 29.09.2020 р. Справа № 755/2110/20. URL: <https://reyestr.court.gov.ua/Review/91885873>.
50. Про затвердження інструкцій з надання послуг телеграфного зв'язку : Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 22.04.2014 р. № 195. URL: <https://zakon.rada.gov.ua/laws/show/z0515-14#Text>.
51. В Україні скасують телеграми. URL: <https://www.bbc.com/ukrainian/news-42095444>.
52. Ткачик А. Б. Таємниця спілкування та її обмеження в кримінальному провадженні: дисертація : дис. – ЛьвДУВС, 2021. URL: http://dspace.lvduvs.edu.ua/bitstream/1234567890/3748/1/tkachik_d.pdf.
53. Крет Г. Р. Загальні положення про втручання в приватне спілкування за кримінальним процесуальним кодексом України //LEGAL SCIENCE, LEGISLATION AND LAW ENFORCEMENT: TRADITIONS AND NEW EUROPEAN APPROACHES. 2021. С. 167. URL: https://archer.chnu.edu.ua/jspui/bitstream/123456789/2240/1/Wloclawek_law_%D0%98%D1%8E%D0%BB%D1%8C_2021.pdf#page=167.
54. Білічак О. А. Втручання у приватне спілкування за кримінальним процесуальним законодавством України. *Слово Національної школи суддів України*. 2018. № 2. С. 94-110. URL: http://nbuv.gov.ua/UJRN/cln_2018_2_11.
55. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20.01.2012 р. № 2-рп/2012. Справа № 1-9/2012. URL: <https://zakon.rada.gov.ua/laws/show/v002p710-12#Text>.

- 56.Постанова Верховного Суду від 23.11.2021 р. Справа № 332/1189/18. URL: <https://verdictum.ligazakon.net/document/101424412>.
- 57.Про адвокатуру та адвокатську діяльність : Закон України від 05.07.2012 р. № 5076-VI. URL: <https://zakon.rada.gov.ua/laws/show/5076-17#Text>.
- 58.Колесник В. А. Гарантії дотримання прав особи при проведенні негласних слідчих (розшукових) дій. *Науковий вісник Ужгородського національного університету*. Серія: Право. – 2021. – №. 63. – С. 293-297. URL: <http://visnyk-pravo.uzhnu.edu.ua/article/view/232284/231093>.
- 59.Кримінально-виконавчий кодекс України : Закон України від 11.07.2003 р. № 1129-IV. URL: <https://zakon.rada.gov.ua/laws/show/1129-15#Text>.
- 60.Про затвердження Правил внутрішнього розпорядку установ виконання покарань : Наказ Міністерства юстиції України від 28.08.2018 р. № 2823/5. URL: <https://zakon.rada.gov.ua/laws/show/z1010-18#Text>.
- 61.Про попереднє ув'язнення : Закон України від 30.06.1993 р. № 3352-XII. URL: <https://zakon.rada.gov.ua/laws/show/3352-12#Text>.
- 62.Ухвала Херсонського міського суду Херсонської області від 31.10.2018 р.
Справа № 766/7213/18. URL: <https://verdictum.ligazakon.net/document/77550997>.
- 63.Ухвала Шаргородського районного суду Вінницької області від 03.03.2020 р.
Справа № 152/239/20. URL: <https://verdictum.ligazakon.net/document/87985481>.
- 64.Перепелиця С. І. Дотримання прав особи під час втручання у приватне спілкування в кримінальному провадженні. *Форум права*. 2019. № 2. С. 70–79. URL: http://nbuv.gov.ua/j-pdf/FP_index.htm_2019_2_10.pdf.
- 65.Питання тимчасового доступу до вмісту електронної поштової скриньки. URL: <https://yur-gazeta.com/publications/practice/inshe/pitannya-timchasovogo-dostupu-do-vmistu-elektronnoyi-poshtovoyi-skrinki.html>.
- 66.Кузубова Т. О., Юхно О. О. Тимчасовий доступ до речей і документів: теоретичні і прикладні проблеми : монографія. За загальною редакцією

доктора юридичних наук, професора О. О. Юхна. Харків : ФОП Панов А.М., 2019. 348 с.

URL: <http://dspace.univd.edu.ua/xmlui/handle/123456789/5743>.

67. Тагієв С. Тимчасовий доступ до інформації, яка знаходиться в операторів і провайдерів телекомунікацій, у кримінальному провадженні. *Слово Національної школи суддів України*. 2013. № 2. С. 13-24. URL: http://nbuv.gov.ua/j-pdf/cln_2013_2_4.pdf.
68. 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>.
69. Ухвала Старокостянтинівського районного суду Хмельницької області від 27.11.2020 р. Справа № 683/2766/20. URL: <https://verdictum.ligazakon.net/document/93188550>.
70. Ухвала Сватівського районного суду Луганської області від 30.10.2018 р. Справа № 426/21771/18. URL: <https://verdictum.ligazakon.net/document/77477870>.
71. Ухвала Богодухівського районного суду Харківської області від 13.11.2018 р. Справа № 613/1508/18. URL: <https://verdictum.ligazakon.net/document/77811700>.
72. Ухвала Індустріального районного суду м. Дніпропетровська від 26.09.2019 р. Справа № 202/5602/19. URL: <https://verdictum.ligazakon.net/document/84814611>.
73. Ухвала Харківського апеляційного суду від 06.12.2018 р. Справа № 818/2677т/18. URL: <https://verdictum.ligazakon.net/document/88167670>.
74. Ухвала Запорізького апеляційного суду від 24.03.2020 р. Справа № 4807/1263/20. URL: <https://verdictum.ligazakon.net/document/94654604>.

75. Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні: Наказ Генеральної прокуратури України, Міністерства внутрішніх справ України, Служби безпеки України, Адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України від 16.11.2012 р. № 114/1042/516/1199/936/1687/5. URL: <https://zakon.rada.gov.ua/laws/show/v0114900-12#Text>.
76. Постанова Верховного Суду України від 16.03.2017 р. Справа № 671/463/15-к. URL: <https://verdictum.ligazakon.net/document/66203468>.
77. Постанова Верховного Суду від 31.05.2021 р. Справа № 646/3986/19. URL: <https://verdictum.ligazakon.net/document/97429838>.
78. Ухвала Миколаївського апеляційного суду від 30.03.2020 р. Справа № 812/1260/19. URL: <https://verdictum.ligazakon.net/document/88483749>.
79. Ухвала Апеляційного суду Харківської області від 27.03.2020 р. Справа № 790/10212т/18. URL: <https://verdictum.ligazakon.net/document/88489048>.
80. Маскалюк І. І. Аудіо-, відеоконтроль особи як різновид втручання у приватне спілкування. *Вісник Пенітенціарної асоціації України*. 2017. №2. С. 209-216. URL: http://nbuv.gov.ua/j-pdf/bpau_2017_2_28.pdf.
81. Збірка інформаційних матеріалів, які регулюють окремі питання кримінального провадження в Україні: [упоряд. С. М. Алфьоров, С. М. Міщенко, В. І. Фаринник та ін.]; за заг. ред. В. І. Сліпченка. — К.: «Хай-Тек Прес», 2013. — 580 с. URL: <https://rm.coe.int/1680098ea0>.
82. Галаган В. І., Шум В. В. Процесуальний порядок накладення арешту на кореспонденцію у кримінальному провадженні України: монографія / К., 2017. 168 с.
URL: http://ekmair.ukma.edu.ua/bitstream/handle/123456789/13188/Galagan_Procesual%60ny%60j_poryadok_nakladennya.pdf?sequence=1.
83. Луцик В. Накладення арешту на кореспонденцію як негласна слідча (розшукова) дія. *Юридичний вісник*. 2014. № 3. С. 232-236. URL: http://nbuv.gov.ua/UJRN/urid_2014_3_44.

84. Ухвала Сумського апеляційного суду від 07.02.2019 р. Справа № 4816/199/19. URL: <https://verdictum.ligazakon.net/document/83810304>.
85. Самбор М. А. Негласні слідчі (розшукові) дії, пов'язані із зняттям інформації з транспортних телекомунікаційних мереж та встановленням місцезнаходження радіоелектронного засобу: підстави для проведення та умови гарантування прав і свобод людини та громадянина як споживача послуг рухомого (мобільного) зв'язку. *Вісник Дніпропетровського університету імені Альфреда Нобеля*. Сер. : Юридичні науки. 2013. № 1. С. 74-81. URL: http://nbuv.gov.ua/UJRN/vdujn_2013_1_13.
86. В яких країнах неможливо купити SIM-карту без документів та реєстрації. URL: <https://www.slovoidilo.ua/2019/11/27/infografika/suspilstvo/yakux-krayinax-nemozhlyvo-kupyty-sim-kartu-dokumentiv-ta-reyestracziyi>.
87. Удовенко Ж. В. Проблеми забезпечення охорони таємниці приватного життя під час зняття інформації з транспортних телекомунікаційних мереж. *Наукові записки НаУКМА*. Юридичні науки. 2019. Т. 3. С. 120-126. URL: http://nbuv.gov.ua/UJRN/NaUKMAun_2019_3_19.
88. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994р. № 80/94-ВР. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>.
89. Ухвала Вищого антикорупційного суду від 09.12.2020 р. Справа № 991/10070/20. URL: <https://verdictum.ligazakon.net/document/94995493>.
90. Постанова Касаційного кримінального суду Верховного Суду від 09.04.2020 р. Справа № 727/6578/17. URL: <https://opendatabot.ua/court/88749345-832f2760eee13a7d536b804edccc496b>.
91. Criminal Procedure Code of the Federal Republic of Germany (1950, as of 2019). Доступ із інформаційно-правової системи OSCE Office for Democratic Institutions and Human Rights. URL: https://www.legislationline.org/download/id/9178/file/GERM_CPC_en.pdf.
92. Уголовно-процессуальный кодекс Эстонии (2003, с изменениями 2021 г.). Доступ з інформаційно-правової системи OSCE Office for Democratic

Institutions and Human Rights. URL:
https://www.legislationline.org/download/id/9738/file/EST_CPC_ru.pdf.

93. Swiss Criminal Procedure Act (2007, as of March 2021). Доступ з інформаційно-правової системи OSCE Office for Democratic Institutions and Human Rights. URL:
https://legislationline.org/sites/default/files/documents/9f/SWITZ_CPC.pdf.