ВТРУЧАННЯ У ПРИВАТНЕ СПІЛКУВАННЯ ШЛЯХОМ ЗНЯТТЯ ІНФОРМАЦІЇ З ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ СИСТЕМ

КУШПІТ Володимир Петрович - кандидат юридичних наук, доцент, доцент кафедри кримінального права і процесу Навчально-наукового інституту права, психології та інноваційної освіти Національного університету «Львівська політехніка»

ORCID ID: 0000-0002-1664-6696

УДК 343.13

DOI 10.32782/NP.2021.4.13

У статті досліджено та проаналізовано ефективність застосування негласної слідчої (розшукової) дії «Зняття інформації з електронних інформаційних систем». Визначено, що не потребує дозволу слідчого судді здобуття відомостей з електронних інформаційних систем або їх частин, доступ до яких не обмежується їх власником, володільцем або утримувачем або не пов'язаний із подоланням системи технічного захисту. Звернено увагу на те, що сучасні технології дозволяють оперативно відстежувати діяльність злочинних співтовариств на принципово іншому рівні. Досліджено досвід спецслужб США в розробці і застосуванні систем «Oasis» і «Magic Lantern» (в перекладі «Чарівний Ліхтар»), які надають можливість не тільки контролювати інформаційний обмін злочинних співтовариств, але й негласно проникати до пам'яті комп'ютера підозрюваних, упроваджувати в них програми-віруси, що дозволяють відстежувати інформацію у цьому комп'ютері. Визначено, що зняття необхідної інформації здійснюється безпосередньо шляхом фізичного доступу до носіїв фахівцями уповноважених технічних оперативних підрозділів правоохоронних органів або шляхом відповідного програмного проникнення. Проведення цих слідчих (розшукових) дій відбувається негласно, у порядку, встановленому положеннями ст.ст. 246, 248, 250 КПК України. У процесі дослідження автором сформулював власні висновки та запропонував нову редакцію ст. 264 КПК України.

Постановка проблеми

Правова система України в цілому, зокрема й система слідчих (розшукових) дій, у сучасному стані повинна розбудовуватися відповідно до визнаного Європейською спільнотою та запровадженого в практиці Європейського суду з прав людини принципу правової визначеності, згідно з яким обмеження основних прав людини та громадянина, а також втілення цих обмежень на практиці допустиме лише за умови забезпечення передбачуваності застосування правових норм, у яких встановлено такі обмеження.

Зняття інформації з електронних інформаційних систем є однією з новел чинного КПК України поряд з іншими негласними слідчими (розшуковими) діями. Ефективність її застосування в певній мірі залежить від забезпечення при регламентації принципу юридичної визначеності та дотримання при її застосуванні принципу пропорційності, на яких наголошує у своїх рішеннях Європейський суд з прав людини.

Аналіз останніх досліджень і публікацій

Дослідженню цього питання присвятили свої праці такі учені, як: Ю. П. Аленін, С. А. Альперт, М. І. Бажанов, О. М. Бандурка, Ю. В. Баулін, В. П. Бож'єв, Т. Ф. Варфоломієва, П. П. Водько, В. І. Галаган, В. Г. Гончаренко, Ю. М. Грошевий, А. Я. Дубинський, Я. П. Зейкан, В. С. Зеленецький, О. В. Капліна, Н. С. Карпов, Є. Г. Кова-

ленко, О. А. Кучинська, О. П. Кучинська, Л. М. Лобойко, Є. Д. Лук'янчиков, В. Т. Малащенко, О. Р. Михайленко, М. М. Михеєнко, В. В. Молдован, В. В. Назаров, В. Т. Нор, О. Ю. Татаров, М. А. Погорецький, В. О. Попелюшко, В. Д. Пчолкін, Д. В. Сімонович, В. М. Тertiшник, Л. Д. Удалова, В. М. Хотенець, В. Ю. Шепітько, В. П. Шибіко, О. Г. Шило, М. Є. Шумило, О. О. Юхно, О. Г. Яновська та ін.

Виклад основних положень

У положеннях ст. 264 КПК України «Зняття інформації з електронних інформаційних систем» закріплено, що пошук, виявлення і фіксація відомостей, що містяться в електронній інформаційній системі або її частині, доступ до електронної інформаційної системи або її частини, а також отримання таких відомостей без відома її власника, володільця або утримувача може здійснюватися на підставі ухвали слідчого судді, якщо є відомості про наявність інформації в електронній інформаційній системі або її частині, що має значення для певного досудового розслідування. Не потребує дозволу слідчого судді здобуття відомостей з електронних інформаційних систем або їх частин, доступ до яких не обмежується їх власником, володільцем або утримувачем або не пов'язаний із подоланням системи технічного захисту. В ухвалі слідчого судді про дозвіл на втручання у приватне спілкування в цьому випадку додатково повинні бути зазначені ідентифікаційні ознаки електронної інформаційної системи, у якій може здійснюватися втручання у приватне спілкування.

З дослідженого питання слід зазначити, що закріплення в КПК України цієї негласної слідчої (розшукової) дії обумовлена сучасним розвитком цивілізації, широким проникненням інформаційних технологій у суспільне життя, фактично формуванням нового типу соціальної парадигми – інформаційного суспільства, тобто ери цифрової технології.

На думку Т. В. Авер'янової, інтеграція в криміналістику досягнень природничих і технічних наук, ускладнення технічних засобів, удосконалення і розвиток методик їх застосування нерідко пов'язано зі складни-

ми технологічними операціями, тому необхідно вести мову вже не лише про криміналістичну техніку, а й про технологію [1].

Як зазначили В. Г. Гончаренко, В. Т. Нор, М. Є. Шумила, О. М. Бандурка, Є. М. Блажівський, В. Я. Тацій та інші, сутність зняття інформації з електронних інформаційних систем полягає у здійсненні на підставі ухвали слідчого судді пошуку, виявлення і фіксації відомостей, що містяться в електронній інформаційній системі або її частин, доступ до яких обмежений власником, володільцем або утримувачем системи розміщення її у публічно недоступному місці, житлі чи іншому володінні особи або логічним захистом доступу, а також отримання таких відомостей без відома її власника, володільця або утримувача [2].

Проблеми процесуального порядку зняття інформації з електронних інформаційних систем залишаються малодослідженими. Однак, дослідження цих проблем набувають усе більшої актуальності, зростає активність науковців у цьому напрямі.

У рамках дослідження цієї проблеми В. В. Бірюков визначив, що комп'ютерні технології, як сукупність методів і програмно-технічних засобів на базі комп'ютера (ЕОМ), об'єднаних у єдиний технологічний ланцюжок, що забезпечує збирання, обробку, збереження і передачу інформації з метою зниження трудомісткості інформаційних процесів, а також підвищення їх надійності й оперативності [3, с. 54].

У ході цієї дискусії М. Я. Сегай зазначив, що інформатизація судочинства має базуватися на законодавчому дозволі застосування в кримінальному процесі інформаційних технологій (комп'ютерної та телекомунікаційної техніки з відповідними програмними продуктами). Це дасть змогу оптимізувати діяльність усіх правових інституцій, що задіяні в судочинстві, зокрема органів досудового розслідування, прокуратури, судово-експертних установ, судів, установ виконання покарань, адвокатури. Застосування інформаційних технологій у судочинстві має бути дозволено при виконанні будь-яких процесуальних дій як у звичайному, так і в інтерактивному (дистанційному) режимі, з одночасним веденням документообігу і діловод-

ства на паперових та електронних носіях, з яких для учасників процесу у випадках, передбачених процесуальним законодавством, виготовляються автентичні копії процесуальних документів [1].

Комп'ютери можуть зберігати, аналізувати, кодувати і декодувати інформацію в такому об'ємі, що це все більше перетворює їх на могутній і, водночас, вразливий інструмент, за допомогою якого можуть здійснюватися збір і розповсюдження інформації; віртуальний простір став самостійним місцем існування людського інтелекту і, як будь-яка об'єктивна реальність, породив безліч проблем, у тому числі і правових [2].

У зв'язку з цим слід звернути увагу на те, що сучасні технології дозволяють оперативно відстежувати діяльність злочинних співтовариств на принципово іншому рівні. Представляє значний практичний інтерес досвід спецслужб США в розробці і застосуванні систем «Oasis» і «Magic Lantern» (у перекладі «Чарівний Ліхтар»), які надають можливість не тільки контролювати інформаційний обмін злочинних співтовариств, але й негласно проникати до пам'яті комп'ютера підозрюваних, упроваджувати в них програми-віруси, що дозволяють відстежувати інформацію у цьому комп'ютері тощо. Magic Lantern встановлює на комп'ютер програму, яка реєструє всі натиснення клавіш на клавіатурі. Таким чином, з допомогою цієї програми можна зчитувати з комп'ютерів зашифровану інформацію. Віруси програми Magic Lantern відсилають до підозрюваного електронною поштою. Якщо можливо, то це робиться від імені родича підозрюваного або його знайомого.

На сьогодні на практиці слідчий стикається не з досконалим законодавчим регламентуванням зазначеної негласної слідчої (розшукової) дії, а фактично лише з дозволом на її проведення. У зв'язку з цим слід підтримати думку В. Я. Тація, що серед великих масивів інформації, що локалізуються в соціальних мережах Інтернету, може бути отримана інформація щодо окремих осіб, які підозрюються в підготовці та вчиненні кримінальних правопорушень, їх зв'язків, та багато інших відомостей, що можуть сприяти вирішенню завдань досудо-

вого розслідування. Оскільки ця інформація є загальнодоступною, дозволу слідчого судді на її пошук та фіксацію кримінальний процесуальний закон не потребує через те, що не відбувається обмеження приватності [1].

Водночас, слід зауважити, що це не стосується інформації, яка передається електронною поштою чи обмінюється між користувачами Інтернету в режимі приватного спілкування. За необхідності отримання доступу до таких відомостей слід застосовувати в передбачуваному законом порядку при провадженні негласної слідчої (розшукової) дії, як зняття інформації з транспортних телекомунікаційних мереж.

Також, на нашу думку, дискусійною видається позиція В. Г. Гончаренка, В. Т. Нора, М. Є. Шумила, що у випадках, коли під час досудового розслідування встановлюється, що файловий сервер електронної інформаційної системи встановлений у публічно недоступному місці, житлі або іншому володінні особи, але доступ до баз даних, розміщених на ньому, не захищений системами логічного захисту доступу і можливий з робочих станцій, розташованих поза межами місць розміщення файлових серверів електронної інформаційної системи, зняття інформації з електронних інформаційних систем або її частин також можливе без дозволу слідчого судді. Науковці зазначають, що у цій ситуації складається тільки протокол зняття інформації з електронних інформаційних систем з відповідними додатками до нього [1].

У положеннях Загальної декларації прав людини ООН, Конвенції про захист прав і основних свобод людини законними вважаються такі обмеження права особи на приватне життя, які: визначені в законі і мають зрозумілу правову основу; переслідують мету, досягнення якої буде більшим благом, ніж шкода, яка ними ж і спричиняється; діють тимчасово; застосовуються без будь-якої дискримінації; є підконтрольними суду; здійснюються після закріплення механізму поновлення незаконно порушених прав та свобод; можна оскаржити відповідно до порядку, встановленого в законі.

Досліджуючи міжнародні критерії законних обмежень права та свободи особи у кримінальному судочинстві, С. Ільченко зазначив, що, зважаючи на можливі негативні наслідки, яких особа може зазнати під час незаконного порушення її прав та свобод у кримінальному судочинстві, наведені міжнародно-правові критерії законних обмежень доцільно брати до уваги під час подальшого реформування кримінального судочинства [2], що ми підтримуємо, але вважаємо за доцільне додати, що насамперед стосується й удосконалення чинного КПК України.

У сучасній науці кримінального процесу набуває свого розвитку дискусія стосовно удосконалення процесуальної регламентації зняття інформації з електронних інформаційних систем. Зокрема, у контексті досліджуваного питання Ю. В. Лисюк зазначив, що зняття інформації з електронних інформаційних систем або їх частин може здійснюватися шляхом отримання інформації, що оброблялася, зберігалася або зберігалася на персональному комп'ютері чи декількох персональних комп'ютерах, об'єднаних у локальну мережу, або ж зовнішніх накопичувачах інформації, що приєднувалися до електронних інформаційних систем [1].

Системи можуть бути локальними, у яких усі їх компоненти (база даних, система управління базою даних, клієнтське програмне забезпечення) знаходяться на одному комп'ютері, і розподіленими, у яких компоненти розподілені по кількох комп'ютерах. Останні поділяють на файл-серверні інформаційні системи (у них база даних знаходиться на файловому сервері, а система управління базою даних та клієнтське програмне забезпечення - на робочих станціях) та клієнт-серверні інформаційні системи (база даних та система управління нею знаходяться на сервері, а на робочих станціях - клієнтське програмне забезпечення). Електронні інформаційні системи можуть бути відкритими і закритими залежно від того, чи обмежується до них доступ. Обмеження доступу може здійснюватися власником, володільцем або утримувачем електронної інформаційної системи шляхом розміщення у публічно недоступних місцях та встановлення систем логіч-

ного захисту доступу з робочих станцій (комп'ютерів) локальної або глобальної мережі Інтернет [2].

Зняття необхідної інформації здійснюється безпосередньо шляхом фізичного доступу до носіїв фахівцями уповноважених технічних оперативних підрозділів правоохоронних органів або шляхом відповідного програмного проникнення. Проведення цих слідчих (розшукових) дій відбувається негласно, у порядку, встановленому положеннями ст.ст. 246, 248, 250 КПК України. Для здійснення таких процесуальних дій правоохоронним органам необхідно мати у своєму розпорядженні сучасні засоби спеціальної техніки з достатнім для проведення негласних слідчих (розшукових) дій обсягом оперативної пам'яті для забезпечення копіювання або збереження інформації у процесі здійснення кримінального провадження. Для зняття ж інформації, доступ до якої не обмежується її власником, володільцем або утримувачем і не передбачає проникнення з подоланням окремих систем захисту, не потрібно ухвали слідчого судді. Відповідну інформацію для виконання завдань, які виникають під час здійснення кримінального провадження, можна знайти серед комп'ютерних систем та мереж відкритої інформації, а також у всесвітній мережі Інтернет. Отже, у цій частині людина є захищеною, оскільки інформація, яка буде отримана для забезпечення кримінального провадження, не передбачає втручання у її приватне спілкування, вона є загальнодоступною та відображає тільки ті відомості, які надаються добровільно самою особою чи знайомими особами для користування, і вона розуміє, що нею можуть користуватися інші особи. Повертаючись до ухвали суду, яка дає дозвіл на проведення негласних слідчих (розшукових) дій щодо зняття інформації з електронних інформаційних систем, необхідно наголосити, що в ухвалі слідчого судді повинні бути чітко зазначені ідентифікаційні ознаки електронних інформаційних систем, які підлягають обробці, найменуванню та ін. За результатами проведених негласних слідчих (розшукових) дій в обов'язковому порядку складається протокол із дотриманням відповідних ви-

мог ст.ст. 104-107, 252 та 265 чинного КПК України.

Однак, з цього питання все ж таки виникають спірні та дискусійні питання, а саме: чи відповідають дійсності отримані в ході негласних слідчих (розшукових) дій документи та чи проведено самі дії з дотриманням усіх вимог чинного КПК України? Більше того, особі, яка є учасником кримінального провадження, неможливо отримати правдиві дані щодо наявності або спростування тієї чи іншої інформації, оскільки неможливо зі стовідсотковою впевненістю зазначити, що протокол, складений після проведення негласних слідчих (розшукових) дій, не підроблено. Тому, знову ж таки, на перший план виходять окремі інтереси осіб, які можуть бути зацікавленими у результатах проведення кримінального провадження, а ці питання будуть постійно виникати та вимагати додаткового, більш глибокого вивчення.

На сьогодні, на думку Ю. В. Лисюка, з упевненістю вже можна зазначити про те, що не всі дії правоохоронних органів під час здійснення кримінальних проваджень за чинним КПК України спрямовано на захист прав людини, хоча КПК є більш демократичним від попереднього і його основою є захист прав людини. Але, виходячи з того, що чинний КПК України направлено на демократизацію, потрібен усе ж таки певний час для того, щоб людина та суспільство направили свої зусилля на виконання вимог чинного національного законодавства, а державні органи ефективно здійснювали політику щодо захисту прав людини й притягнення винних до юридичної відповідальності [1].

Висновки

Враховуючи, що досліджена негласна слідча (розшукова) дія є новою і немає сталої практики її застосування, а детальна регламентація її проведення може мінімізувати можливі помилки, виходячи із загальних вимог, що пред'являються до інституту негласних слідчих (розшукових) дій, пропонуємо ст. 264 КПК України «Зняття інформації з електронних інформаційних систем» викласти в такій редакції: «Зняття інфор-

мації з електронних інформаційних систем проводиться в тих випадках, коли є достатні підстави вважати, що фактичні дані, які мають значення для встановлення істини у кримінальному провадженні чи забезпечення прав і законних інтересів учасників провадження або їх безпеки і безпеки суспільства, можуть знаходитись в електронній інформаційній системі, яка знаходиться в певному приміщенні або місці чи в будь-якої особи, та якщо іншим шляхом досягти виконання завдань кримінального провадження неможливо.

У невідкладних випадках пов'язаних із необхідністю протидії тероризму, врятуванням життя, честі, гідності і здоров'я людини, захисту її прав та свобод чи для забезпечення особистої і суспільної безпеки, коли зволікання з проведенням слідчої (розшукової) дії може призвести до втрати важливих доказів, зняття інформації з електронних інформаційних систем проводиться без дозволу слідчого судді із погодженням з прокурором, але з наступним повідомленням слідчого суддю в добовий строк про проведену слідчу (розшукову) дію та її результати. На ухвалу слідчого судді про відмову в проведенні зняття інформації з електронних інформаційних систем протягом трьох діб з дня її винесення прокурором може бути подана апеляція до апеляційного суду».

Література

1. Криміналістика: Учебник / Т. В. Аверьянова, Р. С. Белкин, Ю. Г. Корухов, Е. Р. Россинская ; под ред. Р.С. Белкина. М.:Изд.-во НОРМА, 2000. С. 131.
2. Кримінальний процесуальний кодекс України. Науково-практичний коментар : у 2 т. Т.1. / О. М. Бандурка, Є. М. Блажівський, та ін.; за заг. ред. В. Я. Тація, В. П. Пшонки, А. В. Портнова. Х. : Право, 2012. С. 581.
3. Бірюков В. В. Використання комп'ютерних технологій для фіксації криміналістично значимої інформації у процесі розслідування : дис канд. юрид. наук : 12.00.09 – кримінальний процес та криміналістика; судова експертиза / Валерій Васильович Бірюков; Нац. акад. внутр. справ України. К., 2001. С. 54.

Kushpit Volodymyr

INTERFERENCE IN PRIVATE COMMUNICATION BY REMOVAL OF INFORMATION FROM ELECTRONIC INFORMATION SYSTEMS

The article investigates and analyzes the effectiveness of the covert investigative (search) action “Removal of information from electronic information systems.” It is determined that it does not require the permission of the investigating judge to obtain information from electronic information systems or parts thereof, access to which is not restricted by their owner, possessor or holder or is not related to overcoming the technical protection system. Attention is drawn to the fact that modern technologies allow you to quickly monitor the activities of criminal communities at a fundamentally different level. The experience of the US intelligence services in the development and use of systems “Oasis” and “Magic Lantern” (translated as “Magic Lantern”), which provide an opportunity not only to control the information exchange of criminal communities, but also to secretly penetrate into the computer memory of suspects, implement viruses in them that allow you to track information on this computer. It is determined that the removal of the necessary information is carried out directly by physical access to the media by specialists of authorized technical operational units of law enforcement agencies or by appropriate software penetration. Carrying out

of these investigative (search) actions occurs secretly, in the order established by provisions of Art. 246, 248, 250 KPK of Ukraine. In the course of the research the author formulated his own conclusions and proposed a new version of Art. 264 of the Criminal Procedure Code of Ukraine «Withdrawal of information from electronic information systems is carried out in cases where there are sufficient grounds to believe that factual data relevant to establishing the truth in criminal proceedings or ensuring the rights and legitimate interests of participants or their safety and security of society may be in electronic information system, which are located in a certain room or place or in any person, and if it is otherwise impossible to achieve the tasks of criminal proceedings.

In urgent cases related to the need to combat terrorism, save lives, honor, dignity and human health, protect human rights and freedoms or to ensure personal and public safety, when delays in the conduct of investigative (search) action may lead to the loss of important evidence, withdrawal of information from electronic information systems is carried out without the permission of the investigating judge in agreement with the prosecutor, but with the subsequent notification of the investigating judge within a day about the investigative (search) action and its results. An appeal may be lodged with the appellate court against the decision of the investigating judge on the refusal to withdraw information from electronic information systems within three days from the date of its issuance by the prosecutor».