

ЗНЯТТЯ інформації

з електронних інформаційних систем: новели Кримінального процесуального кодексу України та євростандарти



В. Г. Уваров

кандидат юридичних наук, докторант кафедри кримінального процесу Дніпропетровського державного університету внутрішніх справ, заслужений юрист України

У статті аналізуються проблеми становлення інституту зняття інформації з електронних інформаційних систем в системі слідчих дій за новим Кримінальним процесуальним кодексом України.

Ключові слова: інформаційні системи, зняття інформації, втручання у приватне життя, міжнародні стандарти.

В статье анализируются проблемы становления института снятия информации с электронных информационных систем в системе следственных действий по новому Уголовному процессуальному кодексу Украины.

Ключевые слова: информационные системы, снятие информации, вмешательство в личную жизнь, международные стандарты.

In article problems of formation of institute of removal of the information from electronic information systems are analyzed in the investigation by the new Criminal procedure code of Ukraine.

Keywords: information systems, information removal, intervention in private life, the international standards.

Із прийняттям нового Кримінального процесуального кодексу України (далі – КПК України) гостро постала проблема становлення та застосування інституту зняття інформації з електронних інформаційних систем.

Актуальність досліджуваної проблеми полягає у тому, що зняття інформації з електронних інформаційних систем є новелою КПК України, яка ще не отримала теоретичного аналізу та практичного досвіду застосування.

Аналіз останніх наукових досліджень показує, що проблеми зняття інформації з електронних інформаційних систем у кримінальному процесі залишаються поки що малодослідженими, хоча аналіз даних проблем стає все більш активними [1-15].

Мета нашої роботи – визначити шляхи реформування інституту зняття інформації з електронних інформаційних систем в контексті міжнародних правових актів та прецедентної практики Європейського суду з прав людини.

У статті 264 нового КПК України («Зняття інформації з електронних інформаційних систем») визначається: «Пошук, виявлення і фіксація відомостей, що містяться в електронній інформаційній системі або їх частин, 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.

2. 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.

3. В ухвалі слідчого судді про дозвіл на втручання у приватне спілкування в цьому випадку додатково повинні бути зазначені ідентифікаційні ознаки електронної інформаційної системи, в якій може здійснюватися втручання у приватне спілкування».

Поява даної слідчої дії обумовлена формуванням нового типу соціальної парадигми – інформаційного суспільства.

На думку М. Я. Сегає, 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, – органів досудового слідства, 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) режимах, з одночасним веденням документообігу і діловодства на паперових та електронних носіях, з яких для учасників процесу у випадках, передбачених процесуальним законодавством, виготовляються автентичні копії процесуальних документів [10, с. 190-198].

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, породила безліч проблем, у тому числі і правових [5, с. 28].

Сучасні нові технології дозволяють оперативно відстежувати діяльність злочинних співтовариств принципово на іншому

рівні. Викликає значний інтерес досвід спецслужб США в розробці і застосуванні систем «Oasis» (ЦРУ) і «Magic Lantern» (ФБР), які уможливають не тільки контролювати інформаційний обмін злочинних співтовариств, а й «зламувати» комп'ютери підозрюваних, упроваджувати в них «трояни» (програми-віруси, що дозволяють відстежувати інформацію у цьому комп'ютері) тощо. Magic Lantern (в перекладі «Чарівний Ліхтар») встановлює на комп'ютер програму, яка реєструє всі натиснення клавіш на клавіатурі. Таким чином, з допомогою даної програми можна прочитувати з комп'ютерів зашифровану інформацію. Віруси програма Magic Lantern відсилає до підозрюваного по електронній пошті. Якщо можливо, то це робиться від імені родича підозрюваного або його хорошого знайомого. Для переміщення в комп'ютер програма Magic Lantern використовує також відомі «дірки» в поширених програмних продуктах [5, с. 57].

Безумовно, що зняття інформації з електронних інформаційних систем може носити як характер розвідувальної чи контррозвідувальної інформаційно-пошукової діяльності, так і характер пізнавально-фіксуєчою, засвідчуваною, доказовою діяльністю, яка притаманна сфері кримінального судочинства.

Але знову і знову ми стикаємось не з законодавчим регламентуванням слідчої дії, а фактично лише з дозволом на її проведення.

Згідно з вимогами Загальної декларації прав людини ООН, Конвенції про захист прав і основних свобод людини та рішень Європейського суду з прав людини законними можна вважати 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.

Зважаючи на 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 внесення змін до КПК України [3, с. 16-19].

Важливим гарантом захисту прав і свобод людини взагалі і при провадженні слідчих дій, зокрема виступає процесуальна форма слідчої дії, яка являє собою приписи закону, які мають на принципах передбачуваності визначати усю процедуру їх провадження: підстави, умови, строки, послідовність та порядок дій учасників процесу, засоби реалізації ними своїх прав, свобод і обов'язків, а також режим документування процесуальної діяльності.

Процесуальна форма слідчої дії є важливим гарантом достовірності отриманої інформації (доказів) та забезпечення верховенства права, виступає важливим гарантом захисту прав і свобод людини.

Як зауважує М. Погорецький, в умовах, коли Україна займає одне з провідних місць в світі за рівнем корумпованості, «при реформуванні кримінально-процесуального законодавства на цьому етапі розвитку держави слід максимально звужувати можливості прийняття процесуальних рішень на власний розсуд особами, які ведуть кримінальний процес, водночас всебічно розробляючи, розширюючи та удосконалюючи процесуальну форму. Оскільки саме недосконалість процесуальної форми, як показує практика, є однією з причин зловживань у кримінальному

процесі, а також однією з причин судово-слідчих помилок...» [8, с. 33].

Основу слідчих дій складають окремі методи пізнання – візуальне спостереження, розпитування, сприйняття, пошук, порівняння (ідентифікація), відтворення, дослідження, які супроводжуються закріпленням (фіксацією та засвідченням) одержаної доказової інформації чи висновків дослідження в відповідних процесуальних документах. Передбачуваний законом для певних випадків метод пізнання втілюється в практичній діяльності слідчого з провадження слідчої дії, а хід і результати пізнання відображаються в протоколі слідчої дії в процесуальному документі. Виступаючи як пізнавально-засвідчувальна дія, слідча дія одночасно є також і актом застосування права, і тому являє собою певну систему правовідносин. Норми права, які регламентують провадження слідчих дій, являють собою певну модель діяльності слідчого і несуть у собі конструктивні засади. Вони створюють правовий інститут – слідчу дію [11, с. 478].

Регламентация зняття інформації з електронних інформаційних систем потребує суттєвого вдосконалення.

Враховуючи, що дана слідча дія нова і немає сталі практики її застосування, а детальна регламентація її проведення може мінімізувати можливі помилки, виходячи з загальних вимог, що пред'являються до інститутів слідчих дій, пропонуємо ст. 264 нового КПК України (Зняття інформації з електронних інформаційних систем) викласти таким чином:

«Зняття інформації з електронних інформаційних систем проводиться в тих випадках, коли є достатні підстави вважати, що фактичні дані, які мають значення для встановлення істини в справі чи забезпечення прав і свобод учасників процесу чи їх безпеки і безпеки суспільства, можуть знаходитись в електронній інформаційній системі, яка знаходиться в певному

приміщенні або місці чи в якої-небудь особі, та якщо іншим шляхом досягти виконання завдань правосуддя неможливо.

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 та користувача може здійснюватися на підставі ухвали слідчого судді.

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.

У невідкладних випадках, пов'язаних із необхідністю протидії тероризму, врятуванням життя, честі, гідності і здоров'я людини, захисту її прав і свобод чи для забезпечення особистої і суспільної безпеки, коли зволікання з проведенням слідчої дії може призвести до втрати важливих доказів, зняття інформації з електронних інформаційних систем проводиться без дозволу слідчого судді з санкції прокурора, але з наступним повідомленням слідчого суддю в добовий строк про проведену слідчу дію і її результати.

При необхідності провести зняття інформації з електронних інформаційних систем слідчий за погодженням з прокурором звертається з поданням до судді за місцем провадження слідства. Суддя негайно і не пізніше доби розглядає подання та матеріали справи і за наявності підстав вносить постанову про зняття інформації з електронних інформаційних систем чи постанову про відмову в проведенні даної слідчої дії.

На постанову 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.

Зняття інформації з електронних інформаційних систем провадяться в присутності власника, володільця чи утримувача та користувача електронної інформаційної системи та двох понятих.

Присутнім при знятті інформації з електронних інформаційних систем особам, понятим і залученим фахівцям повинно бути роз'яснено їхнє право бути присутніми при всіх діях слідчого і робити заяви з приводу цих дій; ці заяви підлягають занесенню до протоколу.

Перед зняттям інформації з електронних інформаційних систем слідчий пред'являє постанову про проведення вказаної слідчої дії власнику, володільцю, утримувачу чи користувачу електронної інформаційної системи і пропонує їм відкрити доступ до необхідної для справи інформації. У разі відмови виконати його вимоги слідчий застосовує сам чи з допомогою спеціаліста заходи подолання системи захисту та проводить пошук, виявлення і фіксацію відомостей, що містяться в електронній інформаційній системі або їх частинах у примусовому порядку.

При цьому слідчий повинен уникати не викликаних необхідністю пошкоджень електронних інформаційних систем та їх програмного забезпечення, втрати їх інформаційного наповнення.

Під час зняття інформації з електронних інформаційних систем слідчий повинен вживати заходів до того, щоб не були розголошені виявлені при цьому обставини особистого життя будь-якої людини, ділової репутації фізичних і юридичних осіб, нотаріальної, комерційної, лікарської чи іншої охоронюваної законом таємниці.

Інформацію, яка має відношення до справи, слідчий має пред'явити понятим та іншим присутнім особам і зафіксувати в протоколі слідчої дії та засобами технічного документування.

Про проведення зняття інформації з електронних інформаційних систем слід-

чий складає протокол не менш ніж у двох примірниках. У протоколі повинні бути вказані, час і місце проведення слідчої дії, хід і результати слідчої дії, які саме електронні інформаційні системи були оглянуті та досліджені, що було виявлено і яким чином було зафіксовано, що і з якою метою було вилучено для залучення до справи.

До протоколу зняття інформації з електронних інформаційних систем заносяться всі заяви і зауваження присутніх осіб, зроблені з приводу тих чи інших дій слідчого. Примірники протоколу підписують слідчий, особа, у якій проводилось дослідження електронних інформаційних систем, та запрошені особи, що були присутні.

Примірник протоколу зняття інформації з електронних інформаційних систем вручається особі, у якій проведено дослідження електронних інформаційних систем, а також іншим особам на їх вимогу, чий права і свободи при цьому були обмежені.

При наявності в протоколі зауважень на неправильні дії, допущені під час слідчої дії, слідчий не пізніше двох діб повідомляє про це прокурора, який здійснює нагляд за слідством, та слідчого суддю».

У відповідності до вимог, викладених у Рішеннях ЄСПЛ, які орієнтують в законодавчій діяльності дотримуватись принципу передбачуваності та верховенства права, зняття інформації з електронних інформаційних систем носить ознаки нової слідчої дії, але процесуальна форма її провадження має бути суттєво вдосконалена з тим, щоб чітко визначити підстави, умови, строки, послідовність та порядок дій учасників процесу, засоби реалізації ними своїх прав, свобод і обов'язків, а також режим документування процесуальної діяльності, які мають забезпечити мінімізувати ризики свавілля.

Перспективи подальшого дослідження проблеми вбачаються в розробці практичних рекомендацій щодо провадження нової слідчої дії – зняття інформації з електронних інформаційних систем.

Список використаної літератури

1. Бірюков В. В. Використання комп'ютерних технологій для фіксації криміналістично значимої інформації у процесі розслідування : дис. ... канд. юрид. наук : 12.00.09 / В. В. Бірюков. – К., 2001. – 206 с.
2. Доронин А. Аналитическая разведка средствами интернета / А. Доронин // Неизвестная разведка. – 2006. – №3-4. – С. 54-61.
3. Ільченко С. Права та свободи особи у кримінальному судочинстві: міжнародні критерії законних обмежень / С. Ільченко // Підприємництво, господарство і право. – 2005. – №5. – С. 16-19.
4. Лук'янчиков Є. Д. Методологічні засади інформаційного забезпечення розслідування злочинів : моногр. / Є. Д. Лук'янчиков. – К. : Нац. акад. внутр. справ України, 2005. – 360 с.
5. Михальчук Т. В. Використання інформації, отриманої телекомунікаційним шляхом, у розслідуванні злочинів : дис. ... канд. юрид. наук. Спец. 12.00.09 / Т. В. Михальчук. – Київ, 2010. – 223 с.
6. Новицький А. М. Оперативно-розшукова діяльність в Інтернеті: проблеми правозастосування / А. М. Новицький // Правова інформатика. – 2009. – №1 (21). – С. 85-90.
7. Номоконов В. А. Новые информационные технологии в борьбе с преступностью [Электронный ресурс] / В. А. Номоконов // Российский криминологический взгляд. – 2005. – №1. – С. 90-93. – Режим доступа : <http://www.telcon.ru>
8. Погорєцький М. Новий КПК України: політичні, теоретичні та юридичні питання / М. Погорєцький // Право України. – 2009. – №2. – С. 29-35.
9. Садова Т. В. Обмеження прав і свобод у кримінальному судочинстві України та держав англо-саксонської правової системи в контексті міжнародних стандартів : моногр. / Т. В. Садова. – Івано-Франківськ, Надвірна : ЗАТ «Надвірнянська друкарня», 2011. – 177 с.
10. Сегай М. Я. Сучасна парадигма інформатизації судочинства і питання захисту прав і законних інтересів учасників кримінального процесу / М. Я. Сегай // Вісник Академії правових наук України. – 2001. – № 4. – С. 190-198.
11. Тертишник В. М. Кримінально-процесуальне право України : підруч. / В. М. Тертишник. – Київ : А. С. К., 2003. – 1120 с.
12. Тертишник В. Гострі кути реформування кримінального процесу: сім раз... не для нас / В. Тертишник // Право і суспільство. – 2012. – №1. – С. 259-262.
13. Шумило М. Є. Реалізація конституційного принципу таємниці листування, телефонних розмов, телеграфної та іншої кореспонденції у досудових стадіях кримінального процесу України : моногр. / М. Є. Шумило, В. С. Рудей. – Харків : СПДФО Бровін О. В., 2012. – 208 с.
14. Хараберюш І. Ф. Використання оперативно-технічних засобів у протидії злочинам, що вчиняються у сфері нових інформаційних технологій : моногр. / [І. Ф. Хараберюш, В. Я. Мацюк, В. А. Некрасов, О. І. Хараберюш]. – К. : КНТ, 2007. – 196 с.
15. Чабайовський Т. В. Підстави та межі кримінально-процесуального втручання в особисте життя громадян : автореф. дис. ... канд. юрид. наук. Спец. 12.00.09 / Т. В. Чабайовський. – Київ, 2012. – С. 3-16.