

7. Мишунин П. Институт прикосновенности к преступлению в советском уголовном праве / П. Мишунин // Социалистическая законность. – 1956. – № 11. – С. 7–16.

8. Молчанова Т., Некрасов В., Корсун С., Усатый Г. Противодействие отмыванию денег: украинско-российский опыт: [монография] / Т. Молчанова, В. Некрасов, С. Корсун, Г. Усатый. – К.: КНТ, 2007. – 238 с.

9. Наумов А. В. Российское уголовное право. Курс лекций. В двух томах. Т. 1. Общая часть. / А. В. Наумов. – [3-е изд., перераб. и доп.]. – М.: Юрид. лит., 2004. – 496 с.

10. Палюх Л. М. До питання про родовий об'єкт злочинів проти правосуддя / Л. М. Палюх // Науковий вісник Львівського державного університету внутрішніх справ. – 2008. – № 3. – С. 275–277.

11. Познышев С. В. Очерк основных начал науки уголовного права. Особенная часть / С. В. Познышев. – М., 1923. – 296 с.

12. Пономаренко Е. В. Некоторые теоретические и законодательные проблемы прикосновенности к преступлению по уголовному праву Российской Федерации: автореф. дис. ... канд. юрид. наук: 12.00.08 / Пономаренко Елена Валерьевна. – Саратов: Саратовская государственная академия права, 2007. – 26 с.

13. Сereжжина К. Н. Прикосновенность к преступлению в уголовном праве России: оптимизация норм и практики их применения: автореф. дис. ... канд. юрид. наук: 12.00.08 / Сereжжина Ксения Николаевна. – Самара, 2009. – 24 с.

14. Семькина О. И. Ответственность за укрывательство преступлений по уголовному праву России: автореф. дис. ... канд. юрид. наук: 12.00.08 / Семькина Ольга Ивановна. – М.: Ставропольский государственный университет, 2003. – 26 с.

УДК 343.132:351.817:654(4ЄС)

**С.В. Єськов**

**РЕГУЛЮВАННЯ ВІДНОСИН  
МІЖ ПРАВООХОРОННИМИ ОРГАНАМИ  
ТА ПРОВАЙДЕРАМИ ТЕЛЕКОМУНІКАЦІЙНИХ  
ПОСЛУГ ЩОДО ВИКОНАННЯ ЗАПИТІВ  
НА ВТРУЧАННЯ У ПРИВАТНЕ СПІЛКУВАННЯ:  
ДОСВІД РАДИ ЄВРОПЕЙСЬКОГО СОЮЗУ**

Стаття присвячена питанням регулювання відносин між правоохоронними органами та провайдерами телекомунікаційних послуг щодо виконання запитів на втручання у приватне спілкування. Розглядається практика Ради Європейського Союзу щодо регулювання цієї діяльності та вітчизняний досвід у цій галузі.

Ключові слова: *втручання у приватне спілкування, негласні слідчі (розшукові) дії, телекомунікаційні послуги, Рада Європейського Союзу.*

Статья посвящена вопросам регулирования отношений между правоохранительными органами и провайдерами телекоммуникационных услуг по исполнению запросов на вмешательство в частное общение. Рассматривается

практика Совета Европейского Союза по регулированию этой деятельности и отечественный опыт в этой области.

Ключевые слова: *вмешательство в частное общение, негласные следственные (розкриття) действия, телекоммуникационные услуги, Совет Европейского Союза.*

Article is devoted to the regulation of relations between law enforcement agencies and providers of telecommunications services to fulfill requests for interference in private communication. The Council of the European Union practice to regulate this activity and domestic experience in this field are analyzed.

Key words: *interference in private communication, covert investigative (detective) actions, telecommunications, the Council of the European Union.*

Законом України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" та Стратегією розвитку інформаційного суспільства в Україні визначено необхідність розвитку таких умов суспільного життя в нашій державі, за яких кожна людина може створювати й накопичувати інформацію та знання, мати до них вільний доступ, користуватися й обмінюватися ними, мати можливість повною мірою реалізувати свій потенціал, сприяти суспільному і особистісному розвитку та підвищувати якість життя. Важливими кроками на цьому шляху нормативно визнано вдосконалення нормативно-правової бази з питань забезпечення розвитку інформаційної сфери та прискорення її адаптації до європейських правових норм і стандартів. Це дає необхідні підстави для констатації чіткого зв'язку обраної для обговорення теми з найважливішими науковими та практичними завданнями, а вдосконалення регламентації втручання у приватне спілкування з урахуванням європейських стандартів дозволяє вважати своєчасним, злободенним та актуальним питанням.

Варто відзначити, що важливість та відповідність потребам сучасності досліджуваної тематики розділяється багатьма вітчизняними науковцями. Її розробці присвятили праці В.П. Кононенко, Я.Ю. Кононюшко, В.Т. Маляренко, В.В. Назаров, Ю.Ю. Орлов, П.П. Підюков, М.А. Погорєцький, Д.Б. Сергєєва, В.О. Серьогін, Н.С. Стефанів, В.Г. Уваров та інші вчені. Водночас у спеціальній літературі основна увага зазвичай приділялася дослідженню прецедентної практики Європейського суду з прав людини, тоді як позиція інших інституцій знаходила відображення лише в поодиноких роботах. Зважаючи на що обставину, як мету презентованої публікації оберемо висвітлення нормотворчої практики Ради Європейського Союзу (далі – Рада ЄС) в контексті регулювання відносин між правоохоронними органами та провайдером телекомунікаційних послуг щодо виконання запитів на втручання у приватне спілкування, а також порівняння з цією практикою вітчизняного досвіду.

Базовими нормативними документами, які дають змогу ознайомитися зі стандартами Ради ЄС щодо регулювання відносин між правоох-

ронними органами та провайдерами телекомунікаційних послуг щодо виконання запитів на втручання у приватне спілкування, є Резолюція Ради ЄС від 17 січня 1995 року "Про законне перехоплення телекомунікацій", Резолюція Ради ЄС від 20 червня 2001 року "Про оперативні запити правоохоронних органів стосовно громадських телекомунікаційних мереж та послуг" та Директива № 2002/58/ЄС Європейського Парламенту й Ради ЄС від 15 грудня 1997 року "Про обробку персональних даних і захист конфіденційності в секторі електронних засобів зв'язку".

Резолюція Ради Європейського Союзу від 17 січня 1995 року "Про законне перехоплення телекомунікацій"<sup>1</sup> присвячена встановленню можливості національних правоохоронних органів проведення перехоплення телекомунікацій й містить стисле викладення пропозицій компетентних правоохоронних органів для технічної реалізації санкціонованого законом перехоплення в сучасних телекомунікаційних системах. Необхідність у прийнятті цього документа виникла через потребу одноманітного врегулювання відносин між правоохоронними органами, уповноваженими на перехоплення, та провайдерами відповідних послуг, унаслідок чого Рада ЄС закликала уряди держав-членів погодити це питання на рівні міністрів, відповідальних за телекомунікації, міністрів юстиції і внутрішніх справ. Інакше кажучи, метою цієї резолюції є забезпечення необхідної платформи для взаємодії постачальників телекомунікаційних послуг і правоохоронних органів щодо виконання оперативних запитів на перехоплення інформації.

Відповідно до положень вказаної резолюції та з урахуванням норм національного законодавства держав-членів ЄС правоохоронні органи з метою належного виконання завдань, що ставляться перед ними, потребують та мають отримати доступ:

- до всіх видів телекомунікацій, зокрема у випадках, коли контрольований об'єкт перехоплення може використовувати функції для переведення дзвінків на інші телекомунікаційні послуги чи термінальне обладнання, включаючи дзвінки, що перетинають більш ніж одну мережу (наприклад, у роумінгу) або обробляються більш ніж одним оператором мережі (постачальником послуг);

- до інформації про зв'язок (у тому числі в режимі реального часу), зокрема: 1) про сигнал щодо стану готовності доступу; 2) для вихідного з'єднання - про номер сторони, з якою зв'язуються, навіть якщо зв'язок не було встановлено; 3) для вхідного з'єднання - про номер сторони, яка зв'язується, навіть якщо зв'язок не було встановлено; 4) про всі сигнали,

---

<sup>1</sup> Council Resolution of 17 January 1995 "On the lawful interception of telecommunications" (96/C 329/01) // Official Journal of the European Communities 4.11.96. - 1996. - No C 329/1. - P. 1-6.

що надходили від об'єктів спостереження, включаючи сигнали після з'єднання, видані для активації функцій, таких, як конференц-зв'язок та передача зв'язку; 5) про початок, кінець та тривалість з'єднання; 6) про фактичне місце призначення та проміжний абонентський номер у разі, якщо зв'язок був переадресований;

- до інформації про якомога точніше географічне місцезнаходження, відоме для відповідної телекомунікаційної мережі;

- до відомостей про особливі послуги, які використовуються контрольованим об'єктом перехоплення, та технічних параметрів для цих видів зв'язку.

Крім цього, оператори мережі (постачальники послуг) відповідно до вказаної резолюції мають забезпечити правоохоронним органам можливість користуватися одним або декількома інтерфейсами, звідки зміст сигналів, що перехоплюються, може бути переданий на контрольні пункти правоохоронних органів. У разі, якщо оператори мережі (постачальники послуг) застосовують кодування, архівацію чи шифрування телекомунікаційного трафіку, правоохоронним органам надаються перехоплені відомості в незашифрованому вигляді. Залежно від рівня поінформованості правоохоронних органів, оператори мережі (постачальники послуг) на їх вимогу зобов'язані повідомляти: а) особу контролюваного за допомогою перехоплення об'єкта, сервісний номер чи інший розпізнавальний ідентифікатор; б) інформацію щодо послуг і функцій телекомунікаційної системи, що використовуються контрольованим об'єктом перехоплення та постачаються йому; в) інформацію щодо технічних параметрів передачі на контрольні пункти правоохоронних органів<sup>1</sup>.

Обов'язковими умовами здійснення перехоплень інформації в телекомунікаційних мережах, які технічно та організаційно забезпечуються операторами (постачальниками послуг), є:

1) утаємниченість цього процесу від об'єкта перехоплення та від будь-якої іншої сторонньої особи й збереження зовнішніх ознак незмінності умов функціонування телекомунікаційного обладнання в цілому;

2) захищеність та конфіденційність інформації, яка має відношення до перехоплення, кількості цих перехоплень, недопустимість її несанкціонованого та неналежного використання;

3) адресність, тобто трансляція перехоплених відомостей лише компетентному органу, визначеному в дозволі на перехоплення;

4) оперативність, яка передбачає швидкість реакції операторів мережі (постачальників послуг) на законні вимоги правоохоронних органів;

---

<sup>1</sup> Резолюція Ради ЄС "Про законне перехоплення телекомунікацій" (96/С 329/01) від 17 січня 1995 року (переклад Центру перекладів актів Європейського права при міністерстві юстиції України) [Електронний ресурс]. – Режим доступу: [http://zakon1.rada.gov.ua/laws/show/994\\_235](http://zakon1.rada.gov.ua/laws/show/994_235). – Назва з екрану.

5) можливість трансляції декількох одночасних перехоплень. Множинні перехоплення можуть вимагатися для забезпечення можливості проведення спостережень більш ніж одним правоохоронним органом в умовах захищеності відомостей про те, які саме органи здійснюють перехоплення, та конфіденційності розслідувань;

6) надійність та якість перехоплення, яка має дорівнювати надійності послуг, що надаються контролюваному об'єкту, та відповідність стандартам якості функціонування, встановлених для певної послуги або виду зв'язку.

Ідею про те, що негласний доступ до телекомунікацій є вкрай важливим в сучасних умовах протидії злочинності, для розкриття тяжких злочинів та переслідування злочинців, розвинуто й в іншому документі Ради ЄС – Резолюції "Про оперативні запити правоохоронних органів стосовно громадських телекомунікаційних мереж та послуг (ENFOPOL)"<sup>1</sup>. Підтвердивши в черговий раз потребу в дотриманні прав осіб на таємницю зв'язку при проведенні заходів щодо перехоплення телекомунікацій, Рада ЄС у зазначеній резолюції звернула увагу на значне розповсюдження негативних явищ у частині використання злочинцями новітніх телекомунікаційних технологій для досягнення протиправних цілей та отримання певних переваг, наданих можливостями телекомунікаційних систем, як з метою уникнення затримання, так і для скоєння злочинів.

Вказавши, що попередню резолюцію з цих питань ("Про законне перехоплення телекомунікацій") було прийнято ще в той час, коли в телекомунікаційній сфері превалювала комутація каналів (а не комутація пакетів – більш сучасний спосіб комутації, коли по одній фізичній лінії зв'язку можуть обмінюватися даними багатьох вузлів), Рада ЄС у резолюції "Про оперативні запити правоохоронних органів стосовно громадських телекомунікаційних мереж та послуг (ENFOPOL)" закріпила низку пояснень й уточнень з урахуванням науково-технічного процесу в цій галузі. У цьому контексті наводяться такі стандарти, протоколи, мережі та послуги, як, наприклад, PSTN, ISDN (цифрова мережа інтегрованих послуг), GPRS, UMTS (універсальна система мобільних телекомунікацій), xDSL, TETRA (транс'європейський стандарт радіозв'язку з автоматичним розподілом каналів), GSM, CDMA, IS-41, AMPS, S-PCS (персональна супутникова система зв'язку) тощо. У принципі, за своїм внутрішнім змістом, резолюція Ради ЄС "Про оперативні запити правоохоронних органів стосовно громадських телекомунікаційних мереж та послуг (ENFOPOL)" є

---

<sup>1</sup> Council Resolution on law enforcement operational needs with respect to public telecommunication networks and services [Electronic Source]. – Mode of access: <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%209194%202001%20INIT>

коментарем до попередніх рішень Ради ЄС з питань перехоплення телекомунікацій стосовно найновіших технологічних рішень<sup>1</sup>.

Враховуючи ту обставину, що розвиток інформаційного суспільства та запровадження нових телекомунікаційних послуг, зокрема успішний транскордонний розвиток таких послуг, здебільшого залежить від віри користувачів в те, що загрози втручання в їхнє особисте життя ці технології не несуть, Рада ЄС спільно з Європейським Парламентом прийняли Директиву № 2002/58/ЄС стосовно обробки персональних даних та захисту права на недоторканність особистого життя у сфері електронних комунікацій. Метою вказаної директиви проголошено гармонізацію положень національного законодавства щодо гарантій відповідного рівня захисту основних прав і свобод, і, зокрема, права на приватне життя та конфіденційність інформації про приватне життя у зв'язку з обробкою персональних даних у сфері електронних комунікацій, і для забезпечення вільного руху таких даних, вільного пересування обладнання для електронного зв'язку та послуг електронного зв'язку. Закріпивши принцип конфіденційності комунікацій та встановивши заборону несанкціонованого прослуховування, підключення, зберігання, будь-яких інших форм перехоплення або стеження за повідомленнями або даними трафіку, директивою допускається обмеження прав людини, зокрема зберігання персональних даних протягом певного періоду, якщо таке обмеження є необхідною, відповідною і пропорційною мірою в рамках демократичного суспільства для здійснення захисту національної безпеки, оборони та громадської безпеки, запобігання, розслідування, виявлення і переслідування злочинних дій або несанкціонованого використання системи електронного зв'язку<sup>2</sup>.

Підбиваючи підсумки висвітлення позиції Ради ЄС зазначимо, що досвід регламентації взаємовідносин між провайдером телекомунікаційних мереж та правоохоронними органами може бути корисним прикладом для нашої держави, оскільки прозорість та деталізація, з якими підійшли до регулювання такої делікатної справи, як втручання у приватне спілкування, потребують уваги та гідні запозичення. Для порівняння: будь-які питання втручання у приватне спілкування або організаційні нюанси співпраці у цьому процесі з провайдером телекомунікаційних послуг відсутні як у "Правилах здійснення діяльності у сфері телекомуні-

---

<sup>1</sup> Резолюція Ради ЄС "Про оперативні запити правоохоронних органів стосовно громадських телекомунікаційних мереж та послуг" (ENFOPOL). [Електронний ресурс]. – Режим доступу: [http://zakon2.rada.gov.ua/laws/show/994\\_234](http://zakon2.rada.gov.ua/laws/show/994_234).

<sup>2</sup> Директива № 2002/58/ЄС Європейського Парламенту і Ради ЄС стосовно обробки персональних даних та захисту права на недоторканність особистого життя в сфері електронних комунікацій [Електронний ресурс]. – Режим доступу: [http://zakon1.rada.gov.ua/laws/show/994\\_b34](http://zakon1.rada.gov.ua/laws/show/994_b34)

кацій (діяльність з надання послуг доступу до Інтернет)", затверджені рішенням Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації № 803 від 10 грудня 2013 р., так й у "Порядку здійснення державного нагляду за ринком телекомунікацій", затвердженому рішенням Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації № 649 від 13 грудня 2012 р.

У "Правилах надання та отримання телекомунікаційних послуг", затверджених постановою Кабінету Міністрів України № 295 від 11 квітня 2012 р. містяться лише загальні згадки про потребу охорони таємниці телефонних розмов, телеграфної чи іншої кореспонденції, що передається технічними засобами телекомунікацій, а також заборону зняття інформації з телекомунікаційних мереж, крім випадків, встановлених законом. Фрагментарні спроби регулювання окремих аспектів втручання у приватне спілкування здійснені в "Порядку взаємодії між СБ України та Адміністрацією Державної служби спеціального зв'язку та захисту інформації України при організації проведення сертифікації технічних засобів телекомунікацій на відповідність вимогам нормативних документів до технічних засобів для здійснення уповноваженими органами оперативно-розшукових заходів у телекомунікаційних мережах загального користування України", однак, як можна впевнитися з вищенаведеного досвіду, цього явно недостатньо. Навряд чи такий підхід відповідає інтересам громадян як користувачів телекомунікаційних послуг та інтересам суб'єктів господарювання, які ці послуги надають.

УДК 658.15.012.8(477)

А.Ю. Кретова

### **СУТНІСТЬ ТА ВЗАЄМОЗВ'ЯЗОК ПОНЯТЬ "ФІНАНСОВА БЕЗПЕКА ПІДПРИЄМСТВ" ТА "ЕФЕКТИВНІСТЬ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА"**

Досліджено поняття "фінансова безпека підприємства", "ефективність діяльності підприємства"; розглянуто ефективність діяльності підприємства відповідно до актуальності вияву ефекту та чинника часу; запропоновано теперішню ефективність діяльності підприємства оцінювати за критерієм "фінансова безпека підприємства".

Ключові слова: *економічна безпека підприємства, фінансова безпека підприємства, ефективність діяльності підприємства, результативність діяльності підприємства, теперішня ефективність діяльності підприємства.*

Исследованы понятия "финансовая безопасность предприятия", "эффективность деятельности предприятия"; рассмотрена эффективность деятельности предприятия в соответствии с актуальностью проявления эффекта и фактора времени; предложено нынешнюю эффективность деятельности предприятия оценивать по критерию "финансовая безопасность предприятия".