

УДК 343.13:343.9(477)

DOI <https://doi.org/10.32782/ln.2025.25.58>**Філімонов М.В.***аспірант кафедри кримінального процесу
Національний університет
«Одеська юридична академія»*

НАЛЕЖНИЙ ПРОЦЕСУАЛЬНИЙ ПОРЯДОК ОЗНАЙОМЛЕННЯ ІЗ ІНФОРМАЦІЄЮ, ЩО МІСТИТЬСЯ НА ЦИФРОВИХ ПРИСТРОЯХ: ОКРЕМІ ПИТАННЯ У КОНТЕКСТІ ПРАКТИКИ ККС ВС

Стрімка цифровізація суспільних відносин та зростання ролі електронних даних у кримінальному провадженні обумовлюють актуальність доктринального осмислення належного процесуального порядку ознайомлення з інформацією, що міститься на цифрових пристроях. Мобільні телефони, комп'ютери, планшети та інші цифрові пристрої акумулюють значні обсяги особистої інформації, яка охоплює приватне життя особи, її комунікації, переміщення, професійну та сімейну діяльність. У зв'язку з цим доступ органів досудового розслідування до такої інформації неминуче пов'язаний із серйозним втручанням у право на повагу до приватного і сімейного життя, гарантоване ст. 8 Конвенції про захист прав людини і основоположних свобод.

Європейський суд з прав людини у своїх правових позиціях послідовно виходить із того, що будь-яке втручання держави у сферу приватності у цифровому середовищі повинно відповідати критеріям законності, легітимної мети, необхідності у демократичному суспільстві та пропорційності. Водночас, у національній правозастосовній практиці нерідко постають проблеми, пов'язані із відсутністю чіткого розмежування між різними процесуальними діями, у ході яких можливе ознайомлення із інформацією, що міститься на цифрових пристроях. Це призводить до невизначеності у питанні відносно коректного розмежування повноважень слідчого, прокурора та слідчого судді щодо обмеження прав осіб у кримінальному провадженні, а також

нівелювання судового контролю.

Дотримання належної правової процедури при ознайомленні з інформацією на цифрових пристроях безпосередньо впливає на допустимість отриманих доказів. Суперечливість процесуального порядку доступу до цифрових даних створює ризики свавільного втручання у приватне життя та подальшого використання таких відомостей у кримінальному провадженні. У цьому контексті формування узгоджених підходів судової практики, зокрема Касаційного кримінального суду у складі Верховного Суду (далі – ККС ВС), та їх наукове осмислення є необхідною передумовою подолання наявних правозастосовних проблем на основі забезпечення балансу між інтересами правосуддя та гарантіями прав осіб у кримінальному провадженні.

До релевантних питань у кримінальній процесуальній доктрині звертались В.С. Бондар, І.В. Гловюк, В.Г. Дрозд, В.П. Корж, К.В. Латиш, Д.В. Лісніченко, О.А. Лучко, А.В. Ратнова, В.В. Романюк, А.В. Скрипник, І.А. Смаль, М.М. Стоянов, О.О. Торбас, Т.Г. Фоміна, А.В. Шило та ін. Утім, динамічність судової практики у розглядуваному аспекті вимагає подальших наукових розвідок.

Враховуючи викладене, мета даної статті полягає у визначенні належного процесуального порядку ознайомлення із інформацією, що міститься на цифрових пристроях та формування пропозицій щодо вдосконалення окремих правозастосовних підходів у цьому аспекті.

Зазначимо, що ознайомлення із інформацією, що міститься на цифрових пристроях може відбуватися у ході низки процесуальних дій, зокрема, огляду, обшуку, тимчасового доступу до речей і документів, а також негласних слідчих (розшукових) дій (далі – НСРД). Кожна із них має різну процесуальну природу, а також різний порядок здійснення, що впливає, у тому числі на дотримання гарантій прав та свобод осіб. Це породжує правову проблему у правозастосуванні.

Одна із найбільших проблем виникає у контексті розмежування огляду та окремих НСРД, зокрема, зняття інформації з електронних інформаційних систем. У ч.2 ст. 264 КПК України встановлено, що 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. Водночас, ч.1 ст. 237 КПК України в редакції Закону України № 2137-IX від 15.03.2022 передбачає, що з метою виявлення та фіксації відомостей щодо обставин вчинення кримінального правопорушення слідчий, прокурор проводять огляд місцевості, приміщення, речей, документів та *комп'ютерних даних* (виділено мною – М.Ф.). Фактично, оновлена редакція ч.1 ст. 237 КПК України внесла ще більше непорозуміння у тому яким має бути процесуальний порядок ознайомлення із відомостями, що містяться на цифрових пристроях.

Хоча, відповідні питання виникали у правозастосовній практиці й раніше. Зокрема, ще у Постанові ККС ВС від 09 квітня 2020 року було зазначено: «Що ж стосується інформації, яка була наявна в мобільному телефоні ОСОБА_8, то вона була досліджена шляхом включення телефону та огляду текстових повідомлень, які в ньому знаходились та доступ до яких не був пов'язаний із наданням володільцем відповідного серверу (оператором мобільного зв'язку) доступу до електронних інформаційних систем. В даному випадку

орган досудового розслідування провів огляд предмета телефона та оформив його відповідним протоколом, який складений з дотриманням вимог кримінального процесуального закону».

За таких обставин Суд не вбачає жодних порушень вимог кримінального процесуального закону при розгляді даного кримінального провадження» [1].

У інших позиціях, ККС ВС при оцінці допустимості відповідних доказів звертав увагу, зокрема, на добровільність надання цифрових пристроїв. До прикладу, у Постанові ККС ВС від 22 лютого 2024 року Суд дійшов такого висновку: «Що ж стосується інформації, яка була наявна в мобільному телефоні ОСОБА_7, то вона була досліджена шляхом включення телефону та огляду фотографій і текстових повідомлень, які в ньому знаходились та доступ до яких був наданий власником добровільно. При цьому ОСОБА_7 добровільно коментував наявну інформацію. В даному випадку орган досудового розслідування провів огляд предмета - телефона та оформив його відповідним протоколом, який складений з дотриманням вимог кримінального процесуального закону» [2].

Фактично, із даної правової позиції суду касаційної інстанції випливає, що добровільне надання телефону автоматично означає відсутність факту проведення НСРД, а релевантною процесуальною дією, спрямованою на фіксацію відомостей, які знаходяться у телефоні є саме огляд.

Ця позиція знаходить відображення і у інших рішеннях ККС ВС. Зокрема, у Постанові ККС ВС від 13 березня 2024 року в контексті оцінки допустимості як доказів аудіофайлів, вилучених з мобільного телефону, суд вказав, що «таємниця виключається, якщо абонент (учасник) спілкування не бажає її зберігати і добровільно розкриває, зокрема, перед державними органами. За таких обставин не відбувається втручання у спілкування, а відбувається фіксація добровільно розкритої інформації, яка втрачає статус таєм-

ниці й набуває статусу відкритості. Доказом у цьому кримінальному провадженні є аудіо-файли, вилучені з телефону самого засудженого, який він безпосередньо надав органу досудового розслідування та які надалі були предметом дослідження експертом та безпосередньо судом» [3].

Така позиція видається загалом обґрунтованою та такою, що відповідає сучасному розумінню меж права на приватність і стандартам допустимості доказів у кримінальному провадженні. Ключовий акцент ККС ВС робить на добровільності розкриття інформації самою особою, яка була безпосереднім учасником відповідного спілкування та є власником цифрового пристрою. За таких обставин, ознаки прихованого або примусового втручання представників держави у сферу приватного життя, що є визначальним критерієм правомірності обмеження права на приватність відповідно до статті 8 Конвенції відсутні.

Не виникають у цьому контексті і питання щодо обсягу наданої інформації. Очевидно, що особі слід усвідомлювати, що у випадку надання дозволу на ознайомлення зі змістом інформації, яка міститься на цифровому пристрої, вона не матиме змогу контролювати те, в якому обсязі і яка саме інформація буде розкрита.

Проте питання щодо належної правової процедури ознайомлення з інформацією, що міститься на цифрових пристроях виникала також і у випадках, коли мало вилучення відповідного пристрою мало примусовий характер. До прикладу, у Постанові ККС ВС від 09 квітня 2024 року Суд виснував, що «огляд інформації, що міститься в телефоні, не становить собою негласне втручання у приватне спілкування, передбачене § 2 Глави 21 КПК, і доступ до інформації, що містилася в ньому не вимагає отримання окремого дозволу у порядку, визначеному тимчасовим доступом до речей і документів, що регулюється Главою 15 КПК, якщо сторона обвинувачення отримала телефон підозрюваного в своє володіння на підставі законно проведеного

обшуку, обставини якого не дають підстав для визнання цього телефону недопустимим доказом» [4].

Зазначимо, що ч.6 ст. 236 КПК України в редакції Закону України № 2137-IX від 15.03.2022 передбачає, що якщо під час обшуку слідчий, прокурор виявив доступ чи можливість доступу до комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, для виявлення яких не надано дозвіл на проведення обшуку, але щодо яких є достатні підстави вважати, що інформація, що на них міститься, має значення для встановлення обставин у кримінальному провадженні, прокурор, слідчий має право здійснити пошук, виявлення та фіксацію комп'ютерних даних, що на них міститься, на місці проведення обшуку.

Погодитись із такою регламентацією дещо складно, адже фактично мова йде про потенційну можливість втручання у приватне спілкування. Крім того, питання виникають й щодо якості закону. Не зовсім зрозумілим з цієї точки зору є формулювання «виявив доступ чи можливість доступу». Очевидно, мова йде про ситуацію, коли вони не захищені паролем чи іншою логічною системою захисту, однак, потенційно такий процесуальний порядок відкриває можливість до непропорційних зловживань.

Однак в цьому контексті теж виникає низка питань. По-перше, відповідна норма не є застосовною в контексті особистого обшуку особи в ході затримання. Нормативна модель цієї процесуальної дії лишається вкрай лаконічною та недеталізованою.

Що ж стосується огляду житла та іншого володіння особи, ситуація дещо інша. На відповідну слідчу (розшукову) дію поширюється процесуальний порядок обшуку житла або іншого володіння особи. Крім того, у ч.2 ст. 237 КПК України також міститься положення про те, що огляд комп'ютерних даних проводиться слідчим, прокурором шляхом відображення у протоколі огляду інформації, яку вони містять, у формі, придатній для сприйняття їх

змісту (за допомогою електронних засобів, фотозйомки, відеозапису, зйомки та/або відеозапису екрана тощо або у паперовій формі). Однак, огляд житла або іншого володіння особи, на відміну, від обшуку, за усталеною практикою ККС ВС може бути здійснено й на підставі добровільної згоди особи. А відтак, у випадку вилучення мобільного телефону чи іншого пристрою під час огляду, відповідне втручання у приватне спілкування здійснюватиметься без судового рішення. У такому випадку можливий лише подальший судовий контроль, що не відповідає у цьому випадку загальним засадам втручання у приватне спілкування, визначеним у КПК України.

Слід зауважити, що питання допустимості огляду мобільного телефону, вилученого у ході обшуку неодноразово поставало у юридичній доктрині. О.О. Торбас вважає, що після вилучення мобільного телефону слідчий або прокурор зобов'язані звернутися до слідчого судді з клопотанням про тимчасовий доступ до речей і документів, а саме – до мобільного телефону, в якому міститься охоронювана законом таємниця. Будь-які інші форми доступу до мобільного телефону задля ознайомлення з текстом повідомлень слід вважати незаконними [5, с. 309].

Про правомірність огляду цифрової інформації у вилучених під час обшуку затриманої особи пристроях виключно на підставі ухвали слідчого судді про тимчасовий доступ до речей і документів веде мову й А.В. Скрипник. На думку науковця, без судового рішення можуть вчинятися виключно ті дії, що спрямовані на: а) огляд зовнішнього вигляду; б) підтримку працездатності пристрою (наприклад, підключення зарядного пристрою); в) унеможливлення знищення інформації до отримання дозволу на ознайомлення з нею (наприклад, застосування екрану (клітки, щиту) Фарадея) [6].

Іншу позицію щодо належної процесуальної форми огляду вмісту інформації мобільного телефону відстоює М.І. Пашковський. Автор зазначає, що пошук, виявлення і фіксація відомостей, що містяться в смартфоні,

отримання таких відомостей, якщо доступ до них обмежується їх власником, володільцем або утримувачем або пов'язаний з подоланням системи логічного захисту, можливі лише на підставі відповідної ухвали слідчого судді шляхом зняття інформації з електронних інформаційних систем або їх частин [7, с. 111]. Таку позицію дослідник обґрунтовує тим, що в порядку тимчасового доступу до речей і документів здійснюється доступ до мобільного терміналу систем зв'язку, який не має ознак електронної інформаційної системи. Саме в цьому він і вбачає можливість розмежування зняття інформації з електронних інформаційних систем та тимчасового доступу до речей і документів.

Ми теж погоджуємось із тією позицією, що будь-яке ознайомлення із інформацією, що міститься на цифрових пристроях, повинно підлягати перевірці слідчим суддею, що відповідає конвенційним стандартам права на приватність, передбаченим ст. 8 Конвенції. Тому у разі, якщо особа не розкриває добровільно інформацію на цифровому пристрої, а ознайомлення передбачатиме подолання логічної системи захисту, то застосовною є норма ч.1 ст. 264 КПК України.

Висновок. Аналіз чинного кримінального процесуального законодавства України та практики Касаційного кримінального суду у складі Верховного Суду свідчить про наявність суперечливих підходів до визначення процесуальної форми доступу до цифрових даних, зокрема у контексті розмежування огляду, тимчасового доступу до речей і документів та окремих негласних слідчих (розшукових) дій.

У випадку добровільного надання особою мобільного телефону чи іншого пристрою для ознайомлення, огляд є релевантною слідчою (розшуковою) дією, спрямованою на фіксацію відомостей, що містяться у ньому. Це відповідає стандартам забезпечення права на приватність, адже у такому разі особа усвідомлює, що вона не здатна контролювати обсяг розкриття.

Норма ч.6 ст. 236 КПК України у частині формулювання такої підстави як «виявив доступ чи можливість доступу до комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку» підлягає корегуванню, оскільки не відповідає вимозі передбачуваності закону та відкриває простір для зловживань з боку сторони обвинувачення.

Ми поділяємо підхід, відповідно до якого будь-який доступ до інформації, яка зберігається на цифрових пристроях, має здійсню-

ватися за умови перевірки слідчим суддею правомірності такого втручання, що узгоджується з конвенційними стандартами захисту права на приватність, закріпленими у статті 8 Конвенції. Таким чином, у випадках, коли власник цифрового пристрою не надає добровільної згоди на розкриття інформації, а ознайомлення з її змістом потребує подолання логічних засобів захисту, застосовним має бути порядок, передбачений ч.1 ст. 264 КПК України.

Анотація

Стаття присвячена аналізу проблем належного процесуального порядку ознайомлення з інформацією, що міститься на цифрових пристроях, у кримінальному провадженні з урахуванням стандартів захисту права на приватність, гарантованого статтею 8 Конвенції про захист прав людини і основоположних свобод. Актуальність дослідження обумовлена стрімкою цифровізацією суспільних відносин, зростанням доказового значення електронних даних та підвищеними ризиками свавільного втручання органів досудового розслідування у сферу приватного життя особи.

Досліджено чинне кримінальне процесуальне законодавство України, зокрема положення статей 236, 237 та 264 КПК України, а також їх співвідношення у контексті доступу до цифрових даних. Проаналізовано процесуальну природу огляду, обшуку, тимчасового доступу до речей і документів та окремих негласних слідчих (розшукових) дій як процесуальних дій, спрямованих на ознайомлення з інформацією, що зберігається на цифрових пристроях. Окрему увагу приділено проблемі розмежування цих процесуальних дій та його впливу на допустимість доказів.

Автор зазначає, що практика Касаційного кримінального суду у складі Верховного Суду демонструє тенденцію до визнання допустимим огляду цифрових пристроїв у випадку їх добровільного надання власником, за відсутності ознак примусового чи прихованого втручання у приватне спілкування. Водночас критично оцінюється нормативна конструкція ч. 6 ст. 236 КПК України, яка через недостатню визначеність створює потенційні передумови для непропорційного обмеження права особи на приватність та нівелювання судового контролю.

Сформульовано висновок про те, що будь-яке ознайомлення з інформацією, яка міститься на цифрових пристроях, у разі відсутності добровільної згоди власника та необхідності подолання логічних засобів захисту, має здійснюватися виключно за процедурою, яка передбачає перевірку правомірності втручання слідчим суддею, зокрема у порядку, визначеному ч. 1 ст. 264 КПК України, як такому, що найбільшою мірою відповідає конвенційним стандартам захисту права на приватність.

Ключові слова: кримінальне провадження, докази, кримінальне процесуальне доказування, електронні докази, слідчі (розшукові) дії, негласні слідчі (розшукові) дії, обшук, огляд, судовий контроль.

Filimonov M.V. The proper procedural framework for accessing information stored on digital devices: selected issues in the context of the case law of the Criminal cassation court of the Supreme Court.

Summary

The article is devoted to the analysis of the problems related to the proper procedural framework for accessing information stored on digital devices in criminal proceedings, taking into account the standards

for the protection of the right to privacy guaranteed by Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms. The relevance of the study is обусловлена the rapid digitalisation of social relations, the growing evidentiary value of electronic data, and the increasing risks of arbitrary interference by pre-trial investigation authorities in an individual's private life.

The study examines the current criminal procedural legislation of Ukraine, in particular the provisions of Articles 236, 237, and 264 of the Criminal Procedure Code of Ukraine, as well as their correlation in the context of access to digital data. The procedural nature of inspection, search, temporary access to items and documents, and certain covert investigative (search) actions as procedural measures aimed at accessing information stored on digital devices is analysed. Special attention is paid to the problem of distinguishing between these procedural actions and to the impact of such differentiation on the admissibility of evidence.

The author notes that the case law of the Criminal Cassation Court within the Supreme Court demonstrates a tendency to recognise the admissibility of inspecting digital devices where they are voluntarily provided by the owner, in the absence of elements of coercive or covert interference with private communications. At the same time, the regulatory construction of part 6 of Article 236 of the Criminal Procedure Code of Ukraine is critically assessed, as its insufficient clarity creates potential prerequisites for disproportionate interference with the individual's right to privacy and the erosion of judicial control.

It is concluded that any access to information stored on digital devices, in the absence of the owner's voluntary consent and where overcoming logical security measures is required, must be carried out exclusively under a procedure that provides for prior judicial review of the lawfulness of such interference by an investigating judge, in particular in accordance with part 1 of Article 264 of the Criminal Procedure Code of Ukraine, as the procedure that most fully complies with the Convention standards for the protection of the right to privacy.

Key words: criminal proceedings, evidence, criminal procedural proof, electronic evidence, investigative (search) actions, covert investigative (search) actions, search, inspection, judicial control.

Список використаних джерел:

1. Постанова Верховного Суду від 09 квітня 2020 року, судова справа № 727/6578/17. URL: <https://reyestr.court.gov.ua/Review/88749345>
2. Постанова Верховного Суду від 22 лютого 2024 року, судова справа № 208/3704/22. URL: <https://reyestr.court.gov.ua/Review/117277325>
3. Постанова Верховного Суду від 13 березня 2024 року, судова справа № 953/3558/22. URL: <https://reyestr.court.gov.ua/Review/117757857>
4. Постанова Верховного Суду від 09 квітня 2024 року, судова справа № 369/4929/19. URL: <https://reyestr.court.gov.ua/Review/118465118>
5. Торбас О. Оцінка законності огляду телефону, який було вилучено під час обшуку. Теоретико-прикладні проблеми правового регулювання в Україні : матеріали V Всеукраїнської науково-практичної конференції (м. Львів, 10 грудня 2021 р.) / за заг. ред. І. В. Красницького. Львів : Львівський державний університет внутрішніх справ, 2021. С. 306-310. С. 309.
6. Скрипник А.В. Окремі цифрові аспекти обшуку затриманої особи. URL: <https://conf.ztu.edu.ua/wp-content/uploads/2021/10/149.pdf>
7. Пашковський М.І. Про колізійність приписів щодо процесуальної форми доступу до змісту відомостей, що містяться в мобільних терміналах систем зв'язку. Процесуальне та криміналістичне забезпечення досудового розслідування: тези доповідей учасників науково-практичного семінару (26 листопада 2021 року) / упор. А.Я. Хитра. Львів: ЛьвДУВС. 2021.С. 108-111. С. 111.