

**ЗАХИСТ ТАЄМНИЦІ КОРЕСПОНДЕНЦІЇ В СОЦІАЛЬНИХ
МЕРЕЖАХ: ПІДХІД ЄВРОПЕЙСЬКОГО СУДУ З ПРАВ ЛЮДИНИ**

correspondent

ЗМІСТ

ВСТУП	2
РОЗДІЛ 1. ЗМІСТ ПОНЯТТЯ «КОРЕСПОНДЕНЦІЯ»	4
1.1. Поняття «кореспонденція»: національне законодавство та правозастосовна практика	4
1.2. Поняття «кореспонденція»: підхід Європейського суду з прав людини ..	8
РОЗДІЛ 2. ПОРЯДОК ОТРИМАННЯ ДОСТУПУ ДО КОРЕСПОНДЕНЦІЇ .	12
2.1. Порядок отримання доступу до кореспонденції: національні законодавство та правозастосовна практика.....	12
2.2. Порядок доступу до кореспонденції: підхід Європейського суду з прав людини.....	17
РОЗДІЛ 3. ПОРЯДОК ОТРИМАННЯ ДОСТУПУ ДО КОРЕСПОНДЕНЦІЇ У СОЦІАЛЬНИХ МЕРЕЖАХ: ПРОБЛЕМИ І ПЕРСПЕКТИВИ.....	21
ВИСНОВКИ.....	28
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	30
Додаток 1.....	36
Додаток 2.....	37

ВСТУП

Актуальність теми. Право на приватність, складовою якого є право на таємницю кореспонденції, існує як одне з основоположних прав людини і громадянина, закріплене як на національному, так і на міжнародному рівнях. Якщо 15 років тому держава ще могла чітко встановити межі та досягти консенсусу між правами осіб на приватність та захистом національної безпеки, то на сьогодні, у епоху глобалізації та інформатизації, цю мету реалізувати достатньо важко – кожного року з’являються якісь нові можливості для спілкування осіб (гаджети, програми тощо), а аудиторія соціальних мереж зростає (див. Додаток 1, 2) [13; 23]. І по суті все це є кореспонденцією. Але, на

жаль, Україна не приділяє достатньої уваги всім цим змінами і не вносить правки до НПА, стосовно складових поняття «кореспонденція» і, як наслідок, порядку отримання доступу до неї.

Особливу увагу, на наш погляд, варто приділити порядку отримання доступу до кореспонденції у соціальних мережах, оскільки саме вони наразі сягнули найбільшої популярності як засіб спілкування між людьми. Але питання стосовно процедури отримання доступу до такого виду листування не забезпечено у нашій державі, оскільки цій аспект має міжнародно-правове підґрунтя. Мова йде саме про те, що більшість соціальних мереж (і особливо найпопулярніші із них) зареєстровані за межами України, і відповідно їх засновниками і керівниками є громадянами іноземних держав. А, отже, органи нашої держави можуть на них впливати лише дуже обмежено. Варто також врахувати результати найсвіжіших досліджень, які вказують на можливість маніпулювати суспільною думкою через суспільні мережі (наприклад, президентські вибори в США 2016 року, референдум щодо Brexit у Сполученому Королівстві). Посилаючись на все вищезгадане, ми можемо припустити, що проблематика теми цієї роботи є достатньо серйозною і потребує ґрунтовного вивчення, а, отже, дослідження права на приватність (таємницю кореспонденції) у соціальних мережах є надзвичайно актуальним.

Стан наукового дослідження. Різноманітні аспекти права на приватність, у тому числі й права на таємницю кореспонденції досліджували В. Малярєнко, Є. Коваленко, Т. Мойсєєва, І. Козякова, Л. Берекашвілі, О. Дроздов, О. Дроздова, Т. Дудаш, Д. Сергєєва, Ж. Чевичалова, В. Спасович, М. Михєєнко, В. Манукян, О. Попазова, Д. Мельник, В. Галаган тощо. Проте, не применшуючи внеску дослідників, зауважимо, що, на жаль, у вітчизняній доктрині відсутні комплексні дослідження права на таємницю кореспонденції в соціальних мережах.

Мета та завдання. Метою дослідження є здійснення аналізу та розгляд проблематики права на приватність (таємницю кореспонденції), у контексті визначення поняття «кореспонденція у соціальних мережах», та отримання

доступу до неї. Відповідно до вищевказаної мети необхідно виконати наступні **завдання**: 1) проаналізувати національне законодавство та практику ЄСПЛ щодо визначення поняття «кореспонденція» та її складових; 2) визначити процедуру отримання доступу до кореспонденції, закріплену на національному рівні та переглянути практику Європейського суду з прав людини з цього питання; 3) дослідити обставини та порядок отримання доступу до кореспонденції у соціальних мережах у світлі користувацьких угод найбільш поширених в Україні соціальних мереж; 4) визначити проблеми реалізації права на приватність кореспонденції в соціальних мережах в Україні та запропонувати шляхи їх вирішення.

Об’єктом дослідження є суспільні відносини, які складаються в процесі реалізації права на приватність (поваги до таємниці кореспонденції). **Предметом дослідження** є суспільні відносини, які складаються з огляду на охорону таємниці кореспонденції в соціальних мережах у праві Ради Європи та національних законодавств і правозастосовній практиці.

Методи обрані, виходячи з поставлених у дослідженні мети й завдань, з урахуванням об’єкта й предмета дослідження. Їх основу складають аналіз, який передбачає дослідження національного законодавства, практики ЄСПЛ та користувацьких угод соціальних мереж, порівняльно-правовий метод, що забезпечує порівняння правового регулювання цього питання і рішень Європейського суду, а також метод аналогії, суть якого передбачає проведення аналогій як у межах законодавства України, так і між практикою ЄСПЛ і національними правом і правозастосовною практикою.

РОЗДІЛ 1. ЗМІСТ ПОНЯТТЯ «КОРЕСПОНДЕНЦІЯ»

1.1. Поняття «кореспонденція»: національне законодавство та правозастосовна практика

На сьогодні проблема захисту прав людини стоїть достатньо гостро як у світі загалом, так і в Україні зокрема. У межах цього дослідження ми зосередимо свою увагу на праві на приватність (ст. 8 Європейської конвенції з прав людини) [27]. Це право охоплює широкий спектр питань, до яких належать: сімейне життя; житло; приватне життя, а саме фізична, психологічна чи моральна цілісність, конфіденційність, індивідуальність та автономія; а також кореспонденція. Саме засоби забезпечення таємниці останньої в умовах глобалізації, інформатизації, поширення соціальних мереж цікавлять нас у передусім. Отже, перше питання, яке перед нами постає, полягає у визначенні поняття кореспонденції та її складових.

Досліджуючи законодавство України, можна стверджувати, що першим і основним законом держави, який захищає право на таємницю кореспонденції, є Конституція України. Відповідно до статті 31 Конституції України, «кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції. Винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинів чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо» [29]. Якщо говорити про тлумачення змісту згаданого права, то законодавець не ухвалив для цього окремого законодавчого акту, проте ми знаходимо закріплення права на таємницю кореспонденції у більш розлогому вигляді ще й у Цивільному кодексі України. У ЦК України таємниці кореспонденції присвячено лише одну статтю. Зокрема, стаття 306 ЦКУ передбачає: «Фізична особа має право на таємницю листування, телеграм, телефонних розмов, телеграфних повідомлень та інших видів кореспонденції. Якщо кореспонденція стосується особистого життя іншої фізичної особи, для її використання, зокрема шляхом опублікування, потрібна згода цієї особи. 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. 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» [45]. Серед інших національних актів, які теж закріплюють право особи на таємницю кореспонденції, слід виокремити Закон України «Про телекомунікації», стаття 9 якого регламентує, що таємниця телефонних розмов, листування, телеграфної та іншої кореспонденції захищається Конституцією та Законами України, а також статтю 6 Закону України «Про поштовий зв'язок», яка передбачає те ж саме, проте стосовно таємниці поштових відправлень [25; 26].

Наведене вище дозволяє нам сформулювати перелік елементів, які можуть іменуватись кореспонденцією відповідно до національного законодавства: листи, телеграми, телефонні розмови, інші засоби поштового зв'язку, а також телеграфні повідомлення. Проте, на наш погляд, цей перелік є застарілим, оскільки деякі із названих видів зв'язку вже досить давно є непопулярними та мало використовуються. Ще одним дискусійним питанням вважаємо розуміння у вказаному контексті поняття «лист»: йдеться про звичайні (паперові) листи, чи враховуються і повідомлення через електронну пошту? Звісно, зараз переважною частиною офіційних і особистих повідомлень обмінюються через електронну пошту, що в разі зручніше. Загалом, з інструментальної точки зору, електронні листи це такі ж листи, як і паперові, але в іншому вираженні. Проте, частина 8 статті 1 Закону України «Про поштовий зв'язок» передбачає, що «лист – це поштове відправлення у вигляді поштового конверта з вкладенням письмового повідомлення або документа, розміри і масу якого встановлено відповідно до законодавства України» [25]. Це визначення вказує, що електронні листи не є складовою частиною кореспонденції, а отже їх таємниця не гарантується у рамках права на приватність та їх перегляд третіми особами не повинен тягти юридичної відповідальності.

Загалом, аналізуючи зміст вказаних вище нормативно-правових актів, нагадаємо, що їх було переважно ухвалено у кінці 90-тих років, а найсвіжіші зміни до них датуються 2012 роком. Між тим, з кожним роком з'являються нові види електронного спілкування, доступ до яких не врегульовано національним законодавством. Більше того, не визначеним навіть залишається питання щодо легального віднесення їх до способів кореспонденції. Найбільш яскравим прикладом такого електронного спілкування є соціальні мережі, без яких наразі неможливо уявити життя людини. Для сучасної молоді ведення життя у соціальних мережах є потребою, адже саме це спілкування відіграє значну роль для їх соціалізації. Проте чи можемо ми вважати, що особисте спілкування у соціальних мережах та месенджерах є конфіденційним? Чи понесе особа покарання за втручання у таке спілкування чи за розголошення змісту такого спілкування між третіми особами? На жаль, ми не можемо із впевненістю відповісти на ці питання, оскільки чинне законодавство України не містить ні вичерпного переліку того, що може вважатись кореспонденцією, ні навіть легального визначення поняття «кореспонденція». Вбачається, що невдовзі вітчизняному законодавцю доведеться звернути увагу на цю проблему.

Зокрема, до поняття «кореспонденція» широко звертається кримінальне та кримінально-процесуальне законодавство. Наприклад, стаття 163 КК України передбачає, що «порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер, - караються штрафом від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або обмеженням волі до трьох років» [30]. Отже, ми можемо припустити, що це визначення розширює значення поняття «кореспонденція», адже інформацією, що передається засобами зв'язку чи через комп'ютер, може бути і листи, які надсилаються електронною поштою, і повідомлення у месенджерах, встановлених на мобільних телефонах, а також відеозв'язок, голосові та відеоповідомлення. Тлумачачи поняття

«кореспонденція», вітчизняні науковці, поряд з листуванням, телефонними розмовами та телеграфною кореспонденцією, говорять про повідомлення, зроблені по телетайпу, телефаксу, за допомогою пейджингового зв'язку, електронної пошти (електронні листи та інші повідомлення, які передаються через комп'ютер) [28], SMS та MMS-повідомлення [34].

Проте, найбільш неоднозначні тлумачення поняття «кореспонденція» пропонує нам національна правозастосовна практика. Зокрема, у вироку Першотравневого районного суду міста Чернівці від 29 серпня 2008 року у справі № 1-235/2008р суд визнав порушенням таємниці кореспонденції незаконний доступ до листування через програми `ja3c.exe` і `ICQ.exe`, а також через соціальну мережу «Однокласники» [19]. У більш пізніх рішеннях суди уникають подібної кваліфікації – зокрема, у вироку Рівненського міського суду Рівненської області від 13 вересня 2019 року у справі № 569/12334/19 як порушення таємниці кореспонденції було кваліфіковано лише доступ до електронної скриньки потерпілої особи, але не «крадіжку» та блокування її особистого профілю у соціальній мережі Facebook [21]. Також за статтею 163 КК України зазвичай кваліфікується незаконний доступ до даних, які стосуються мобільного телефонного зв'язку, а саме відомості 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 (наприклад, вироки Ірпінського міського суду Київської області від 20 листопада 2018 року у справі № 1-кп/367/310/2018 [18] або Придніпровського районного суду міста Черкаси від 23 березня 2017 року у справі № 711/10887/16-к [20]).

1.2. Поняття «кореспонденція»: підхід Європейського суду з прав людини

На регіональному рівні право на таємницю кореспонденції міститься у статті 8 Конвенції про захист прав людини та основоположних свобод у вигляді права на «безперервне і безперешкодне спілкування з іншими» - хоча у цьому вислові слово «кореспонденція» прямо не вжито, проте це формулювання перелічує головні його ознаки [27]. З огляду на те, що ЄСПЛ розглядає Конвенцію як живий організм, поняття «кореспонденція» у практиці суду розвивалось разом з відповідними комунікативними технологіями. Зокрема, у справі «Голдер проти Сполученого Королівства» («Golder v. the UK» від 21.02.1975) Суд визнав кореспонденцією лише «письмову кореспонденцію» [4]. Пізніше, у 1978 році, ЄСПЛ дещо розширив зміст цього поняття, включивши до нього ще й телефонні розмови (справа «Класс та інші проти ФРН» («Klass and others v. Germany» від 06.09.1978) [5]. Задовольняючи позовні вимоги пана Мелоуна, ЄСПЛ у справі «Мелоун проти Сполученого Королівства» («Malone v. The UK» від 02.08.1984) включив до змісту поняття «кореспонденція» ще й тривалість розмов, їх дати та номери абонентів [8]. Тобто, із розвитком технологій практика Європейського суду наповнювалася новими справами, які стосувалися захисту таємниці кореспонденції, а саме значення і зміст поняття «кореспонденція» поступово включав у себе все нові і нові доповнення. Пізніше ЄСПЛ включив до цього поняття електронні повідомлення та результати запитів в Інтернеті – саме ці висновки і містить рішення Європейського суду з прав людини у справі «Копленд проти Сполученого Королівства» («Copland v. the UK» від 03.07.2007). У цій справі заявниця поскаржилася на свого роботодавця, який порушував її право на таємницю кореспонденції шляхом прослуховування телефонних розмов, перегляду електронних листів та перевірки запитів у мережі Інтернет. Суд прийшов до висновку, що порушення ст. 8 ЄКПЛ все ж було, оскільки пані Копленд не була попереджена про можливість такого втручання, а також це не було закріплено юридично, шляхом поміщення у нормативні локальні акти вказівки на право роботодавця проглядати відповідну кореспонденцію [38].

Тож, розглядаючи цю справу, Суд ще більше розширив зміст поняття «кореспонденція».

Особливої уваги, на нашу думку, заслуговує також справа «Ліберт проти Франції» (*Libert v. France* від 22.02.2018). Заявник-громадянин Франції стверджував, що директор залізничної станції, на якій працював заявник, порушив його право на таємницю кореспонденції. Директор установи здійснив перевірку, у ході якої на робочому комп'ютері пана Ліберта була знайдена папка під назвою «D:/personal data», в якій знаходилася інформація порнографічного змісту. За національним законодавством Франції, якщо файли знаходяться на робочому комп'ютері, але містять позначку про приватність, то їх можна відкрити лише у випадку присутності найманого працівника, який працює за цим комп'ютером чи повідомивши його заздалегідь. Саме ці обставини і були викладені паном Лібертом у скарзі. ЄСПЛ протягом довгого періоду часу (майже 10 років) досліджував всі обставини справи, і у 2018 році нарешті виніс рішення, у якому відхилив скаргу позивача посилаючись на те, що файл не був підписаний як приватний, хоча у назві і вбачалися ознаки особистого життя [7]. Проте, виходячи із рішення суду можна зробити висновок, що файли особистого характеру, назви яких містять позначку приватності та розміщені на робочому комп'ютері, у окремих випадках можуть захищатися правом людини на таємницю кореспонденції.

Також неможливо оминати увагою справу «Барбулеску проти Румунії» («*Barbulescu v. Romania*» від 12.01.2016). Заявник у справі пан Барбулеску використав Інтернет-додаток, встановлений на робочому комп'ютері та призначений для спілкування з клієнтами, у своїх особистих цілях. За допомогою цього додатку («Yahoo Messenger») заявник у робочий час спілкувався із дружиною та братом, знаючи, що такі дії заборонені локальними нормативними актами його роботодавця. Унаслідок проведення перевірки директором установи вище назване порушення було виявлено і пан Барбулеску втратив роботу. У своїй скарзі до Європейського суду з прав

людини заявник посилався на порушення ст. 8 ЄКПЛ. Палата ЄСПЛ погодилася із рішеннями національних судів Румунії і відхилила вимоги заявника, оскільки він знав про заборону використання робочих комп'ютерів, факсів та інших приладів в особистих цілях, до того ж пан Барбулеску не зміг підтвердити, що мав необхідність порушувати це право. Проте один із суддів Палати ЄСПЛ пан Пауло Пінто де Альбукерке не погодився із такою позицією суду та висловив свою думку стосовно вирішення цієї справи. Відтак, Велика палата ЄСПЛ, дослідивши всі обставини справи, зробила висновок, що порушення статті 8 ЄКПЛ все ж мало місце, оскільки хоча працівники і знали про заборону користуватися робочим обладнанням у власних цілях, проте локальним актом не було передбачено можливість перевірки дотримання цієї норми. Тож у роботодавця не було підстав проводити таку перевірку, і, як наслідок, звільняти позивача [1]. Таким чином, ЄСПЛ також відніс спілкування у месенджерах до кореспонденції, таємниця якої охороняється статтею 8 ЄКПЛ.

Отже, аналізуючи усе вище наведене ми можемо зробити висновок, що українське законодавство регулює питання, пов'язані із захистом таємниці кореспонденції, лише фрагментарно, оскільки не закріплює ні визначення поняття «кореспонденція», ні переліку його елементів. Дослідивши вітчизняні акти можна зробити висновок, що поняття «кореспонденція» охоплює листи (у паперовому вигляді), телефонні розмови, телеграфні повідомлення, а також «інші види кореспонденції, що передаються через засоби зв'язку чи комп'ютер». Проте, що законодавець розуміє під останньою фразою є незрозумілим, адже спектр інформації і засоби її обміну через ці носії є настільки об'ємним і настільки швидко змінюються і обновляються, що виділити окреме коло складових дуже важко без уточнень законодавця.

Аналіз практики ЄСПЛ показує, що Суд виокремлює досить чітко зміст кореспонденції, до якої відносить «паперову кореспонденцію» (листи, телеграми, факсимільні повідомлення), телефонні розмови, тривалість розмов, їх дати, номери абонентів, електронні повідомлення, результати запитів в

Інтернеті, файли особистого характеру, які містять позначку приватності та знаходяться на робочому комп'ютері, а також повідомлення у Інтернет додатках (месенджерах). Це дозволяє дійти висновку, що ЄСПЛ проявляє більшу гнучкість, ніж вітчизняний законодавець у тлумаченні поняття «кореспонденція» і використовує переважно інструментальний підхід: кореспонденцією є все, що слугує для передачі інформації між визначеними суб'єктами.

З огляду на вище викладене, враховуючи швидкий розвиток технологій комунікації та негативний ефект від постійного внесення змін до законодавства, пропонуємо у національному праві застосувати підхід, схожий на підхід ЄСПЛ, і закріпити визначення поняття «кореспонденція» не через перелічення можливих видів кореспонденції, а через вказівку на суттєві ознаки кореспонденції: *«кореспонденцією вважається текстова, графічна, аудіовізуальна чи інші види інформації, яка передається адресно за допомогою каналів і способів, що не передбачають доступу необмеженого кола осіб»*.

РОЗДІЛ 2. ПОРЯДОК ОТРИМАННЯ ДОСТУПУ ДО КОРЕСПОНДЕНЦІЇ

2.1. Порядок отримання доступу до кореспонденції: національні законодавство та правозастосовна практика

Кожна держава встановлює норми законодавства, які дозволяють обмежувати право особи на таємницю кореспонденції, не винятком є і Україна. Проте, такі дії повинен вчиняти компетентний орган при наявності вагомих підстав, вичерпний перелік яких закріплено у законодавстві, і у суворій відповідності до встановленої законом процедури. Національне законодавство передбачає кілька порядків доступу до кореспонденції.

По-перше, отримання доступу до кореспонденції уповноваженими органами закріплено у статті 261 КПК України і належить до так званих

негласних слідчих (розшукових) дій (НСРД). Першим кроком для доступу до кореспонденції особи є звернення прокурора чи слідчого за погодженням з прокурором до слідчого судді апеляційного суду, який є гарантом дотримання прав і свобод людини і громадянина на етапі досудового розслідування, з клопотанням про дозвіл на втручання у приватне спілкування, і отримання на це ухвали (частини 1,2 статті 258 КПК України) [31].

Підставою для отримання доступу до кореспонденції є неможливість отримати відомості про злочин або особу, яка його вчинила, у інший спосіб. До того ж, таке втручання у приватність можливе лише при розслідуванні злочинів, які належать до категорії тяжких та особливо тяжких (ч. 2 ст. 246 КПК України). Проте, законодавець передбачає виключні випадки, коли уповноважені органи мають право вчиняти НСРД до отримання дозволу слідчим суддею. До таких невідкладних випадків належать ситуації, пов'язані з порятунком людських життів, а також здійснення цих дій як превентивних заходів, тобто з метою запобігання неправомірним діям. Але на здійснення НСРД у виключних випадках також потрібен письмовий дозвіл прокурора чи слідчого за погодженням з прокурором. До того ж, при виникненні таких ситуацій, прокурор зобов'язаний першочергово після початку вчинення негласних слідчих (розшукових) дій звернутися до слідчого судді для отримання відповідної ухвали, і у разі незгоди судді із таким рішенням, ці дії повинні бути негайно припинені (стаття 250 КПК України) [31; 35]. Загалом, національне законодавство закріплює порядок здійснення негласних слідчих (розшукових) дій, до яких належить і отримання доступу до кореспонденції. Важливо пам'ятати, що дотримання процедури є дуже важливим моментом на етапі досудового розслідування, адже у разі її порушення спрацьовує принцип «плодів гнилого дерева», який засвідчує, що всі докази, здобуті незаконним шляхом, не беруться до уваги суду.

Прослідкуємо етапи доступу до кореспонденції відповідно до національного законодавства. Перш за все, перед таким обмеженням приватності особи слідчий повинен накласти арешт на кореспонденцію. Про

такі наміри агента держави особа може бути попереджена або не попереджена. У останньому випадку ці дії належать до НСРД, порядок вчинення яких описаний вище. Вичерпний перелік кореспонденції, на яку може бути накладено арешт, наведено у частині 4 статті 261 КПК України: «листи усіх видів, бандеролі, посилки, поштові контейнери, перекази, телеграми, інші матеріальні носії передання інформації між особами». Вітчизняні науковці вказують, що до цього переліку мають належати листи, поштові картки, бандеролі, секограми, дрібні пакети, міжнародні відправлення з оголошеною цінністю, посилки, прямі поштові контейнери, мішок «М», відправлення «EMS» [33].

Аналізуючи формулювання «матеріальні носії передання інформації» та «поштово-телеграфна кореспонденція», які наведено у частині 2 цієї ж статті, ми можемо дійти висновку, що ця норма не може поширюватися на засоби зв'язку та електронну комунікацію, хоча й містить згадку про листи усіх видів (можливо навіть електронні) [31].

Після накладення арешту на кореспонденцію, слідчий має право здійснити її огляд і виїмку, а відповідно і дослідження. Згідно з частиною 1 статті 262 КПК України «огляд затриманої кореспонденції проводиться в установі зв'язку, якій доручено здійснювати контроль і затримувати цю кореспонденцію, за участю представника цієї установи, а за необхідності - за участю спеціаліста. У присутності зазначених осіб слідчий вирішує питання про відкриття і оглядає затриману кореспонденцію». Про кожен випадок проведення огляду, виїмки або затримання кореспонденції складається протокол, у якому обов'язково зазначається, які саме відправлення були оглянуті, що з них вилучено і що має бути доставлено адресату або тимчасово затримано, з яких відправлень знято копії чи отримано зразки (частина 4 статті 262 КПК України) [31]. Проте, як зазначалося, вказаний вище порядок стосується лише так званої «поштово-телеграфної кореспонденції» і не може поширюватись на інші види кореспонденції.

Також кримінально-процесуальним законом передбачено зняття інформації з електронних інформаційних систем (стаття 264 КПК України) та транспортних телекомунікаційних мереж (стаття 263 КПК України) [31]. При цьому, телекомунікаційна мережа - це комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням (стаття 1 ЗУ «Про телекомунікації») [26]; визначення поняття «електронна інформаційна система» національне законодавство не містить.

Аналіз судової практики показує, що під зняттям інформації з транспортних телекомунікаційних мереж зазвичай розуміють спостереження, відбір та фіксацію змісту телефонних розмов, іншої інформації та сигналів (SMS, MMS), які передаються телефонним каналом зв'язку (наприклад, ухвала слідчого судді Апеляційного суду Харківської області від 24 березня 2016 року у кримінальному провадженні № 42015220000000329 [41] чи ухвала слідчого судді Апеляційного суду Сумської області від 21 липня 2015 року у кримінальному провадженні № 12014200100000150 [40]).

При цьому, під зняттям інформації з електронних інформаційних систем розуміють: 1) отримання від провайдерів зв'язку інформації про тип з'єднання (вхідні, вихідні дзвінки, SMS, MMS) в тому числі з'єднання нульової тривалості, дату, час та тривалість з'єднання, IMEI телефона, адресу розташування базової станції, ідентифікаційні ознаки терміналу, з яким відбувається сеанс зв'язку за конкретним номером абонента мобільного зв'язку (ухвала слідчого судді Олевського районного суду Житомирської області від 12 червня 2015 року у кримінальному провадженні № 12015060260000306 [43]); 2) отримання інформації з жорстких дисків s/n zza4wf28 та s/n c 20bg9jf108535, на які накладено арешт (ухвала слідчого судді Малиновського районного суду м. Одеси від 07 серпня 2017 року у кримінальному провадженні №32017160020000004 [42]); 3) отримання усіх

наявних в електронних поштовій скриньці та видалених електронних листів разом із прикріпленими (приєднаними) файлами в період з 01 січня 2013 року по дату відправлення чи отримання останнього електронного листа, інформації щодо IP-адрес відправників та одержувачів таких листів, дати та часу отримання та відправки пошти із зазначенням IP-адрес, з яких проводиться доступ до вказаних електронних поштових скриньок (ухвала слідчого судді Тернопільського міськрайонного суду Тернопільської області від 15 травня 2018 року у кримінальному провадженні №12017210010003595 [44]) тощо.

По-друге, законодавець передбачив ще одну процедуру, яка дозволяє отримати доступ до деяких видів кореспонденції: тимчасовий доступ до речей і документів (стаття 163 КПК України). Відповідно до статті 162 КПК України, до таких речей і документів може належати, у тому числі, особисте листування особи та інші записи особистого характеру, 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 [31]. Цей порядок є спрощеним, тому що належить не до НСРД, а до заходів забезпечення кримінального провадження. Тимчасовий доступ до електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку здійснюється шляхом зняття копії інформації, що міститься в таких електронних інформаційних системах або їх частинах, мобільних терміналах систем зв'язку, без їх вилучення. Такі заходи не можуть бути здійснені щодо продуктів обміну інформацією між клієнтом та його адвокатом, або будь-якої особою, яка представляє клієнта, якщо дані повідомлення містять інформацію, яка пов'язана із наданням правової допомоги та здійсненням представництва [31].

Закон автоматично надає право працівникам пенітенціарних закладів здійснювати перевірку кореспонденції осіб, узятих під варту та засуджених, а для можливості листування потрібен дозвіл уповноважених органів (для осіб, узятих під варту, це особа або орган, що здійснює кримінальне провадження,

а для ув'язнених - адміністрація закладу, де вони перебувають). Проте є винятки і у цьому правилі, які стосуються обох категорій осіб. Саме до таких винятків і належить кореспонденція, яку адресують та одержують від омбудсмана, ЄСПЛ, а також інших відповідних органів міжнародних організацій, членом або учасником яких є Україна, уповноважених осіб таких міжнародних організацій, прокурора а також адвоката у кримінальному провадженні [24; 32].

2.2. Порядок доступу до кореспонденції: підхід Європейського суду з прав людини

Звертаючись до практики ЄСПЛ щодо отримання законного доступу до кореспонденції, варто вказати на таку резонансну справу як «Роман Захаров проти Російської Федерації» («Roman Zakharov v. Russia» від 04.12.15). Заявник – правозахисник Роман Захаров не погоджувався із нормами, які були занесені до Законів РФ «Про оперативно-розшукову діяльність», «Про Федеральну службу безпеки», «Про зв'язок» та низки наказів Міністерства зв'язку РФ, які передбачали, що уповноважені органи мають право, не отримавши дозволу суду, перехоплювати дзвінки та читати повідомлення будь-якого громадянина. Заявник стверджував, що ці норми суперечать статті 8 ЄКПЛ. При розгляді справи у ЄСПЛ уряд держави-відповідача заявив, що пан Захаров не обов'язково зазнав такого впливу від уповноважених органів, оскільки у нього немає доказів, що конкретно його телефонні розмови і повідомлення були перехоплені. Проте Європейський суд із такою позицією уряду не погодився, стверджуючи, що навіть саме існування такого законодавства порушує право людини на приватність (таємницю кореспонденції). Суд погодився, що агентами держави можуть застосовувати таємні заходи спостереження, проте для цього він запропонував чітко-визначений, вичерпний перелік мінімальних гарантій, які повинні бути закріплені у законі: 1) визначення характеру злочинів, які можуть призвести

до наказу про перехоплення; 2) визначення категорій осіб, чиї телефони можуть прослуховуватися; 3) обмеження тривалості прослуховування телефону; 4) процедура, якої необхідно дотримуватися для вивчення, використання і зберігання отриманих даних; 5) заходи обережності, яких необхідно дотримуватися при переданні даних іншим сторонам; 6) обставини, за яких записи можуть або мають бути знищені [9].

На наш погляд, Європейський суд з прав людини урівноважив такими критеріями інтереси особи стосовно зберігання її приватності та інтереси держави у сфері здійснення оперативно-розшукової діяльності.

Особливо цікавою когортою справ, які стосуються захисту таємниці кореспонденції, є справи, де заявниками є адвокати, адже у такому випадку здійснюється посягання як на приватність адвоката та його клієнтів, так і на право на справедливий суд. Зокрема, у справі «Копп проти Швейцарії» («Korpp v. Switzerland» від 25.03.1998) заявник був адвокатом і працював у юридичній конторі, а його дружина була членом уряду. Подружжя було звинувачено у тому, що пані Копп передавала інформацію, яка була секретною, а пан Копп, у свою чергу, використовував її для захисту своїх клієнтів у суді. Національний суд видав дозвіл на прослуховування телефонних розмов юридичної контори, де працював заявник, проте із умовою «ігнорувати» дзвінки, які ведуться між адвокатом та клієнтом і становлять адвокатську таємницю. Європейський суд з прав людини у своєму рішенні погодився із можливістю такого втручання у випадках та відповідно до процедур, визначених національним законодавством. Проте ЄСПЛ наголосив на відсутності визначення особи, яка повинна розмежовувати дзвінки між адвокатом-клієнтом та дзвінки, які становили сторонню юридичну консультацію. У випадку із паном Коппом це здійснював працівник юридичного відділу пошти, без здійснення контролю незалежним суддею, саме тому ЄСПЛ визнав таку ситуацію втручанням у приватне життя та підтвердив наявність порушення статті 8 ЄКПЛ [6].

У справах щодо України ЄСПЛ вказував на недосконалість національного законодавства щодо забезпечення таємниці кореспонденції. Зокрема, у справі «Беляєв та Дігтяр проти України» («Belyaev and Digtyar v. Ukraine», 16.05.2012 року) листи заявників до ЄСПЛ, які вони надсилали, перебуваючи у пенітенціарних закладах, були прочитані працівниками канцелярії та не надіслані. Суд зазначив, що національне законодавство з цього питання не відповідало стандарту якості для такого закону. Суд також наголосив, що відсутність достатніх гарантій у цій сфері могла мати наслідком свавільні відмови відсилати деякі листи заявників, як вони стверджували, а отже мало місце порушення статті 8 Конвенції щодо обох заявників стосовно їхнього права на кореспонденцію протягом попереднього ув'язнення [2].

У справі «Віслогузов проти України» («Visloguzov v. Ukraine», 20.05.2010 року) від імені заявника, який відбував покарання у місцях несвободи, з ЄСПЛ листувалась його дружина. Під час одного із побачень вона віддала листа з Суду чоловіку. До останнього було застосовано покарання за порушення порядку відправлення кореспонденції у вигляді поміщення в карцер на п'ятнадцять днів, а лист вилучено. Оцінюючи матеріали справи, Суд дійшов висновку, що не було причин, які змушували б національні органи влади утримувати адресований заявникові лист після його перевірки. З огляду на це, Суд вказав, що органи влади вийшли за межі наданої їм свободи розсуду в цій справі і що таке втручання не було пропорційним і необхідним у демократичному суспільстві. Таким чином, мало місце порушення статті 8 Конвенції [10].

У справі «Волохи проти України» («Volkhy v. Ukraine», 02.11.2006 року) на кореспонденцію заявників було накладено арешт у ході розслідування кримінального провадження щодо них. Згодом кримінальне провадження було закрито, але заявники не змогли отримати компенсації за втручання в їх приватність. Суд зауважив, що вимоги «пропорційності» втручання, його винятковий та тимчасовий характер були передбачені у статті 31 Конституції та статті 9 Закону України «Про оперативно-розшукову діяльність» від 18

лютого 1992 року, проте ні стаття 187 Кримінально-процесуального кодексу у редакції, яка була чинна під час подій, які розглядаються, ні жодне інше положення законодавства не передбачали механізм, який міг би гарантувати дотримання вищезазначених принципів на практиці. Зокрема, не було вказівки щодо осіб, до яких застосовуються ці заходи, обставин, за яких вони вживаються, та строків, які мають встановлюватись та дотримуватись. Таким чином, положення КПК України щодо арешту кореспонденції не могло бути визнане таким, що є достатньо чітким та детальним, щоб забезпечити відповідний захист від неналежного втручання органів державної влади у право заявників на повагу до їх приватного життя та кореспонденції [11]. Відтак, ЄСПЛ дійшов висновку, що втручання у приватність заявників не може розглядатися як таке, що було здійснене «згідно із законом», оскільки законодавство України не визначало з достатньою чіткістю межі та умови здійснення органами влади своїх дискреційних повноважень у сфері, про яку йдеться, та не передбачало достатніх гарантій захисту від свавілля при застосуванні таких заходів спостереження.

Відтак, ЄСПЛ встановив певний стандарт втручання у право на таємницю кореспонденції. Зокрема, таке втручання має здійснюватись згідно з законом, який відповідає вимогам щодо якості (є доступним, його положення є чіткими і зрозумілими, застосовуються послідовно). Крім того, втручання має переслідувати легітимну мету та бути пропорційним. Пропорційність втручання визначається з огляду на існування реальної можливості оскаржити втручання, на відповідність між тяжкістю ймовірно вчиненого правопорушення та тяжкістю втручання, на необхідність періодичного перегляду санкціонування втручання тощо.

Підсумовуючи викладене у цьому розділі, зазначимо, що переважна частина недоліків національного законодавства, на які вказував ЄСПЛ у справах щодо України, були виправлені з ухваленням нового Кримінального процесуального кодексу. Тим не менш, окремі питання, на нашу думку, все ще залишаються не вирішеними. До таких, належать, зокрема, реальне

розмежування випадків зняття інформації з електронних інформаційних систем та транспортних телекомунікаційних мереж – судова практика з цього приводу залишається доволі суперечливою. Крім того, перелік складових кореспонденції є значно ширшим у кримінально-процесуальному законі, ніж у профільному законодавстві, що порушує принцип правової визначеності та право підозрюваного/обвинуваченого на приватність і на захист. Вкажемо, що лише кілька критеріїв, сформульованих ЄСПЛ у справі «Роман Захаров проти Росії», виконуються в Україні. Зокрема, національне законодавство містить вказівку на характер злочинів, які можуть призвести до наказу про перехоплення; вимогу щодо обмеження тривалості прослуховування телефону; процедуру, якої необхідно дотримуватися для вивчення, використання і зберігання отриманих даних. Проте, залишаються відсутніми у законодавстві або недостатньо чітко сформульованими визначення категорій осіб, чиї телефони можуть прослуховуватися; заходи обережності, яких необхідно дотримуватися при переданні даних іншим сторонам та обставини, за яких записи можуть або мають бути знищені.

РОЗДІЛ 3. ПОРЯДОК ОТРИМАННЯ ДОСТУПУ ДО КОРЕСПОНДЕНЦІЇ У СОЦІАЛЬНИХ МЕРЕЖАХ: ПРОБЛЕМИ І ПЕРСПЕКТИВИ

У попередніх двох розділах цього дослідження ми звернулись до поняття «кореспонденція» та вивчили порядок доступу до неї. Тим не менш, проведене дослідження не дозволило нам із впевненістю відповісти на питання про те, як охороняється конфіденційність спілкування у соціальних мережах і який порядок доступу до матеріалів такого спілкування.

Кожна соціальна мережа діє на основі користувацьких угод, які закріплюють порядок їх використання. Із соціальною мережею Facebook пов'язаний наймасштабніший скандал стосовно злиття особистої інформації про користувачів, тому умови користувацької угоди цієї мережі ми розглянемо

у першу чергу. Отже, Політика використання даних Facebook, закріплює відомості про таке: 1) яку саме інформацію вони збирають; 2) як вони використовують цю інформацію; 3) яким чином інформація розповсюджується; 4) як компанії Facebook співпрацюють; 5) як саме ви можете керувати інформацією про себе та видаляти її; 6) яким чином Facebook керує даними і передає їх у рамках глобальних послуг; 7) яким чином повідомляється про зміни у політиці використання даних користувачам тощо [37].

Варто зазначити, що ця Політика поширюється не лише на Facebook, але і його Продукти, до яких відносять мобільний додаток Facebook і браузер у додатку, а також Messenger, Instagram, пристрій Portal, додаток Bonfire, додаток Facebook Mentions, програмне забезпечення Spark AR Studio, Audience Network, додаток від NPE Team, а також будь-які інші функції, додатки, технології, програмні забезпечення, продукти і сервіси, які пропонує компанія Facebook. Проте ця соціальна мережа має деякі додатки, які не належать до її продуктів, а отже, вони мають власну політику використання даних. До таких додатків відносять Workplace, Free Basics та Messenger для дітей [39].

Досліджуючи питання порушення права на таємницю кореспонденції, у першу чергу потрібно звернути увагу на те, які відомості Facebook збирає. До такої інформації належать: 1) дані користувачів та їх дії (повідомлення та інша інформація, яку створюють користувачі під час використання Продуктів соціальної мережі); 2) інформація про контент, який публікується (мається на увазі геолокація або дата створення файлів), 3) маски та фільтри, які можна застосовувати, користуючись камерою; 4) дані про мережі та зв'язки користувачів (інформація про людей, сторінки, облікові записи, хештеги й групи, з якими взаємодіють користувачі); 5) номер кредитної або дебетової карти та інші реквізити карти, інформація щодо рахунку й автентифікації, а також платіжні реквізити, дані про відвантаження і контактна інформація у разі здійснення покупок та пожертв; 6) інформація про своїх користувачів, яку

вони отримують від інших користувачів (коментування фотографій, відправлене повідомлення або завантаження контактної інформації) [37].

Також Facebook отримує й іншу інформацію, яка стосується не соціальної мережі, а пристроїв користувача: 1) атрибути пристроїв (рівень заряду акумулятора, потужність сигналу, вільне місце для зберігання даних, тип браузера, назви й типи додатків і файлів тощо); 2) робота пристрою, за допомогою якої відрізнення людини від бота; 3) ідентифікатори (мається на увазі прив'язка Продуктів компанії Facebook до одного пристрою чи облікового запису); 4) сигнали пристроїв (сигнали Bluetooth, а також дані про близькі точки доступу до Wi-Fi та вежі мобільного зв'язку); 5) інформація щодо налаштувань пристрою; 6) мережа та підключення; 7) інформація із файлів cookie [37]. Зауважимо, що cookie – це маленькі текстові файли, які зберігаються на комп'ютері, планшеті чи мобільному телефоні. Вони не становлять загрози для вашого пристрою і коли користувач відвідує веб-сайт, ці файли допомагають веб-сайту «запам'ятати» його і його діяльність на сайті протягом кількох візитів [16].

Проте інформацію про користувачів Facebook може отримувати не лише безпосередньо від них самих, але й від своїх партнерів. Мова йде саме про те, що інтернет-магазини чи компанія, яка займається організацією інтернет-ігор, може надавати цій соціальній мережі дані чим цікавляться і як з ними взаємодіють користувачі. Тож, Facebook може збирати інформацію про користувачів навіть тоді, коли вони не користуються його послугами [37].

Відтак, можна дійти висновку, що принаймні частина інформації, яка збирається соціальною мережею, є кореспонденцією відповідно до запропонованого нами визначення (листування між користувачами, позначки про вподобання і репости, голосові повідомлення, фото і відео, які надсилаються в особистих повідомленнях тощо).

Згідно своєї Політики, Facebook надає вище перелічену інформацію таким особам: 1) партнери, які використовують послуги даної компанії з аналітики; 2) рекламодавці, яким Facebook надає інформацію про типи людей,

які реагують на їх продукцію, але не розкриває їх особисту інформацію, за допомогою якої можна розпізнати особу; 3) продавці і постачальники послуг, які підтримують бізнес соціальної мережі; 4) науковці, які отримують інформацію з метою сприяння прогресу та інновацій; 5) правоохоронні органи, яким керівництво даної компанії надає дані особистого і неособистого характеру, які вони мають про своїх користувачів, у разі наявності офіційного запиту уповноваженими органами США (ордер на обшук, судове розпорядження чи повістка), чи уповноваженим органом іншої держави. Але за таких умов компанія повинна сама погодитися, що дії її користувача були неправомірними і розголошення його даних є необхідним. На наш погляд, таке положення можна назвати навіть «дискреційним повноваженням» Facebook. Також керівництво цієї соціальної мережі може «поділитися інформацією» з метою запобігання та боротьби з шахрайством, несанкціонованим використанням Продуктів, порушенням політики та іншою шкідливою або незаконною діяльністю; для захисту своїх прав; для захисту прав інших користувачів, зокрема в рамках проведення розслідувань або запитів органів контролю, нагляду та регулювання; або для запобігання смерті чи тілесним ушкодженням [37]. Тобто перелік випадків розкриття інформації про користувачів є доволі широким.

Проте, ми не можемо бути впевнені, що Facebook та інші компанії дотримуються своїх же правил. Як приклад можна навести скандал, який виник через звинувачення згаданої соціальної мережі у тому, що буцімто компанія продавала особисті дані користувачів і використовували антиконкурентні практики. Керівництво цієї компанії заперечує усі звинувачення, проте фактами залишається те, що 14 грудня 2018 року в компанії Facebook заявили про можливий витік фото 6,8 млн користувачів, які раніше були приховані налаштуваннями приватності або неопубліковані. А 2 листопада 2018 дані 257 тисяч користувачів соцмережі були розміщені у вільному доступі в інтернеті, в тому числі приватні повідомлення понад 80 000 користувачів. Нещодавно Facebook звинуватили ще й у передачі іншим

компаніям аудіозаписів голосових повідомлень користувачів для їх розшифровки. Компанія заперечувала свою вину, але федеральна торгова комісія США все ж визнала факт витоку особистих даних користувачів і оштрафувала Facebook на п'ять мільярдів доларів [12; 14].

Відтак звернемося до такого відомого в Україні мобільного додатку як Viber. Всі дані, які пересилаються у цьому додатку, підпадають під сформульоване нами поняття «кореспонденція»: особисте листування, особисті фото, дзвінки і голосові повідомлення, опитування та малюнки. Політика конфіденційності цього месенджера закріплює, що компанія не має можливості прослуховувати телефонні розмови, а зберігання повідомлень можливо лише до прочитання його одержувачем або спливу 2 тижнів від його відправлення. Як запевняє у одному із своїх інтерв'ю Телмон Марко, засновник Viber, 80 % повідомлень видаляються швидше ніж за секунду. Щодо можливості передавання інформації із цього месенджера іншим особам, то політика конфіденційності передбачає таку можливість лише у трьох випадках: 1) згідно із нормами закону або у разі здійснення судового процесу проти компанії; 2) під час виконання підписаних угод (з метою захисту своєї власності та дотримання своїх прав); 3) наявність крайньої потреби, з метою забезпечення безпеки користувачів, громадськості чи служби месенджера [36; 15].

Тобто, спираючись на положення, закріплені у Політиці конфіденційності Viber, можна зробити висновок, що ключ шифрування може бути наданий третім особам лише у виключних випадках, про які користувачі попереджені. Але із слів Телмона Марко можна зрозуміти, що уряди деяких держав намагаються одержати ці дані застосовуючи примус. Зокрема мова йде про уряд Саудівської Аравії, який схилив дану компанію до «співпраці» у якості моніторингу повідомлень та телефонних розмов, проте керівництво Viber відмовилося. Саме тому згаданий месенджер і заблоковано у цій країні на відміну від Skype і WhatsApp, які також отримували таку «пропозицію» [15].

Політика, правила і конфіденційність месенджера WhatsApp дуже схожа із Політикою конфіденційності мобільного додатку Viber. Проте, існує декілька відмінностей: повідомлення видаляються, у разі їх не прочитання, протягом 30 днів, а також компанія має право зберігати інформацію про дату й час, пов'язану з успішно доставленими повідомленнями, а також номери мобільних телефонів, задіяних у повідомленнях, і будь-які інші дані, які WhatsApp юридично змушений збирати. Крім цього засновники компанії наголошують, що вони мають право розкривати персональну чи не персональну інформацію, якою володіють, державним правоохоронним органам у разі, якщо це передбачено законом державного чи федерального рівня, міжнародною угодою або ж при наявності постанови суду, повістки із суду, ордеру на обшук чи наявності загрози фізичної безпеки особи [15].

Як бачимо, видається, що таємниця кореспонденції у соціальних мережах і месенджерах теоретично захищена від розголошення стороннім особам, які не є агентами держави. Особа, яка не є агентом держави, може отримати доступ до такої кореспонденції лише за згодою власника сторінки. Ми вважаємо, що у випадках «злому сторінки» за такі дії має наставати кримінальна відповідальність за статтею 361 КК України: «несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації. Але, на наш погляд, варто зазначити, що максимальною санкцією за вчинення такого злочину є позбавлення волі на строк до трьох років [30].

Варто зауважити, що ЄСПЛ ще не висловив однозначної думки щодо того чи охороняється правом на таємницю кореспонденції листування у соціальній мережі. Взагалі однією із перших справ Суду, пов'язаних із інформацією у соціальних мережах, стала справа «Егіль Ейнарсон проти Ісландії» («Egill Einarsson v. Iceland» від 07.11.2017). Згадана справа мало

стосується таємниці кореспонденції чи отримання до неї доступу, лише визначаючи положення стосовно законності посту у соціальних мережах певного змісту [3]. Тим не менш, Суд у цій справі поширив правила, які стосуються приватності та свободи висловлювань на віртуальний простір і соціальні мережі. Відповідно, немає жодних підстав вважати, що правила щодо таємниці кореспонденції є незастосовними у соціальних мережах та віртуальному просторі.

Ще далі Суд пішов у згаданій вище справі «Барбулеску проти Румунії» («*Barbulescu v. Romania*» від 12.01.2016), визнавши спілкування в месенджері видом приватного спілкування. І хоча справа стосувалась звільнення заявника, саме невиправдана перевірка його кореспонденції у соціальних мережах призвела до такого результату [1].

Як бачимо, існує кілька способів розкриття інформації, яка становить таємницю кореспонденції у соціальних мережах і месенджерах, правоохоронними органами: 1) вилучення відповідних пристроїв (ПК, ноутбуків, планшетів, смартфонів), за допомогою яких здійснювався доступ до соціальної мережі/месенджера та отримання від власника відповідного пристрою коду доступу; 2) отримання інформації від відповідної компанії, яка власником месенджера/соціальної мережі на основі ухвали/ордера, виданого судом; 3) отримання інформації від компанії, яка є власником месенджера/соціальної мережі за її власною ініціативою.

З огляду на те, що переважна частина компаній-власників месенджерів і соціальних мереж є резидентами іноземних держав, останні два способи є ускладненими, у той час як перший спосіб є неприйнятним при проведенні негласних слідчих розшукових дій. Підписання Україною міжнародної угоди про правову допомогу з іншої державою, де зареєстрована компанія-власник соціальної мережі чи месенджера, для отримання доступу до листування чи телефонних розмов значно спростило б ситуацію. Проте, такі дії можуть бути допустимі лише при розслідування тяжких та особливо тяжких злочинів. Таку практику мають намір розпочати США та Велика Британія. Згідно угоди

британська поліція зможе отримати доступ до повідомлень у соціальних мережах, зареєстрованих у США, під час розслідування таких злочинів як тероризм чи педофілія. Також варто зазначити, що таких нововведень можуть зазнати користувачі таких мереж як Facebook і WhatsApp [17].

ВИСНОВКИ

Отже, підсумовуючи вищевикладене, наголосимо на такому:

1. Національне законодавство гарантує право на таємницю кореспонденції, проте стрімкий розвиток засобів комунікації призвів до того, що значна частина інформації, яка за своєю суттю становить кореспонденцію, залишилась поза правовим регулюванням. Особливо це стосується спілкування у соціальних мережах та месенджерах, які прямо не охоплюються національним законодавством. Аналіз практики ЄСПЛ з цього приводу доводить, що Суд тлумачить Конвенцію гнучко і використовує інструментальний підхід для визначення поняття «кореспонденція». З огляду на стрімкість розвитку науково-технічного прогресу у сфері комунікацій вважаємо, що нинішній підхід законодавця, який полягає у переліченні способів кореспонденції для формулювання її визначення, є недосконалим і потребує постійної ревізії законодавства. Відтак, доцільним буде закріплення єдиного визначення, побудованого на основі інструментально-суттєвого підходу. Пропонуємо частину 1 статті 163 КК України викласти у такій редакції: *«порушення таємниці кореспонденції, - караються штрафом від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або обмеженням волі до трьох років»*. Вважаємо за необхідне доповнити статтю 163 КК України приміткою такого змісту: *«кореспонденцією вважається текстова, графічна, аудіовізуальна чи інші види інформації, яка передається адресно за допомогою каналів і способів, що не передбачають доступу необмеженого кола осіб»*. Також пропонуємо частину 1 статті 306 ЦК викласти у такій редакції:

«Фізична особа має право на таємницю кореспонденції, якою вважається текстова, графічна, аудіовізуальна чи інші види інформації, яка передається адресно за допомогою каналів і способів, що не передбачають доступу необмеженого кола осіб».

2. Внести зміни до національного кримінально-процесуального законодавства, які допоможуть привести його у відповідність із практикою ЄСПЛ, зокрема визначити категорії осіб, до чиеї кореспонденції можна отримати доступ у порядку проведення негласних слідчих розшукових дій або окремо закріпити спеціальні гарантії щодо неможливості отримувати доступ до кореспонденції, якщо вона становить медичну (лікарі), нотаріальну (нотаріуси), адвокатську (адвокати) таємницю, таємницю сповіді (священнослужителі) тощо; чітко окреслити коло осіб, які можуть працювати з інформацією, яка становить таємницю кореспонденції; сформулювати порядок поводження із матеріальними носіями інформації, яка становить таємницю кореспонденції та порядок видалення/знищення такої інформації у разі, якщо обвинувальний акт щодо особи так і не було направлено до суду протягом визначеного строку або щодо особи було постановлено виправдувальний вирок.

3. Спілкування у соціальних мережах та месенджерах підпадає під визначення поняття «кореспонденція», запропонованого нами у першому розділі дослідження. Аналіз практики ЄСПЛ показує, що суд поширює правила і гарантії, встановлені Конвенцією, і на відносини у віртуальному світі, зокрема у соціальних мережах. Відповідно, немає перешкод для того, щоб охороняти кореспонденцію у соціальних мережах як і будь-які інші види кореспонденції. Користувацькі угоди Facebook, WhatsApp та Viber, які ми проаналізували, дозволяють вилучення інформації, яка становить таємницю кореспонденції, лише за наявності відповідного рішення суду. Відтак, доцільним вбачається підписання угод про правову допомогу з державами, резидентами яких є найбільш поширені в Україні соціальні мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Case of Barbulescu v. Romania. / European Court of Human Rights HUDOC. URL: <https://hudoc.echr.coe.int> (дата звернення: 09.12.2019)
2. Case of Belyaev and Digtyar v. Ukraine. European Court of Human Rights HUDOC. URL: <http://hudoc.echr.coe.int/eng?i=001-171897> (дата звернення: 09.12.2019)
3. Case of Egill Einarsson v. Iceland. European Court of Human Rights HUDOC. URL: <https://hudoc.echr.coe.int/> (дата звернення: 09.12.2019)
4. Case of Golder v. the United Kingdom. European Court of Human Rights HUDOC. URL: <https://hudoc.echr.coe.int/rus> (дата звернення: 09.12.2019)
5. Case of Klass and others v. Germany. European Court of Human Rights HUDOC. URL: <https://hudoc.echr.coe.int/rus> (дата звернення: 09.12.2019).
6. Case of Kopp v. Switzerland. European Court of Human Rights HUDOC. URL: <https://hudoc.echr.coe.int/> (дата звернення: 09.12.2019)
7. Case of Libert v. France. European Court of Human Rights HUDOC. URL: <https://hudoc.echr.coe.int/> (дата звернення: 09.12.2019).
8. Case of Malone v. the United Kingdom (Article 50). European Court of Human Rights HUDOC. URL: <https://hudoc.echr.coe.int/> (дата звернення: 09.12.2019).
9. Case of Roman Zakharov v. Russia. European Court of Human Rights HUDOC. URL: <https://hudoc.echr.coe.int/rus> (дата звернення: 09.12.2019).
10. Case of Visloguzov v. Ukraine. European Court of Human Rights HUDOC. URL: <http://hudoc.echr.coe.int/eng?i=001-172050> (дата звернення: 09.12.2019)
11. Case of Volokhy v. Ukraine. European Court of Human Rights HUDOC. URL: <http://hudoc.echr.coe.int/eng?i=001-172266> (дата звернення: 09.12.2019)
12. Facebook звинуватили в продажу особистих даних користувачів. / Кореспондент. net. URL: <https://ua.korrespondent.net/business/web/4066237->

[Facebook-zvynuvatyly-v-prodazhu-osobystykh-danykh-korystuvachiv](#) (дата звернення: 09.12.2019)

13. У 2018 інтернет-користувачів стало 4 млрд, з них понад 3 млрд користуються соцмережами — дослідження / Громадське. URL: <https://hromadske.ua/posts/u-2018-internet-koristuvachiv-stalo-4-mlrd-z-nih-ponad-3-mlrd-koristuyutsya-socmerezhami-doslidzhennya> (дата звернення: 09.12.2019)

14. Made for minds. Facebook визнав прослуховування розмов користувачів / Deutsche Welle. URL: <https://www.dw.com/uk/facebook-визнав-прослуховування-розмов-користувачів/a-50016817> (дата звернення: 10.12.2019)

15. Media Sapients. Хто може читати повідомлення у Viber та WhatsApp? / Детектор медіа. URL: https://ms.detector.media/web/cybersecurity/khto_mozhe_chitati_povidomlennya_u_viber_ta_whatsapp/ (дата звернення: 19.12.2019)

16. Regus. Правила щодо Cookie-файлів. / Regus. URL: <https://www.regus.ua/cookies>. (дата звернення: 09.12.2019)

17. Британська поліція отримає доступ до листування в Facebook і WhatsApp, – ЗМІ. / Букви. URL: <https://bykvu.com/ua/bukvy/britanskaja-policija-poluchit-dostup-k-perepiskam-v-facebook-i-whatsapp-smi/> (дата звернення: 09.12.2019)

18. Вирок Ірпінського міського суду Київської області від 20 листопада 2018 року у справі № 1-кп/367/310/2018 / Єдиний державний реєстр судових рішень. URL: <http://reyestr.court.gov.ua/Review/77955979> (дата звернення: 09.12.2019)

19. Вирок Першотравневого районного суду міста Чернівці від 29 серпня 2008 року у справі № 1-235/2008р / Єдиний державний реєстр судових рішень. URL: <http://reyestr.court.gov.ua/Review/2394418> (дата звернення: 09.12.2019)

20. Вирок Придніпровського районного суду міста Черкаси від 23 березня 2017 року у справі № 711/10887/16-к / Єдиний державний реєстр судових рішень. URL: <http://reyestr.court.gov.ua/Review/65598556> (дата звернення: 09.12.2019)

21. Вирок Рівненського міського суду Рівненської області від 13 вересня 2019 року у справі № 569/12334/19 / Єдиний державний реєстр судових рішень. URL: <http://reyestr.court.gov.ua/Review/84251500> (дата звернення: 09.12.2019)

22. Гарантії адвокатської діяльності: ЄСПЛ навів ключові рішення / Закон і Бізнес. URL: https://zib.com.ua/ua/print/131858-garantii_advokatskoi_diyalnosti_espl_naviv_klyuchovi_rishenn.html. (дата звернення: 09.12.2019)

23. Most popular social networks worldwide as of October 2019, ranked by number of active users / Statista. URL: <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/> (дата звернення: 09.12.2019).

24. Закон України «Про попереднє ув'язнення» / База «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/3352-12> (дата звернення: 09.12.2019)

25. Закон України «Про поштовий зв'язок» / База «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/2759-14> (дата звернення: 09.12.2019)

26. Закон України «Про телекомунікації» / База «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/1280-15> (дата звернення: 09.12.2019)

27. Конвенція про захист прав людини і основоположних свобод / База «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/995_004 (дата звернення: 07.12.2019)

28. Кондратов Д. Ю. Порухення таємниці кореспонденції (коментар до статті 163 КК України). *Вісник Харківського національного університету внутрішніх справ*. 2010. № 1. С. 71-79.

29. Конституція України / База «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр> (дата звернення: 09.12.2019)

30. Кримінальний кодекс України / База «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/2341-14> (дата звернення: 09.12.2019)

31. Кримінальний процесуальний кодекс України / База «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/4651-17> (дата звернення: 09.12.2019)

32. Кримінально-виконавчий кодекс України / База «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/1129-15> (дата звернення: 09.12.2019)

33. Луцик В. Накладення арешту на кореспонденцію як негласна слідча (розшукова) дія. *Юридичний вісник*. 2014. № 3. С. 232-236.

34. 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. Число 1. С. 119-125.

35. Наказ Генеральної прокуратури України, Міністерства внутрішніх справ України, Служби безпеки України, Адміністрації державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України «Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні» від 16.11.2012 № 114/1042/516/1199/936/1687/5 / База «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/v0114900-12> (дата звернення: 09.12.2019)

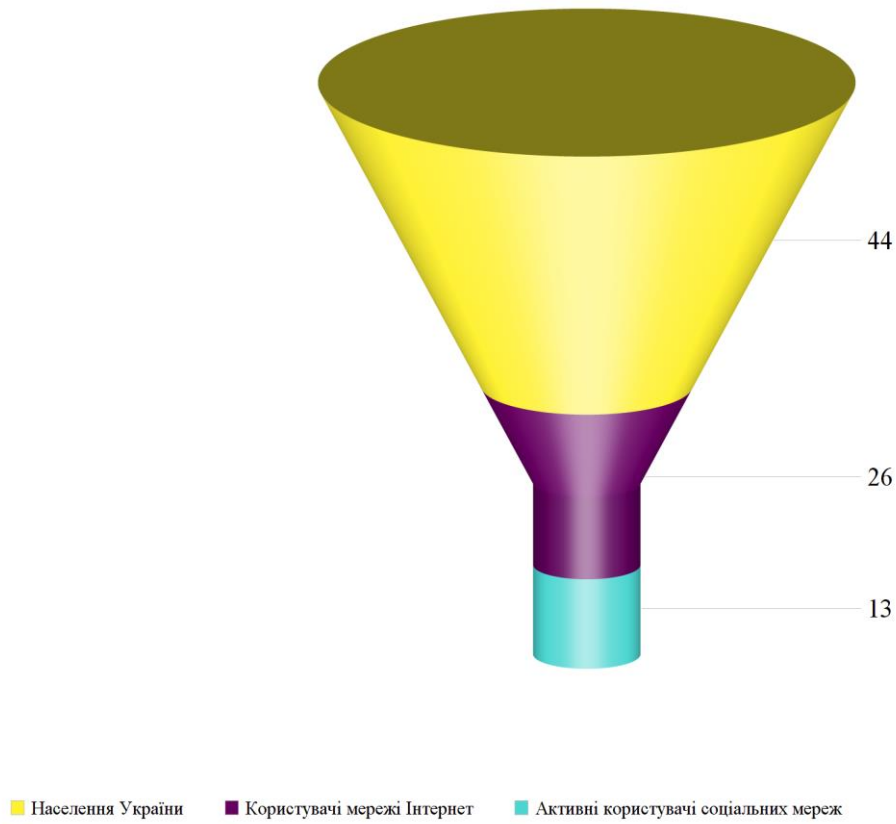
36. Политика конфиденциальности Viber. / Viber. URL: <https://www.viber.com/ru/terms/viber-privacy-policy/> (дата звернення: 09.12.2019)

37. Політика використання даних Facebook. / Facebook. URL: <https://uk-ua.facebook.com/privacy/explanation> (дата звернення: 09.12.2019)
38. Справа «Copland проти Сполученого Королівства» / European Court of Human Rights HUDOC. URL: <https://hudoc.echr.coe.int/rus> (дата звернення: 09.12.2019)
39. Справочный центр Facebook. Что такое Продукты Facebook? / Facebook. URL: https://ru-ru.facebook.com/help/1561485474074139?helpref=page_content (дата звернення: 09.12.2019)
40. Ухвала слідчого судді Апеляційного суду Сумської області від 21 липня 2015 року у кримінальному провадженні № 12014200100000150 / Єдиний державний реєстр судових рішень. URL: <http://reyestr.court.gov.ua/Review/77841093> (дата звернення: 09.12.2019)
41. Ухвала слідчого судді Апеляційного суду Харківської області від 24 березня 2016 року у кримінальному провадженні № 42015220000000329 / Єдиний державний реєстр судових рішень. URL: <http://reyestr.court.gov.ua/Review/61377244> (дата звернення: 09.12.2019)
42. Ухвала слідчого судді Малиновського районного суду м. Одеси від 07 серпня 2017 року у кримінальному провадженні №32017160020000004 / Єдиний державний реєстр судових рішень. URL: <http://reyestr.court.gov.ua/Review/69401424> (дата звернення: 09.12.2019)
43. Ухвала слідчого судді Олевського районного суду Житомирської області від 12 червня 2015 року у кримінальному провадженні № 12015060260000306 / Єдиний державний реєстр судових рішень. URL: <http://reyestr.court.gov.ua/Review/44845593> (дата звернення: 09.12.2019)
44. Ухвала слідчого судді Тернопільського міськрайонного суду Тернопільської області від 15 травня 2018 року у кримінальному провадженні №12017210010003595 / Єдиний державний реєстр судових рішень. URL: <http://reyestr.court.gov.ua/Review/74178885> (дата звернення: 09.12.2019)

45. Цивільний кодекс України / База «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/435-15> (дата звернення: 09.12.2019).

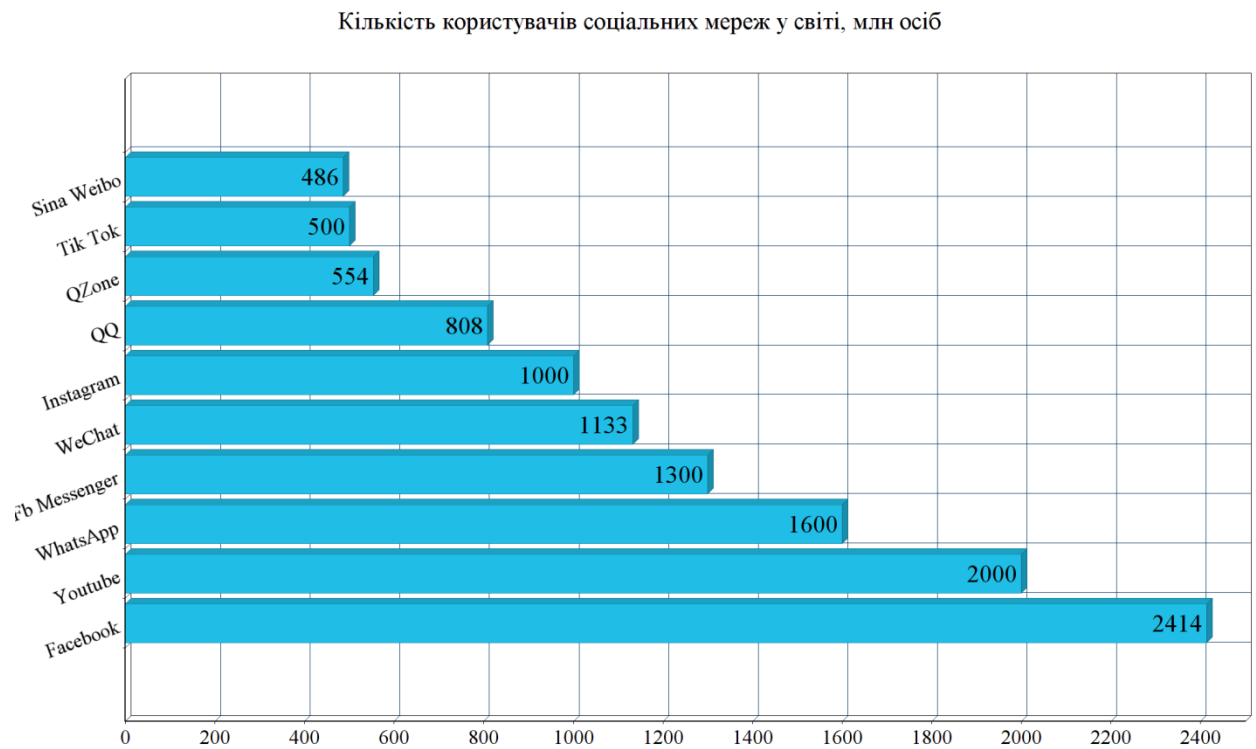
Додаток 1

Кількість користувачів соціальних мереж у порівнянні з кількістю населення України, млн осіб



Діаграма 1. Активні користувачі соціальних мереж у порівнянні з кількістю населення України станом на 2018 рік, млн. осіб

Додаток 2



Діаграма 2. Кількість користувачів 10 найбільших соціальних мереж у світі
станом на жовтень 2019, млн. осіб