Шило А.В.
здобувач,
Національний юридичний університет
імені Ярослава Мудрого;
оперативний співробітник Служби безпеки України

ПРОБЛЕМНІ АСПЕКТИ ЗБИРАННЯ ДОКАЗІВ ШЛЯХОМ ОТРИМАННЯ ІНФОРМАЦІЇ З ВИЛУЧЕНОЇ ЕЛЕКТРОННОЇ ТЕХНІКИ ТА МОЖЛИВОСТІ ЇХ РОЗВ'ЯЗАННЯ

Зважаючи на сучасний рівень комп'ютеризації суспільних відносин, на сьогодні левова частка інформації зберігається на електронних носіях або на віддалених серверах з використанням, так званих, «хмарних технологій»[1]. При цьому вказана характеристика сучасного світу перебуває у постійній позитивній динаміці, а відтак не може не враховуватися при збиранні інформації в рамках досудового розслідування. У цьому ключі на сьогодні досить гостро як з 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 існуючої на сьогодні судової практики дає можливість констатувати відсутність єдності у даному питанні як серед слідчих та прокурорів, так і серед суддів. У свою чергу досить часто при дослідженні такого роду інформації на предмет її допустимості захисниками піднімається питання про незаконне втручання у приватне спілкування (яке можливе лише в межах передбачених законом негласних слідчих (розшукових) дій (далі – НСРД)), як результат, суддями підтримується така позиція, що призводить до втрати стороною обвинувачення частини доказової інформації. Проте, на наше переконання, вказаний підхід, хоч і не

[1] *Примітка:* доступ до такої інформації у свою чергу також здійснюється через персональні електронні пристрої.

позбавлений раціонального зерна, все ж є досить спірним. Тож, зупинимось детально на даному питанні із викладенням власного бачення ситуації.

Перш за все зауважимо, що аналіз існуючої судової практики дає можливість виділити три підходи до вирішення ситуації із ознайомленням та фіксацією інформації, що міститься на вилученій електронній техніці. Найпоширенішим на сьогодні способом процесуального оформлення дії, що полягають в огляді та фіксації електронної інформації, яка міститься на вилучених у межах інших процесуальних дій електронних пристроях, є складання слідчим протоколу огляду в порядку ст. 237 КПК. При цьому, зважаючи на необхідність спеціальних знань при проведенні вказаної дії, такого роду огляд проводиться із залученням спеціаліста, завдання якого й полягає у тому, щоб виявити інформацію в електронному пристрої, що досить часто вимагає застосування спеціального програмного забезпечення (використовуються програми «Ufed Physical Analyzer», «Мобільний криміналіст» та інші).

У свою чергу, як вже зазначалось, стороною захисту досить часто ставиться питання про визнання результатів такого огляду недопустимими доказами, зважаючи на те, що мало місце втручання у приватне спілкування. При цьому судові рішення з даного питання є діаметрально протилежними.

Зокрема, одні судді не вбачають в процедурі такого огляду ознак втручання у приватне спілкування та визнають протоколи огляду допустимими доказами [1; 9].

Натомість інші суди в аналогічних випадках вважають, що ознайомлення із інформацією з електронного пристрою є втручанням у приватне спілкування та визнають протоколи огляду недопустимими доказами [5; 4; 7; 2; 6]. При цьому показово, що у своїх рішеннях судді лише ставлять питання про втручання у приватне спілкування та необхідність отримання відповідного дозволу слідчого судді на таке вручання, але не вказують на форми (види НСРД) у яких таке втручання мало б відбутися.

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

По-перше, складно погодитися із позицією адвокатів-захисників з 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 із транспортних телекомунікаційних мереж. Річ у тім, що, як правильно вказують у вищенаведених рішеннях судді, дана НСРД передбачає «перехоплення» інформації в «онлайн» режимі і не стосується статичних електронних даних, якими є sms, електронні листи, повідомлення у різного роду месенджерах тощо.

По-друге, на наш погляд, сумнівним у даному випадку взагалі є підхід, відповідно до якого в описаній ситуації має місце втручання у приватне спілкування (принаймні у тому сенсі, який в дане 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. Разом із тим, зміст таких листів традиційно фіксується у протоколі огляду й питання про втручання у приватне спілкування не виникає.

По-третє, навряд чи у даній 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 вже не йдеться. Зокрема, не може у даному випадку йтися і 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, з використанням віддаленого доступу через мережу Інтернет, під'єднання через дротову мережу тощо), або безпосереднє копіювання інформації при негласному проникненні до приміщення. Проте у 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 [6] або ухвали про накладення арешту на електронний пристрій, вилучений у власника при затриманні, ще не надає права на вилучення інформації, що міститься на такому пристрої. Інформація у даному випадку є окремим об'єктом, який не слід ототожнювати із її фізичним носієм – електронним пристроєм. Проте, при цьому навряд чи можна погодитися із позицією, відповідно до якої відсутність паролю на смартфоні, ноутбуці або 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 частини, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту. Така позиція прослідковується у вироку Придніпровського районного суду м. Черкаси від 6 жовтня 2016 р. (справа № 699/268/15-к).

На наш погляд, у даній ситуації можна провести аналогію із проникненням до житла та іншого володіння, вказавши наступне: 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 даній ситуації також не може бути застосована, оскільки дана норма відноситься до 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).

Підсумовуючи вищевикладене, маємо констатувати, що інформація, яка міститься на електронних пристроях, не може ототожнюватися із самим електронним пристроєм як її фізичним носієм.

Така інформація є окремим об'єктом права власності та об'єктом охорони таємниці приватного життя, а відтак її вилучення / копіювання має відбуватися на підставі судового рішення, проте не в режимі застосування НСРД.

Отримання та фіксування такої інформації має здійснювати на підставі ухвали слідчого судді про тимчасовий доступ до речей і документів (у даному випадку – документів, що існують в електронній формі).

Список використаних джерел:

1. Вирок Голосіївського районного суду м. Києва, від 18 квітня 2016 р., справа № 752/15787/15-к [Електронний ресурс]. – Режим доступу: http://www.reyestr.court.gov.ua/Review/57301468.

2. Вирок Дружківського міського суду Донецької області від 26 травня 2016 р. (справа № 229/2532/15-к) [Електронний ресурс]. – Режим доступу: http://www.reyestr.court.gov.ua/Review/57906232.

3. Вирок Зарічного районного суду м. Суми від 17 серпня 2015 р. (справа № 591/8396/13-к) [Електронний ресурс]. – Режим доступу: http://www.reyestr.court.gov.ua/Review/48529766.

4. Вирок Красноармійського міськрайонного суду Донецької області від 16 листопада 2015 р. (справа № 235/3606/15-к) [Електронний ресурс]. – Режим доступу: http://www.reyestr.court.gov.ua/Review/53461747.

5. Вирок Орджонікідзевського районного суду м. Маріуполя Донецької області, вирок від 10 серпня 2016 р. (справа № 265/7387/15-к) [Електронний ресурс]. – Режим доступу: http://www.reyestr.court.gov.ua/Review/59646144.

6. Вирок Придніпровського районного суду м. Черкаси від 6 жовтня 2016 р. (справа № 699/268/15-к) [Електронний ресурс]. – Режим доступу: http://www.reyestr.court.gov.ua/Review/61844780.

7. Вирок Селидівського міського суду Донецької області від 02 березня 2016 р. [Електронний ресурс]. – Режим доступу: http://www.reyestr.court.gov.ua/Review/56200716.

8. Оконенко Р.И. «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.: спец.12.00.09 – уголовный процесс; М., 2016. – 158 с.

9. Ухвала Жовтневого районного суду м. Запоріжжя від 16.01.2017 (справа № № 1-кп/331/23/2017) [Електронний ресурс]. – Режим доступу: http://www.reyestr.court.gov.ua/Review/64135237.