УДК 351.81.085 (477)
DOI https://doi.org/10.32847/ln.2022.18.25

Назимко Є.С.
перший проректор
Донецького державного університету внутрішніх справ,
доктор юридичних наук, професор

Малаховська І.Б.
кандидат юридичних наук

Пономарьова Т.І.
завідувач науково–дослідної лабораторії з проблем запобігання
кримінальним правопорушенням
Донецького державного університету внутрішніх справ,
кандидат юридичних наук

НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ МЕРЕЖАХ

Постановка проблеми. Захист персональних даних громадян є одним із пріоритетних завдань, які на сьогоднішній день стоять перед державою. На ґрунті стрімкого розвитку глобального інформаційного суспільства, інформаційних та електронних комунікаційних технологій наразі спостерігаються кардинальні трансформаційні процеси у сфері захисту інформації, що не може не позначатися на діяльності Національної поліції в процесі доступу до інформаційних ресурсів, які містять персональні дані. Нерідкими є випадки несанкціонованого розповсюдження персональних даних, що не тільки спричиняє збитки численним вітчизняним та міжнародним організаціям, але й порушує права громадян на недоторканність приватного життя, особисту та сімейну таємницю.

Особливої актуальності це питання набуває у зв'язку із необхідністю доступу правоохоронних органів до різного роду інформації під час реалізації службових повноважень. Аналіз нормативно-правової бази свідчить про те, що, не дивлячись на достатню кількість нормативних актів і документів, низка проблемних питань, пов'язаних із регулюванням особливостей доступу поліції до персональних даних залишається відкритою для дискусій. Зокрема це також стосується тих даних, які знаходяться в електронних комунікаційних мережах.

Аналіз останніх досліджень і публікацій. Проблема забезпечення захисту персональних даних в діяльності Національної поліції України не є новою для правових наук та розглядалась у працях таких учених як Ю.К. Базанов, В.М. Брижко, В.М. Гуцалюк, І.В. Костенко, Д.В. Цвірюк, В.С. Цимбалюк, М.Я. Швець, О.М. Шевчук та інші. При цьому, окремі проблеми встановлення правових засад доступу уповноважених підрозділів Національної поліції до персональних даних в електронних комунікаційних мережах залишаються невирішеними, що і зумовлює актуальність обраної для дослідження теми.

Метою статті є розгляд та узагальнення правових засад доступу уповноважених підрозділів Національної поліції до персональних даних в електронних комунікаційних мережах.

Викладення основного матеріалу. Забезпечення Національною поліцією захисту гро-

мадян від кримінально протиправних посягань, ефективне розкриття та розслідування вчинених правопорушень за сучасних умов неможливе без використання інформації, значна концентрація якої фокусується у мережах електронного комунікаційного зв'язку. Разом із цим, діяльність органів та підрозділів Національної поліції в цьому напрямі обмежується положеннями статті 31 Конституції України, яка гарантує кожній особі таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції. При цьому, винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти кримінальному правопорушенню чи з'ясувати істину в кримінальному провадженні, якщо іншими способами одержати інформацію неможливо [1]. Забезпечення інформаційної безпеки під час кримінального провадження та реалізації функціональних обов'язків працівниками правоохоронних органів є важливим аспектом в межах правової діяльності, що сприяє дотриманню прав та свобод людини і громадянина, а також свідчить про прагнення держави відповідати європейським та міжнародних стандартам відправлення правосуддя.

У загальному вигляді ключовим аспектом триваючої й дотепер дискусії залишається пошук розумного балансу між дотриманням прав громадян на невтручання у їх особисте життя, в частині доступу до їх персональних даних, а з іншого – законна діяльність правоохоронних органів щодо забезпечення публічного порядку та державної безпеки. Т. Обуховська з цього приводу зазначає про необхідність поєднання принципу недоторканності особи із принципом недоторканності власності. Тобто, на думку вченої, «особливої уваги потребує проблема врегулювання балансу інтересів сторін: особистості, суспільства і держави, на основі механізму взаємоврахування інтересів [2, с. 101]. Пошук оптимального балансу потребує створення виваженої нормативно–правової бази, яка б створювала алгоритм, необхідний для забезпечення нормального перебігу досудового розслідування із урахуванням прав та особистих інтересів громадян країни.

При цьому, необхідно також звернути увагу на те, що в контексті першого аспекту ефективна організація процесу надання електронних комунікаційних послуг виступає надійною гарантією реалізації громадянами права на приватність, в тому числі, й у сфері захисту персональних даних [3, с. 90]. Разом з цим, один із суттєвих проявів безпосереднього втручання у особисте та сімейне життя громадян дійсно пов'язаний із діяльністю органів та підрозділів Національної поліції, в процесі зняття інформації з електронних комунікаційних мереж.

У національному законодавстві право на таємницю особистого та сімейного життя врегульовано низкою законодавчих актів, першорядне місце серед яких посідає Конституція України, стаття 32 якої передбачає заборону втручання у особисте та сімейне життя осіб, за винятком випадків, передбачених Конституцією України. Частина 2 коментованої статті також містить заборону обігу конфіденційної інформації про особу без її згоди, однак, передбачає й певні виключення із цього правила, а саме: а) підстави, визначені законом; б) інтереси національної безпеки, економічного добробуту та прав людини [1]. Отже, на конституційному рівні визначено цінність захисту особистого життя громадян, що, в свою чергу, створює платформу для формування відповідної нормативно-правової бази, яка забезпечить можливість здійснювати правоохоронні та судові функції із урахуванням принципу законності.

Низку основоположних правил щодо забезпечення захисту особистого життя від свавільного втручання містить й Цивільний кодекс України, стаття 301 якого прямо передбачає право фізичної особи на особисте життя. Доволі чіткою та справедливою є позиція законодавця, висловлена у частині 2 цієї статті, яка пов'язана із власним визначенням фізичної особи кола та меж свого особистого життя та можливості ознайомлення з ним

інших осіб [4]. Також із змісту статті 306 ЦК України можемо зробити висновок, що правовою категорією «кореспонденція» охоплюються не тільки листи та будь-які письмові документи, але й всі інші матеріальні та віртуальні носії інформації, а саме: телеграми, телефонні розмови, телеграфні повідомлення та інші види кореспонденції. Така позиція підтверджується й переважною більшістю науковців, які вкладають у термін «кореспонденція» такі її різновиди, як: телефонні розмови, телеграфні повідомлення, повідомлення електронною поштою, пейджером, SMS-повідомлення тощо. В ч. 5 цієї статті вказано, що порушення таємниці кореспонденції може бути дозволено судом у випадках, встановлених законом, з метою запобігання кримінальному правопорушенню чи під час кримінального провадження, якщо іншими способами одержати інформацію неможливо [4]. Отже, останнім положенням законодавець чітко окреслив випадки, в яких доступ до кореспонденції може бути дозволений, зокрема, такими випадками було встановлено саме необхідність захисту інтересів суспільства та держави, які можуть бути порушені у зв'язку зі вчиненням чи потенційною загрозою вчинення кримінального правопорушення.

Водночас, охорона права громадян на втручання у їх особисте життя на законодавчому рівні визначена Кримінальним кодексом України, стаття 163 якого передбачає відповідальність за порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер [5].

Таким чином, аналіз вищенаведених законодавчих актів надав змогу висловити з цього приводу певні міркування.

1. Слід констатувати доволі значний масив законодавчих актів, які визначають, на перший погляд, досконалий механізм забезпечення захисту особистої інформації громадян від втручання правоохоронних органів.

2. Складається доволі парадоксальна ситуація, коли законодавець на конституційному та законодавчому рівні намагається доволі ретельно захистити особисту таємницю, не визначаючи при цьому її зміст. Наприклад, за результатами аналізу конституційних норм доходимо висновку, що всі врегульовані національним законодавством таємниці можна розділити на: а) державні; б) особисті; в) інші, під якими, вірогідно, розуміються таємниці за сферами соціально-економічних відносин, а саме: банківська, лікарська, адвокатська та ін.

3. У той же час, на відміну від особистої, розуміння державної таємниці доволі повно розкрито в Законі України «Про державну таємницю», стаття 1 якого визначає останню як «вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою» [6]. Тобто державна таємниця представлена у вигляді сукупності відомостей у різних сферах державного управління, які функціонують в режимі таємної інформації.

4. Разом з цим, сукупність відомостей, які утворюють поняття особистої таємниці в жодному з проаналізованих законодавчих актів не визначено. Наприклад, якщо вважати, що зміст особистої таємниці складатиме таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції, то як визначити правовий режим захисту персональних даних, які містяться в мережі Інтернет, а саме: в хмарних сервісах, соціальних мережах, Інтернет-магазинах тощо. Уявляється, що вказана персоніфікована інформація також буде складати зміст особистої таємниці.

Тому, вважаємо за доцільне сформулювати визначення особистої таємниці як виду таємної інформації про фізичну особу, яка включає персональні дані цієї особи та іншу персоніфіковану інформацію, яка підлягає охороні державою, а її розголошення може завдати шкоди інтересам фізичної особи. Із наведеного визна-

чення стає зрозумілим, що особиста таємниця включає два різновиди інформації: а) персональні дані; б) інша персоніфікована інформація, яка, на нашу думку, включає персональні дані, функціонування яких врегульоване спеціальними законами України.

З іншого боку, аналіз законодавчих актів у сфері захисту персональних даних дає підстави для висновку про наявність виключень із загального конституційного правила про заборону втручання у особисте життя громадян. Саме такі виключення й слугують підставою для правомірного втручання Національної поліції у приватне життя громадян, шляхом доступу до їх персональних даних в електронних комунікаційних мережах.

Слід зазначити, що порядок доступу до персональних даних, які містяться у електронних комунікаційних мережах врегульований низкою законодавчих та підзаконних актів.

Зокрема, Кримінальний процесуальний кодекс України доволі докладно врегульовує порядок втручання у приватне спілкування громадян, різновидами якого, відповідно до статті 258 КПК, є: 1) аудіо-, відеоконтроль особи; 2) арешт, огляд і виїмка кореспонденції; 3) зняття інформації з електронних комунікаційних мереж; 4) зняття інформації з електронних інформаційних систем [7]. Стаття 263 коментованого законодавчого акту врегульовує процедурні питання щодо зняття інформації з електронних комунікаційних мереж. Так, в ч. 4 коментованої статті вказано, що зняття інформації з електронних комунікаційних мереж покладається на уповноважені підрозділи органів Національної поліції, Бюро економічної безпеки України, Національного антикорупційного бюро України, Державного бюро розслідувань та органів безпеки. Керівники та працівники операторів електронних комунікацій зобов'язані сприяти виконанню дій із зняття інформації з електронних комунікаційних мереж, вживати необхідних заходів щодо нерозголошення факту проведення таких дій та отриманої інформації, зберігати її в незмінному вигляді [7]. Таким чином, кримінальне процесуальне законодавство передбачає чіткий перелік суб'єктів, які можуть мати доступ до електронних комунікаційних мереж з метою зняття інформації.

Водночас, уявляється, що в наведеному правовому положенні дискусійним виглядає розуміння сприяння правоохоронним органам та його змістовного наповнення. Відповідь на це запитання частково надана в Законі України «Про електронні комунікації». Так, в ст. 121 вказано, що доступ до інформації про споживача, факти надання електронних комунікаційних послуг, у тому числі до даних, що обробляються з метою передачі такої інформації в електронних комунікаційних мережах, здійснюється виключно на підставі рішення прокурора, суду, слідчого судді у випадках та порядку, передбачених законом. Зняття інформації з електронних комунікаційних мереж постачальників електронних комунікаційних послуг забезпечується єдиною системою технічних засобів, що використовується всіма уповноваженими законом органами, на умовах автономного доступу до інформації у порядку, визначеному законодавством. Постачальник електронних комунікаційних послуг та/або мереж повинен забезпечити можливість підключення технічних засобів, зазначених у частині другій цієї статті, в точці для такого доступу в електронній комунікаційній мережі, визначеній постачальником електронних комунікаційних мереж та/або послуг [8]. Отже, наведені положення свідчать про наявність чіткого алгоритму надання доступу до інформації, яка міститься в електронних комунікаційних мережах, зокрема увага законодавцем акцентована на необхідності наявності рішення прокурора, суду, слідчого судді для зняття даних з таких мереж.

Підстави та порядок зняття інформації з каналів зв'язку в електронних комунікаційних мережах підрозділами Національної поліції, які здійснюють оперативно-розшукову діяльність, також визначено статтею 8 Закону України «Про оперативно-розшукову діяльність», в якій вказано, що оперативним

підрозділам для виконання завдань оперативно-розшукової діяльності надається прав здійснювати аудіо-, відеоконтроль особи, зняття інформації з електронних комунікаційних мереж, електронних інформаційних мереж згідно з положеннями статей 260, 263-265 Кримінального процесуального кодексу України [9]. Вказана норма має відсильний характер, адже передбачає реалізацію цієї діяльності відповідно до ст.ст. 260, 263-265 Кримінального процесуального кодексу України.

У той же час, в ч. 3 коментованої статті вказано, що негласне обстеження публічно недоступних місць, житла чи іншого володіння особи, аудіо-, відеоконтроль особи, аудіо-, відеоконтроль місця, спостереження за особою, зняття інформації з електронних комунікаційних мереж, електронних інформаційних мереж, накладення арешту на кореспонденцію, здійснення її огляду та виїмки, установлення місцезнаходження радіоелектронного засобу проводяться на підставі ухвали слідчого судді, постановленої за клопотанням керівника відповідного оперативного підрозділу або його заступника, погодженого з прокурором. Ці заходи застосовуються виключно з метою запобігання вчиненню тяжкого або особливо тяжкого злочину, запобігання і припинення терористичних актів та інших посягань спеціальних служб іноземних держав та організацій, якщо іншим способом одержати інформацію неможливо [9]. Вказане правове положення яскраво демонструє намагання законодавця встановити суворо визначені правові межі діяльності правоохоронних органів у сфері доступу до персональних даних, які містяться в електронних комунікаційних мережах. Такий висновок підтверджується й сформульованою метою застосування вищенаведених оперативно-розшукових заходів, які здійснюються, відповідно до тієї ж норми, виключно з метою запобігання вчиненню тяжкого або особливо тяжкого злочину, запобігання і припинення терористичних актів та інших посягань спеціальних служб іноземних держав та організацій, якщо іншим способом одержати інформацію неможливо [9].

Закон України «Про державний захист працівників суду і правоохоронних органів», серед видів спеціальних заходів забезпечення безпеки передбачає використання технічних засобів контролю і прослуховування телефонних та інших переговорів, а також візуальне спостереження, що також можна розцінювати в якості збору персоніфікованої інформації (стаття 5 Закону). Підстави та умови застосування наведених заходів деталізовані у статті 8 коментованого законодавчого акту, яка, зокрема, передбачає, що в разі загрози вчинення насильства або інших протиправних дій щодо осіб, взятих під захист, за письмовими заявами або згодою цих осіб може проводитися прослуховування телефонних та інших переговорів. У ході прослуховування переговорів осіб, взятих під захист, може застосовуватися звукозапис [10]. Аналогічні додаткові підстави доступу до персональних даних осіб, які беруть участь у кримінальному судочинстві викладені у ст.ст. 7, 10 Закону України «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві» [11].

Аналіз вказаних норм дозволяє класифікувати підстави доступу уповноважених підрозділів Національної поліції до персональних даних на основні та додаткові. Основні підстави визначені Кримінальним процесуальним кодексом України, та передбачають обов'язкову наявність: а) клопотання керівника відповідного оперативного підрозділу Національної поліції або його заступника; б) погодження прокурора; в) ухвали слідчого судді. Разом з цим, існують і додаткові підстави доступу до персональних даних, які, наприклад, в Законах «Про державний захист працівників суду і правоохоронних органів» та «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві» виражені у наявності загрози вчинення насильства або інших протиправних дій щодо осіб, взятих під захист. Крім того, закон вимагає обов'язкової згоди охоронюваних осіб на

фактичне втручання уповноважених підрозділів Національної поліції у їх особисте життя або написання ними письмової заяви. Уявляється, що головна особливість застосування основних та додаткових підстав доступу до персональних даних полягає у взаємозалежності цих підстав, жодна з них не застосовується самостійно, а застосування додаткових підстав є процесуальним продовженням щодо застосування основних.

Висновки. Проведене дослідження дозволило підсумувати, що обрання конкретних заходів захисту, технічних рішень, керівних стандартів, архітектоніки інформаційних систем, оцінювання ризиків неправомірного доступу до конфіденційної інформації залишається у віданні розпорядників персональних даних. Останні самостійно визначають необхідні заходи захисту даних, із врахуванні їх правової природи та обсягу, вартості захисного обладнання, характеристик інформаційних систем тощо. Крім цього, у більшості законодавчих актів країн ЄС міститься норма про необхідність врахування економічної доцільності заходів щодо захисту персональних даних, за умови відсутності вимог щодо встановлення будь-яких конкретних заходів захисту персональних даних. Тобто в законодавчих актах зарубіжних країн встановлюються вимоги стосовно змістовної характеристики захисту персональних даних, тоді як у національній правовій практиці підзаконними нормативно-правовими актами встановлені формальні вимоги, які фактично не мають відношення до змістовного забезпечення захисту персональних даних.

Анотація

У статті розглядаються особливості захисту персональних даних, які містяться в електронних комунікаційних мережах. Вказано, що особливої актуальності це питання набуває у зв'язку із необхідністю доступу правоохоронних органів до різного роду інформації під час реалізації службових повноважень. Аналіз нормативно-правової бази свідчить про те, що, не дивлячись на достатню кількість нормативних актів і документів, низка проблемних питань, пов'язаних із регулюванням особливостей доступу поліції до персональних даних залишається відкритою для дискусій. Зокрема це також стосується тих даних, які знаходяться в електронних комунікаційних мережах. Звертається увага на те, що в країнах, які імплементували у національне законодавство норми міжнародних документів, відсутні будь-які спеціальні заходи захисту, крім загальноприйнятих, які висуваються до володільців персональних даних, компетенція яких обмежується питаннями управління інформаційною безпекою та підготовкою кваліфікованого персоналу. Поряд з цим, обрання конкретних заходів захисту, технічних рішень, керівних стандартів, архітектоніки інформаційних систем, оцінювання ризиків неправомірного доступу до конфіденційної інформації залишається у віданні розпорядників персональних даних. Останні самостійно визначають необхідні заходи захисту даних, із врахуванні їх правової природи та обсягу, вартості захисного обладнання, характеристик інформаційних систем тощо. Пошук оптимального балансу потребує створення виваженої нормативно–правової бази, яка б створювала алгоритм, необхідний для забезпечення нормального перебігу досудового розслідування із урахуванням прав та особистих інтересів громадян країни. Констатовано, що доволі значний масив законодавчих актів, які визначають, на перший погляд, досконалий механізм забезпечення захисту особистої інформації громадян від втручання правоохоронних органів, фактично не відповідає вимогам сьогодення.

Ключові слова: персональні дані, електронні комунікаційні мережі, досудове розслідування, кримінальне провадження, захист прав, Національна поліція, державна таємниця, несанкціоноване розповсюдження.

Nazymko Ye.S., Malakhovska I.B., Ponomarova T.I. Legal regulation of personal data protection in electronic communication networks

The article considers the features of protection of personal data contained in electronic communication networks. It is indicated that this issue becomes particularly relevant in connection with the need for law enforcement agencies to access various types of information during the exercise of their official powers. The analysis of the legal framework shows that, despite the sufficient number of normative acts and documents, a number of problematic issues related to the regulation of the peculiarities of police access to personal data remain open for discussion. In particular, this also applies to those data that are in electronic communication networks. Attention is drawn to the fact that in countries that have implemented the norms of international documents into national legislation, there are no special protection measures, other than generally accepted ones, which are put forward to the owners of personal data, whose competence is limited to issues of information security management and the training of qualified personnel. Along with this, the selection of specific protection measures, technical solutions, management standards, architecture of information systems, assessment of risks of unauthorized access to confidential information remains in the hands of personal data controllers. The latter independently determine the necessary data protection measures, taking into account their legal nature and scope, the cost of protective equipment, characteristics of information systems, etc. The search for an optimal balance requires the creation of a balanced regulatory and legal framework, which would create an algorithm necessary to ensure the normal course of the pre-trial investigation, taking into account the rights and personal interests of the country's citizens. It was established that a rather significant array of legislative acts, which define, at first glance, a perfect mechanism for ensuring the protection of personal information of citizens from interference by law enforcement agencies, actually do not meet the requirements of today.

Key words: personal data, electronic communication networks, pre-trial investigation, criminal proceedings, protection of rights, National Police, state secret, unauthorized distribution.

Список використаних джерел:

1. Конституція України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text
2. Обуховська Т. Захист персональних даних в умовах розвитку інформаційного суспільства: передумови, принципи та міжнародне законодавство. *Вісник НАДУ*. 2014. №1. С. 95-103.
3. Курочка М.Й. Законність в ОРД та прокурорський нагляд за її дотриманням: Монографія / За ред. члена-кореспондента АпрН України. Луган. ін-т внутр. справ. Луганськ: РВВ ЛІВО, 2001. 210 с.
4. Цивільний кодекс України від 16 січня 2003 р. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text
5. Кримінальний кодекс України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14
6. Про державну таємницю від 21.01.1994 № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text
7. Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text
8. Про електронні комунікації від 16.12.2020 № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text
9. Про оперативно-розшукову діяльність від 18.02.1992 № 2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text
10. Про державний захист працівників суду та правоохоронних органів від 23.12.1993 № 3781-XII. URL: https://zakon.rada.gov.ua/laws/show/3781-12#Text
11. Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві від 23.12.1993 № 3782-XII. URL: https://zakon.rada.gov.ua/laws/show/3782-12#Text