УДК 343.13

Шило А.В.
здобувач кафедри кримінального процесу
Національний юридичний університет імені Ярослава Мудрого,
оперативний співробітник
Служба безпеки України

ОТРИМАННЯ ІНФОРМАЦІЇ З ВИЛУЧЕНОЇ ЕЛЕКТРОННОЇ ТЕХНІКИ ЯК СПОСІБ ЗБИРАННЯ ДОКАЗІВ: СПІРНІ ПИТАННЯ ПРАКТИЧНОГО ПРАВОЗАСТОСУВАННЯ

Постановка проблеми. Інформація, яка міститься на вилучених у ході процесуальних дій (обшуків, затримань) електронних пристроях (персональних комп'ютерах, ноутбуках, смартфонах, телефонах тощо) не може ототожнюватися із самим електронним пристроєм як її фізичним носієм. Така інформація є окремим об'єктом права власності й об'єктом охорони таємниці приватного життя, а отже, її вилучення/копіювання має відбуватися на підставі судового рішення, проте не в режимі застосування негласних слідчих (розшукових) дій (далі – НСРД). Отримання та фіксування такої інформації має здійснюватися на підставі ухвали слідчого судді про тимчасовий доступ до речей і документів (у цьому разі – документів, що існують в електронній формі).

Огляд останніх досліджень і публікацій. Насамперед зауважимо, що аналіз судової практики дає можливість виділити три підходи до вирішення ситуації з ознайомленням і фіксацією інформації, що міститься на вилученій електронній техніці. При цьому складність ситуації полягає в тому, що щодо кожного зі способів можна знайти як аргументи за, так і аргументи проти його відповідності букві й духу кримінального процесуального закону.

Формулювання завдання дослідження. Зважаючи на сучасний рівень комп'ютеризації суспільних відносин, нині левова частка інформації зберігається на електронних носіях або на віддалених серверах із використанням так званих «хмарних технологій»[1]. При цьому вказана характеристика сучасного світу перебуває в постійній позитивній динаміці, а отже, не може не враховуватися під час збирання інформації в рамках досудового розслідування. У цьому ключі досить гостро як із позиції теорії доказового права, так і з погляду його прикладного застосування постала проблема правильного процесуального оформлення дії, яка полягає в огляді та фіксації електронної інформації, що міститься на вилучених у межах інших процесуальних дій (затримання, обшуку) електронних носіях (персональних комп'ютерах, ноутбуках, смартфонах, телефонах тощо). Дослідження наявної судової практики дає можливість констатувати відсутність єдності в цьому питанні як серед слідчих і прокурорів, так і серед суддів. Досить часто під час дослідження такого роду інформації на предмет її допустимості захисниками піднімається питання про незаконне втручання в приватне спілкування (яке можливе лише в межах передбачених законом НСРД), тому суддями підтримується така позиція, що призводить до втрати стороною обвинувачення частини доказової інформації. Проте, на наше переконання, указаний підхід хоч і не позбавлений раціонального зерна, усе ж є досить спірним. Тож зупинимось детально на цьому питанні з викладенням власного бачення ситуації.

[1] Доступ до такої інформації також здійснюється через персональні електронні пристрої.

Виклад основного матеріалу. Найпоширенішим сьогодні способом процесуального оформлення дії, яка полягає в огляді та фіксації електронної інформації, що міститься на вилучених у межах інших процесуальних дій електронних пристроях, є складання слідчим протоколу огляду в порядку ст. 237 Кримінального процесуального кодексу України (далі – КПК України). При цьому, зважаючи на необхідність спеціальних знань для проведення вказаної дії, такого роду огляд проводиться із залученням спеціаліста, завдання якого полягає в тому, щоб виявити інформацію в електронному пристрої, що досить часто вимагає застосування спеціального програмного забезпечення (використовуються програми «Ufed Physical Analyzer», «Мобільний криміналіст» та інші).

Як уже зазначалося, стороною захисту досить часто ставиться питання про визнання результатів такого огляду недопустимими доказами, зважаючи на те, що мало місце втручання в приватне спілкування. При цьому судові рішення із цього питання є діаметрально протилежними. Так, деякі судді не вбачають у процедурі такого огляду ознак втручання в приватне спілкування та визнають протоколи огляду допустимими доказами. Для ілюстрації наведемо кілька прикладів.

Як зазначається у вироку Голосіївського районного суду м. Києва, «Протоколом огляду мобільного телефону «Sony (SoniEricsson)_ D5803 Xperia Z3 Compact» imei Номер_2, в якому знаходиться сім-картка російського мобільного оператора зв'язку «МТС» з абонентським номером Номер_3, на сім-картці надруковано номер: НОМЕР_4, що знаходився в користуванні громадянина Російської Федерації Особа_10, військовослужбовця за контрактом Збройних Сил Російської Федерації, (військова частина 21208), який було вилучено під час надання йому медичної допомоги в Щастинській міській лікарні, від 20.05.2015 р., згідно з яким у ході огляду й оброблення інформації, яка міститься у вказаному вище телефоні, виявлено інформацію, яка міститься в СМС-повідомленнях, у розділах «Контакти», «Зображення», «Відео», «Vk», «Viber», «Документи», яка була ретельно досліджена, переглянута, прослухана й оголошена судом і є доказом винності обвинувачених і по суті, поряд з іншими дослідженими судом доказами, спростовує їх твердження з приводу часу, мети та цілей перебування на території України. Аналізуючи докази сторони обвинувачення на предмет належності та допустимості, суд не погоджується з доводами сторони захисту про необхідність визнання їх недопустимими. Протоколи огляду, про які говорить сторона захисту, складені відповідно до вимог процесуального законодавства, і суд не знаходить підстав визнавати їх недопустимими доказами» [1].

Зарічний районний суд м. Суми, контраргументуючи позицію сторони захисту з приводу визнання протоколів огляду телефону недопустимими доказами (оскільки, на думку сторони захисту, для такого огляду слідчий мав би отримати ухвалу суду на проведення НСРД у вигляді зняття інформації з транспортних телекомунікаційних мереж), указав таке: «Вирішуючи питання про допустимість протоколів огляду телефонів Особа_2 й Особа_5, суд вважає, що посилання сторони захисту на те, що на огляд телефону слідчий повинен був отримати ухвалу суду про зняття інформації з транспортних телекомунікаційних мереж, не ґрунтуються на законі, оскільки така ухвала надається судом для зняття інформації онлайн, тобто в ході використання особою засобів комунікації, а не постфактум» [2].

Аналогічний підхід, але з більш деталізованою аргументацією знаходимо й в ухвалі Жовтневого районного суду м. Запоріжжя. Зокрема, у мотивувальній частині вказане таке: «У судовому засіданні обвинуваченим Особа_2 і його захисником адвокатом Особа_1 заявлене клопотання про визнання очевидно недопустимими доказів сторони обвинувачення, а саме протоколу огляду мобільного телефону від 21.10.2015 р., через

те, що зазначена слідча дія проводилася без ухвали слідчого судді, оскільки слідчим було вчинене втручання в приватне спілкування обвинуваченого, роздруківка змісту смс-повідомлень, вхідних і вихідних дзвінків, що може бути зроблено лише за дозволом суду. Прокурор заперечував проти задоволення клопотання обвинуваченого та зазначив, що огляд мобільних телефонів проводився значно пізніше після їх вилучення, вони оглядалися як речовий доказ на предмет виявлення інформації, яка могла стосуватися обставин учиненого злочину, і вважав, що для проведення огляду телефонів отримання якого-небудь дозволу суду не є необхідним. Вислухавши думку учасників судового процесу, перевіривши матеріали кримінального провадження, суд вважає клопотання таким, що не підлягає задоволенню, з таких підстав. <…> Згідно зі ст. 258 КПК ніхто не може зазнавати втручання в приватне спілкування без ухвали слідчого судді. Прокурор, слідчий за погодженням із прокурором зобов'язаний звернутися до слідчого судді з клопотанням про дозвіл на втручання в приватне спілкування в порядку, передбаченому ст. ст. 246, 248, 249 цього Кодексу, якщо будь-яка слідча (розшукова) дія включатиме таке втручання. Спілкуванням є передання інформації в будь-якій формі від однієї особи до іншої безпосередньо чи за допомогою засобів зв'язку будь-якого типу. Спілкування є приватним, якщо інформація передається та зберігається за таких фізичних чи юридичних умов, за яких учасники спілкування можуть розраховувати на захист інформації від втручання інших осіб. Втручанням у приватне спілкування є доступ до змісту спілкування за умов, якщо учасники спілкування мають достатні підстави вважати, що спілкування є приватним. Різновидами втручання в приватне спілкування є такі: 1) аудіо-, відеоконтроль особи; 2) арешт, огляд і виїмка кореспонденції; 3) зняття інформації з транспортних телекомунікаційних мереж; 4) зняття інформації з електронних інформаційних систем. Таким чином, зі змісту наведеної вище норми права вбачається, що втручання в приватне спілкування за дозволом суду може бути здійснене безпосередньо під час такого спілкування (телефонної розмови, надіслання смс-повідомлень). Як видно з протоколу огляду від 21.10.2015 р., огляд мобільного телефону Особа_2 проводився слідчим після спливу більше ніж одного місяця після фактичного здійснення спілкування Особа_2 з іншими особами, які мають стосунок до вчиненого ним злочину, тому інформація, отримана після огляду цього телефону, не є приватним спілкуванням і не потребує отримання дозволу суду» [3].

Натомість інші суди в аналогічних випадках прислуховуються до позиції сторони захисту з приводу того, що ознайомлення з інформацією з електронного пристрою є втручанням у приватне спілкування, і визнають протоколи огляду недопустимими доказами. Так, наприклад, Орджонікідзевський районний суд міста Маріуполя Донецької області, розглядаючи це питання, у своєму вироку вказав таке: «Список контактів внутрішньої пам'яті наданого мобільного телефону», «Журнал викликів наданого мобільного телефону», «Список СМС-повідомлень», які долучені до висновку експерта, суд розцінює як втручання в приватне спілкування, проведене без законних підстав, і не приймає як належний і допустимий доказ. <…> Відповідно до висновку експерта № 265 від 19.06.2015 р. (т. 1, с. 105–113) системний блок ПЕОМ, який був вилучений у ході обшуку квартири Адреса_2, знаходиться в технічно справному стані. Файли, фрагменти історії роботи Інтернет-браузерів, вибіркові електронні листи зі сторінки Особа_32, які долучені до висновку експерта, суд розцінює як втручання в приватне спілкування, проведене без законних підстав, і не приймає як належний і допустимий доказ» [4]. Аналогічний підхід можна знайти й в інших судових рішеннях [5; 6; 7].

При цьому показово, що у своїх рішеннях судді лише ставлять питання про втручання в приватне спілкування та необхідність отри-

мання відповідного дозволу слідчого судді на таке вручання, але не вказують на форми (види НСРД), у яких таке втручання мало б відбутися. Щоправда, усе ж можливо віднайти поодинокі судові рішення, де контекст мотивувальної частини дає можливість припустити, що йдеться про НСРД, передбачену ст. 264 КПК (зняття інформації з електронних інформаційних систем). Зокрема, про те, що саме таку НСРД суд розглядає як можливу форму втручання в приватне спілкування під час ознайомлення з інформацією, що міститься на жорсткому диску ноутбука, свідчить урахування судом факту обмеження власником доступу до інформації шляхом установлення системи логічного захисту – паролю (про це йдеться виключно в ч. 2 ст. 264 КПК). Із цього приводу у вироку Придніпровського районного суду м. Черкаси зазначено таке: «Незважаючи на те, що слідчим суддею в установленому законодавством порядку надано дозвіл на проведення обшуку з метою виявлення й вилучення в підсудного Особа_2 певних речей і документів, зокрема й магнітних носіїв інформації, ПЕОМ (т. 1, а. с. 41, 85), слід виходити з таких вимог законодавства щодо втручання в приватне спілкування: згідно з ч. 1 ст. 258 КПК ніхто не може зазнавати втручання в приватне спілкування без ухвали слідчого судді. Вилучений у підсудного під час обшуку ноутбук є обладнанням із накопиченою інформацією як приватного характеру, так і інформацією про діяльність ТОВ «Колорит», власником якого є підсудний Особа_2, яка згідно з ч. 2 ст. 21 Закону України «Про інформацію» є конфіденційною. Як стверджує підсудний, і це не спростовано органом обвинувачення, ним на ноутбуку було встановлено пароль, тобто він поставив логічний захист персональних даних приватного характеру. У цьому разі орган досудового розслідування міг отримати доступ до цієї інформації тільки на підставі ухвали слідчого судді» [8].

Аналіз вищенаведеної судової практики дає нам можливість сформулювати низку тез для побудови власного підходу до вирішення вказаного питання.

По-перше, складно погодитися з позицією адвокатів-захисників із приводу того, що для правильного процесуального оформлення дії, яка полягає в огляді та фіксації електронної інформації, що міститься на вилучених у межах інших процесуальних дій електронних пристроях, слід застосовувати таку НСРД, як зняття інформації з транспортних телекомунікаційних мереж. Річ у тім, що, як правильно вказують у вищенаведених рішеннях судді, ця НСРД передбачає «перехоплення» інформації в онлайн-режимі й не стосується статичних електронних даних, якими є sms, електронні листи, повідомлення в різних месенджерах тощо.

По-друге, на наш погляд, сумнівним у цьому разі взагалі є підхід, відповідно до якого в описаній ситуації має місце втручання в приватне спілкування (принаймні в тому сенсі, який у це поняття вкладає чинний КПК). Зокрема, в порядку аналогії можна навести ситуацію, коли під час обшуку буде вилучено не смартфон або ноутбук, які містять електронне листування, а, скажімо, паперові листи, які, безумовно, також є засобом передання інформації в рамках приватного спілкування. Зміст таких листів традиційно фіксується в протоколі огляду, і питання про втручання в приватне спілкування не виникає.

По-третє, навряд чи в цій ситуації взагалі можна ставити питання про фіксування такого роду інформації шляхом застосування інституту НСРД. Річ у тім, що НСРД за своїм визначенням передбачає отримання інформації без відома особи, яка є її власником, володільцем, адресатом, адресантом тощо. При цьому в разі відкритого вилучення електронного носія інформації власник такого носія абсолютно чітко розуміє мету такого вилучення, тож про негласний доступ уже не йдеться. Зокрема, не може в цьому разі йтися й про застосування такої НСРД, як зняття інформації з електронних інформаційних систем, оскільки остання передбачає або

негласне отримання доступу до електронного носія інформації опосередкованим (віддаленим) шляхом (наприклад із використанням віддаленого доступу через мережу Інтернет, під'єднання через дротову мережу тощо), або безпосереднє копіювання інформації під час негласного проникнення до приміщення. Проте в ситуації, коли електронний носій інформації знаходиться «в руках слідства», зазначені методи доступу втрачають сенс.

По-четверте, абсолютно правильним є висновок Придніпровського районного суду м. Черкаси з приводу того, що наявність ухвали слідчого судді про дозвіл на обшук, під час проведення якого вилучено електронний пристрій [8], або ухвали про накладення арешту на електронний пристрій, вилучений у власника під час затримання, ще не надає права на вилучення інформації, що міститься на такому пристрої. Інформація тут є окремим об'єктом, який не слід ототожнювати з її фізичним носієм (електронним пристроєм[2]) [9, с. 77]. Проте при цьому навряд чи можна погодитися з позицією, відповідно до якої відсутність паролю на смартфоні, ноутбуці чи іншому електронному носії інформації дає право вилучити й зафіксувати таку інформацію в порядку ч. 2 ст. 264 КПК, згідно з якою не потребує дозволу слідчого судді здобуття відомостей з електронних інформаційних систем або її частин, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний із подоланням системи логічного захисту [8]. На наш погляд, у цій ситуації можна провести аналогію з проникненням до житла чи іншого володіння, указавши таке: як незамкнені двері до будинку не свідчать про надання власником добровільної згоди на проникнення до житла, так і відсутність паролю для доступу до інформації на електронному пристрої не свідчить про те, що доступ до такої інформації не обмежується її власником, володільцем або утримувачем. Тож, на наше переконання, ч. 2 ст. 264 КПК у цій ситуації також не може бути застосована[3].

Підсумовуючи вищевикладене, маємо констатувати, що інформація, яка міститься на електронних пристроях, не може ототожнюватися із самим електронним пристроєм як її фізичним носієм. Отже, така інформація є окремим об'єктом права власності й об'єктом охорони таємниці приватного життя, а тому її вилучення/копіювання має відбуватися на підставі судового рішення, проте не в режимі застосування НСРД. Тож, на наш погляд, отримання та фіксування такої інформації має здійснюватися на підставі ухвали слідчого судді про тимчасовий доступ до речей і документів (у цьому разі – документів, що існують в електронній формі). Показово, що такий висновок підтверджується й найновішою судовою практикою. Зокрема, досить промовистою в цьому ключі є ухвала слідчого судді Солом'янського районного суду м. Києва. Аналізуючи деталі справи, слідчий суддя вказав таке: «Наведений зміст протоколу огляду чітко вказує на те, що детектив НАБУ здійснив не зовнішній огляд, який дозволяється чинним КПК, а безпосередній доступ і втручання до змісту інформації, яка зберігалася на вилученому мобільному телефоні IPhone 6+ A1522 IMEI Номер_1, та USB флеш-накопичувачі Transcend 16 GB чорного кольору з маркуванням C780032365, здійснив зняття копії інформації, яка зберігалася на вилученому мобільному телефоні IPhone 6+ A1522 IMEI Номер_1 і USB флеш-накопичувачі Transcend 16 GB чорного кольору з маркуванням C780032365, здійснив зняття копії інформації, що не охоплюється поняттям проведення огляду речей. Крім того, як установлено в судовому засіданні, уже після призначення детективом НАБУ експертизи «підбирався» пароль доступу до телефону, оглядалася та зберігалася у відповідних

[2] Примітка: досить показовою в цьому ключі є практика, що застосовується в США. Так, комп'ютер прирівнюється суддями до закритого контейнера, тому для його дослідження потрібний судовий дозвіл.

[3] Примітка: ч. 2 ст. 246 КПК застосовується для негласного отримання інформації, розміщуючи яку, особа усвідомлює можливість доступу необмеженого кола осіб до такої інформації (відкриті Інтернет-форуми, загальнодоступна інформація на сторінках соціальних мереж тощо).

звітах інформація з телефону та резервні копії інформації, збереженої на флеш-накопичувачі, про що безпосередньо вказано в описовій частині висновку експерта. Як вбачається, 12.10.2016 р., тобто вже після отримання висновків комп'ютерно-технічної експертизи, детектив НАБУ отримав ухвалу слідчого судді Солом'янського районного суду м. Києва про отримання дозволу на тимчасовий доступ до речей і документів із можливістю зняття копій із відповідних документів (інформації). Отже, фактично зазначеною ухвалою слідчого судді детектив отримав дозвіл на доступ до тієї інформації, яка вже на той час була вилучена з мобільного телефону, флеш-накопичувача та скопійована на електронні носії інформації. <…> Ураховуючи викладене, слідчий суддя ухвалив таке: визнати незаконною бездіяльність детектива НАБУ, яка полягала в незверненні до слідчого судді з клопотанням про тимчасовий доступ до речей і документів із можливістю зняття копій відповідних документів (інформації), які мають значення для кримінального провадження, у розумні строки для здійснення цієї процесуальної дії до початку огляду та для копіювання інформації, яка зберігалася на вилучених речах, і про призначення комп'ютерної технічної експертизи» [10].

Висновки. Інформація, яка міститься на вилучених у ході процесуальних дій (обшуків, затримань) електронних пристроях (персональних комп'ютерах, ноутбуках, смартфонах, телефонах тощо), не може ототожнюватися із самим електронним пристроєм як її фізичним носієм. Така інформація є окремим об'єктом права власності й об'єктом охорони таємниці приватного життя, а отже, її вилучення/копіювання має відбуватися на підставі судового рішення, проте не в режимі застосування НСРД. Отримання та фіксування такої інформації має здійснюватися на підставі ухвали слідчого судді про тимчасовий доступ до речей і документів (у цьому разі – документів, що існують в електронній формі).

Анотація

У статті розглянуті проблемні аспекти збирання доказів шляхом отримання інформації з вилученої електронної техніки та можливості їх розв'язання. На підставі аналізу матеріалів кримінальних проваджень автором визначені особливості визнання недопустимими доказів, які отримані в результаті огляду та фіксації електронної інформації, що міститься на вилучених під час кримінального провадження електронних пристроях. Акцентовано увагу на проблемі втручання в приватне життя під час таких дій. Ураховуючи правові колізії, у статті наводяться рекомендації, які мають на меті впорядкування окремих проблемних аспектів кримінального провадження.

Ключові слова: інформація, докази, електронна техніка, негласні слідчі (розшукові) дії, приватне життя.

Аннотация

В статье рассмотрены проблемные аспекты сбора доказательств путем получения информации с удаленной электронной техники и возможности их решения. На основании анализа материалов уголовных производств автором определены особенности признания недопустимыми доказательств, полученных в результате осмотра и фиксации электронной информации, содержащейся на изъятых во время уголовного производства электронных устройствах. Акцентировано внимание на проблеме вмешательства в частную жизнь во время таких действий. Учитывая существующие правовые коллизии, в статье приводятся рекомендации, которые имеют целью упорядочение отдельных проблемных аспектов уголовного производства.

Ключевые слова: информация, доказательства, электронная техника, негласные следственные (розыскные) действия, частная жизнь.

Shilo A.V. Obtaining information from seized electronic equipment as a method of collection of evidence: disputed questions of practical enforcement

Summary

The article deals with the problematic aspects of gathering evidence by obtaining information from seized electronic equipment and the possibility of solving them. On the basis of analysis of materials of criminal proceedings, the author identifies the features of recognition of inadmissible evidence obtained as a result of the inspection and fixing of electronic information contained in electronic devices detained during the criminal proceedings. The focus is on the issue of interference with privacy in the course of such actions. Taking into account the existing legal conflicts, the article gives recommendations aimed at the ordering of certain problematic aspects of criminal proceedings.

Key words: information, evidence, electronic equipment, secret investigative (search) actions, private life.

Список використаних джерел:

1. Вирок Голосіївського районного суду м. Києва від 18 квітня 2016 р., справа № 752/15787/15-к. URL: http://www.reyestr.court.gov.ua/Review/57301468.
2. Вирок Зарічного районного суду м. Суми від 17 серпня 2015 р. (справа № 591/8396/13-к). URL: http://www.reyestr.court.gov.ua/Review/48529766.
3. Ухвала Жовтневого районного суду м. Запоріжжя від 16 січня 2017 р. (справа №№ 1-кп/331/23/2017). URL: http://www.reyestr.court.gov.ua/Review/64135237.
4. Вирок Орджонікідзевського районного суду м. Маріуполя Донецької області від 10 серпня 2016 р. (справа №265/7387/15-к). URL: http://www.reyestr.court.gov.ua/Review/59646144.
5. Вирок Красноармійського міськрайонного суду Донецької області від 16 листопада 2015 р. (справа № 235/3606/15-к). URL: http://www.reyestr.court.gov.ua/Review/53461747.
6. Вирок Селидівського міського суду Донецької області від 02 березня 2016 р. URL: http://www.reyestr.court.gov.ua/Review/56200716.
7. Вирок Дружківського міського суду Донецької області від 26 травня 2016 р. (справа № 229/2532/15-к). URL: http://www.reyestr.court.gov.ua/Review/57906232.
8. Вирок Придніпровського районного суду м. Черкаси від 6 жовтня 2016 р. (справа № 699/268/15-к). URL: http://www.reyestr.court.gov.ua/Review/61844780.
9. Оконенко Р. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации: дисс. … канд. юрид. наук.: 12.00.09 – уголовный процесс; М., 2016. 158 с.
10. Ухвала слідчого судді Солом'янського районного суду м. Києва від 20 вересня 2017 р. (справа № 760/12767/17). URL: http://www.reyestr.court.gov.ua/Review/69160909.