

Горпинюк О. П., к.ю.н., доцент,
Львівський державний університет
внутрішніх справ, м. Львів, Україна

УДОСКОНАЛЕННЯ ЗАКОНОДАВЧОГО ВИЗНАЧЕННЯ ЗЛОЧИННИХ ФОРМ ПОРУШЕННЯ НЕДОТОРКАНОСТІ ПРИВАТНОГО ЖИТТЯ (СТАТТЯ 182 КК УКРАЇНИ)

Аналіз злочинних форм поведінки у посяганні, передбаченому ст. 182 КК України, дозволяє виокремити певні недоліки у формулюванні диспозиції зазначеної статті. Зокрема, ст. 182 КК України передбачає кілька альтернативних діянь (збирання, зберігання, використання, поширення, зміна, знищення). Вчинення хоча б однієї з кількох можливих дій передбачає відповідальність за цей злочин. Водночас, М. І. Хавронюк [1, с. 186], С. Я. Лихова [2, с. 282] відзначають, що незаконні використання і поширення конфіденційної інформації про особу завдають їй реальної шкоди, тому суспільна небезпечність таких дій є вищою, ніж суспільна небезпечність збирання і зберігання вказаної інформації. Це має бути відображено у законі шляхом створення у ст. 182 КК двох окремих складів злочинів. Ю. І. Дем'яненко не погоджується з такими пропозиціями і вважає, що незаконне збирання інформації може мати своїм наслідком повне позбавлення власника можливості її використовувати на своє благо (у разі вилучення разом із носієм). Це, на думку автора, може завдавати шкоди фізичній особі, й навіть більшої, ніж її поширення, якщо інформація стосується близьких осіб, родинних відносин тощо. Крім того, на думку Ю. І. Дем'яненко, саме наявність відповідальності за незаконне збирання та зберігання дозволяє боротися з тіньовим злочинним використанням такої інформації [3, с. 189]. Видається, що думки М. І. Хавронюка та С. Я. Лихової є цілком слушними. Адже законодавець в інших статтях КК України завжди вказує на збирання, зберігання інформації з певною метою, або для вчинення інших, більш суспільно небезпечних дій (розголошення інформації). Саме таким способом сконструйовані норми, що передбачають певні діяння: передача або збирання з метою передачі іноземній державі відомостей, що становлять державну таємницю («Шпигунство», ст. 114 КК України); умисне порушення таємниці голосування, що виявилось у розголошенні змісту волевиявлення громадянина («Порушення таємниці голосування», ст. 159 КК України); умисні дії, спрямовані на отримання відомостей, що становлять комерційну або банківську таємницю, з метою розголошення чи іншого використання («незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю», ст. 231 КК України); передача або збирання з метою передачі

іноземним підприємствам відомостей, що становлять конфіденційну інформацію, яка знаходиться у володінні держави («Передача або збирання відомостей, що становлять конфіденційну інформацію, яка знаходиться у володінні держави», ст. 330 КК України). Водночас, не заперечуючи, що збирання і зберігання є менш суспільно небезпечними, ніж використання та поширення інформації, все ж, видається, недоцільно виділяти їх окремою частиною в диспозиції ст. 182 КК України. Часто такі дії, як збирання та зберігання, поєднуються з іншими суспільно небезпечними діями чи навіть передують використанню та поширенню конфіденційної інформації. Здебільшого злочинець спочатку здобуває в незаконний спосіб інформацію, деякий час може зберігати її на комп'ютері, компакт-диску, флеш-карті, а вже згодом збуває чи поширює її іншим особам.

Однак, потрібно наголосити, що продовження тенденції казуалізації шляхом перерахування у диспозиціях статей Особливої частини КК максимально можливої кількості альтернативних діянь, які часто неможливі одне без одного, не може бути схвалене. Диспозиція ст. 182 КК України має бути сформульована так, щоб посягання охоплювало як діяння з інформацією, що зберігається в електронному вигляді, так і без такого. Зокрема, як слушно звертає увагу М. В. Карчевський, досліджуючи злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), розширення кола діянь, заборонених нормою, призводить до ускладнень урахування об'єктивних чинників суспільної небезпечності відповідних посягань. Науковець пропонує незаконні діяння з інформацією з обмеженим доступом позначати зворотом «незаконний доступ до інформації». Головним аргументом на користь такого формулювання науковець називає те, що відповідне законодавче формулювання має охоплювати суспільно небезпечні види незаконного отримання доступу до інформації, поданої в традиційному вигляді (паперовий документ) і до інформації у формі, яка дозволяє здійснювати її обробку за допомогою різноманітних технічних засобів [4, с. 303]. Науковець також звертає увагу, що поняття «доступ до інформації» визначено в законодавстві. Загалом підхід М. В. Карчевського є обґрунтованим, однак аналіз законодавства щодо інформації спонукає до висловлення певних зауважень. Відповідно до Закону України від 5 липня 1994 року «Про захист інформації в інформаційно-телекомунікаційних системах», доступ до інформації в системі – це отримання користувачем можливості обробляти інформацію в системі. Згідно з цим же Законом, а також Законом України від 1 червня 2010 року «Про захист персональних даних», «обробка інформації в системі» чи «обробка персональних даних» – це виконання однієї або кількох операцій: збирання, записування, реєстрація, накопичення, перетворення, зчитування, зберігання, поширення (розповсюдження), знищення тощо, у тому числі з

використанням інформаційних (автоматизованих) систем. Виходячи із зазначених законодавчих положень, «доступ до інформації» – це лише отримання можливості вчиняти дії з інформацією, а безпосередні дії з інформацією охоплюються поняттям «обробка», особливо, якщо інформація певним чином систематизована, в тому числі в електронному вигляді. Крім того, відповідно до Закону України від 13 січня 2011 року «Про доступ до публічної інформації», формулювання поняття «доступ до інформації про особу» передбачає лише можливість ознайомитись із тим, які діяння безпосередньо вчинялися з інформацією, якою була мета вчинення таких дій. Враховуючи викладене, пропонуємо диспозицію ст. 182 КК України сформулювати так: «порушення режиму доступу чи обробки інформації з обмеженим доступом про особу». Вказівка саме на порушення режиму доступу обґрунтовується тим, що таке формулювання вказує на недотримання визначеного законодавством порядку вчинення дій із інформацією. Так, режим доступу до інформації – це передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації. Своєю чергою, вказівка на порушення режиму обробки інформації охоплюватиме дії з інформацією, що систематизована у бази даних, як у формі картотек, так і з використанням автоматизованих інформаційних систем (посягання, що сьогодні є найбільш поширеними). Крім того, законодавче узагальнення всіх можливих діянь з інформацією з обмеженим доступом про особу дозволить уникнути існуючих суперечок серед правників щодо різної суспільної небезпечності дій, шляхом яких вчиняють посягання, передбачене ст. 182 КК України.

Література

1. Хавронюк М. І. Довідник з Особливої частини Кримінального кодексу України / М. І. Хавронюк. – К.: Істина, 2004. – 504 с.
2. Лихова С. Я. Злочини у сфері реалізації громадянських, політичних та соціальних прав і свобод людини і громадянина / С. Я. Лихова. – К.: Видавничо-поліграфічний центр «Київський університет», 2006. – 573 с.
3. Дем'яненко Ю. І. Кримінальна відповідальність за порушення недоторканності приватного життя: дис. ... канд. юрид. наук: 12.00.08 / Юлія Іванівна Дем'яненко. – Х., 2008. – 215 с.
4. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України: монограф. / М. В. Карчевський; Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. – Луганськ: РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. – 528 с.