

ПИТАННЯ ЗАБЕЗПЕЧЕННЯ ПРАВА ОСОБИ НА ПОВАГУ ДО ПРИВАТНОГО ЖИТТЯ У КІБЕРПРОСТОРІ В ПРАКТИЦІ ЄВРОПЕЙСЬКОГО СУДУ З ПРАВ ЛЮДИНИ

ISSUES OF ENSURING THE RIGHT TO RESPECT FOR PRIVATE LIFE IN CYBERSPACE IN THE CASE-LAW OF THE EUROPEAN COURT OF HUMAN RIGHTS

Філімонов М.В., аспірант кафедри кримінального процесу
Національний університет «Одеська юридична академія»

Стаття присвячена аналізу практики Європейського суду з прав людини щодо тлумачення та застосування статті 8 Конвенції про захист прав людини і основоположних свобод у контексті втручання держави у сферу електронного приватного спілкування та обробки цифрових даних. У межах дослідження узагальнено підходи Суду до визначення меж допустимого втручання у приватне життя в умовах використання сучасних інформаційно-комунікаційних технологій та здійснення прихованих форм спостереження.

Проаналізовані рішення ЄСПЛ, зокрема у справах *Roman Zakharov v. Russia*, *Szabó and Vissy v. Hungary*, *Centrum för Rättvisa v. Sweden*, *Big Brother Watch and Others v. the United Kingdom*, *Ekimdzhiev and Others v. Bulgaria*, дозволяють дійти висновку, що Суд послідовно розглядає «якість закону» як ключову передумову відповідності національних режимів втручання в електронні комунікації стандартам ст. 8 Конвенції про захист прав людини та основоположних свобод. Вона передбачає не лише формальну наявність правової підстави, а й достатній рівень чіткості, передбачуваності та доступності правового регулювання для осіб, яких воно стосується.

Узагальнюючи практику ЄСПЛ, автор доходить висновку, що правомірність втручання у цифрове приватне спілкування з точки зору статті 8 Конвенції зумовлюється дотриманням сукупності взаємопов'язаних критеріїв, серед яких визначальними є: 1) наявність ефективного попереднього або наступного судового контролю; 2) чітке обмеження дискреційних повноважень органів державної влади; 3) встановлення прозорих і загальнодоступних правил щодо збирання, зберігання, доступу, використання, передачі та знищення електронних даних; 4) наявність дієвих механізмів незалежного нагляду; реальне забезпечення процедур інформування особи та ефективних засобів правового захисту. Сукупне дотримання цих критеріїв розглядається ЄСПЛ як необхідна умова забезпечення належного балансу між інтересами національної безпеки, ефективності кримінального переслідування та захистом права особи на повагу до приватного життя у кіберпросторі.

Ключові слова: кримінальне провадження, доказування, слідчі (розшукові) дії, втручання у приватне життя, таємниця спілкування, кіберпростір, судовий контроль, Європейський суд з прав людини.

The article is devoted to the analysis of the case-law of the European Court of Human Rights concerning the interpretation and application of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms in the context of State interference with electronic private communications and the processing of digital data. Within the framework of the study, the approaches developed by the Court to defining the limits of permissible interference with private life in the conditions of modern information and communication technologies and covert forms of surveillance are systematised.

An analysis of the ECtHR judgments, in particular in the cases of *Roman Zakharov v. Russia*, *Szabó and Vissy v. Hungary*, *Centrum för Rättvisa v. Sweden*, *Big Brother Watch and Others v. the United Kingdom*, and *Ekimdzhiev and Others v. Bulgaria*, makes it possible to conclude that the Convention consistently regards the “quality of law” as a key prerequisite for the compliance of national regimes governing interference with electronic communications with the standards of Article 8 of the Convention. This requirement implies not only the formal existence of a legal basis, but also a sufficient degree of clarity, foreseeability and accessibility of the relevant legal regulation for the persons concerned.

Summarising the ECtHR's case-law, the author concludes that the lawfulness of interference with digital private communications under Article 8 of the Convention depends on compliance with a set of interrelated criteria. Among the decisive ones are: 1) the existence of effective prior or subsequent judicial review; 2) clear limitations on the discretionary powers of public authorities; 3) the establishment of transparent and publicly accessible rules governing the collection, retention, access, use, transfer and destruction of electronic data; 4) the presence of effective mechanisms of independent oversight; and the genuine обеспечение of procedures for notifying individuals and of effective remedies. The cumulative observance of these criteria is regarded by the ECtHR as a necessary condition for ensuring a proper balance between the interests of national security, the effectiveness of criminal prosecution, and the protection of the individual's right to respect for private life in cyberspace.

Key words: criminal proceedings; evidentiary process; investigative (search) measures; interference with private life; secrecy of communications; cyberspace; judicial control; European Court of Human Rights.

Вступ. Рішення Європейського суду з прав людини (далі – ЄСПЛ, Суд) мають фундаментальне значення для розвитку та функціонування національної правової системи, адже виступають джерелом тлумачення положень Конвенції про захист прав людини і основоположних свобод. Правові позиції, викладені у них забезпечують наповнення конвенційних норм реальним змістом, формують єдині стандарти захисту прав людини у держава-членах Ради Європи та виступають орієнтиром у правозастосуванні для національних судів.

Суд у свої рішеннях традиційно дотримується принципу динамічного тлумачення її положень, який передбачає адаптацію вже наявних позицій та підходів до змін, які обумовлені у тому числі й науково-технічним прогресом. Це стосується й питання про забезпечення права на повагу до приватного та сімейного життя у кіберпросторі.

У класичній інтерпретації, право на повагу до приватного і сімейного життя, житла і кореспонденції, гарантоване ст. 8 Конвенції у кримінально-правовому вимірі стосується аспектів, пов'язаних із втручанням у сферу

таємниці спілкування, кореспонденції та недоторканості житла або іншого володіння. Але тотальна цифровізація усіх сфер суспільного життя дедалі частіше породжує питання про застосовність основних підходів, сформульованих Судом щодо стандартів захисту прав, передбачених ст. 8 Конвенції у ситуаціях, коли їх порушення здійснюється у цифровому середовищі.

І хоча Суд послідовно наголошує, що будь-яке втручання у цифрову сферу приватного життя також повинно відповідати вимогам законності, легітимної мети та необхідності у демократичному суспільстві, а національне законодавство має містити чіткі, передбачувані та ефективні гарантії від зловживань, очевидно, що цей аспект має свою специфіку. Це обумовлює необхідність з'ясування правових позицій Суду у цьому контексті задля адаптації національного законодавства та правозастосовної практики до стандартів ст. 8 Конвенції.

Аналіз останніх досліджень та публікацій. До питання забезпечення права особи на повагу до приватного життя у доктрині звертались І.В. Басиста, Л.П. Брич,

В.К. Волошина, В.І. Галаган, І.В. Гловюк, О.П. Горпинюк, О.М. Дроздов, В.А. Завтур, О.В. Капліна, Г.Р. Крет, О.П. Кучинська, Л.М. Лобойко, В.В. Матолич, В.Т. Нор, М.А. Погорєцький, В.О. Серьогін, М.М. Стоянов, Л.Д. Удалова, Ж.В. Удовенко, Т.І. Фулей, О.Г. Яновська.

Водночас, проблеми забезпечення права особи на повагу до приватного життя у кіберпросторі в контексті практики ЄСПЛ лишаються малодослідженими у вітчизняній кримінальній процесуальній доктрині.

Метою даної статті є виокремлення основних стандартів, які сформовані у практиці ЄСПЛ щодо забезпечення права на повагу до приватного життя у кіберпросторі.

Основні результати дослідження. Однією із перших справ, у яких порушувалося питання про забезпечення права на приватне життя у контексті цифрових технологій та кіберпростору була справа «Роман Захаров проти Росії» (*Zakharov v. Russia*). Заявник стверджував, що російське законодавство про оперативно-розшукову діяльність дозволяло таємне перехоплення його телефонних і електронних комунікацій без достатніх правових гарантій. Він не вказував, що відносно нього здійснювалося прослуховування, але зазначав, що сама наявність правового режиму масового перехоплення створює постійну загрозу втручання у його приватне життя.

Ключовим питанням у цій справі було відповідність системи SORM (*System for Operative Investigative Measures*), яка надавала російським органам безпеки прямий технічний доступ до мереж операторів зв'язку вимогам ст. 8 Конвенції. Судові дозволи на перехоплення, навіть якщо формально вимагалися, не забезпечували ефективного попереднього та подальшого контролю, оскільки оператори не могли перевірити законність доступу, а особа не інформувалася про втручання навіть постфактум.

Суд дійшов висновку про порушення ст. 8 Конвенції у цій справі, зазначивши, що російська система перехоплення електронних комунікацій порушує статтю 8 Конвенції, оскільки не відповідає вимогам якості закону, передбачуваності, пропорційності та ефективного судового контролю. Аналізована справа стала доволі важливим прецедентом щодо захисту права на приватність у контексті сучасних цифрових комунікацій [1].

Одним із ключових рішень у розглядуваному аспекті є також рішення ЄСПЛ у справі «Сабо та Віссі проти Угорщини» (*Szabó and Vissy v. Hungary*). Заявники у цій справі ставили питання про відповідність стандартам ст. 8 Конвенції положень законодавства, яке дозволяло таємне стеження, включно з доступом до цифрових даних та перехопленням електронних комунікацій.

У цій справі ЄСПЛ підкреслив, що для звернення до Суду не має необхідності доводити факт реального стеження, якщо закон створює реальну загрозу втручання у такий спосіб.

Суд констатував порушення ст. 8, оскільки закон дозволяв перехоплення без вимоги індивідуалізації особи і не вимагав зв'язку між особою та загрозою нацбезпеці. Фактично, це створювало умови для масового та невибіркового цифрового стеження. Крім того, дозвіл на таємне спостереження надавався посадовою особою, що є представником виконавчої влади, натомість судовий контроль до початку втручання був відсутній. Це доволі важливий висновок, який Суд сформулював саме у аналізованій справі, оскільки він встановив стандарт, відповідно до якого контроль з боку виконавчої влади не може замінити судовий контроль, особливо в випадках, коли мова йде про обмеження прав у цифровому середовищі, де втручання у момент його здійснення не є очевидним.

Водночас, Судом були встановлені й інші порушення, зокрема, у контексті строків перехоплення, які могли продовжуватися без обмежень, відсутність чітких правил щодо зберігання електронних даних, їх подальшого вико-

ристання та знищення. У підсумку Суд дійшов висновку, що угорська система не забезпечувала мінімальний рівень захисту від свавільного втручання, оскільки на практиці дозволяла практично необмежене таємне перехоплення електронних комунікацій [2].

Питання дотримання стандартів ст. 8 Конвенції у контексті перехоплення електронних комунікацій розглядалося також Судом у справі «Centrum för Rättvisa v. Sweden». У ній шведська правозахисна організація ставила питання про відповідність ст. 8 Конвенції системи масового перехоплення комунікацій, що здійснювалося Національною радіотехнічною установою Швеції. Зокрема, заявники стверджували про невідповідність вимогам якості законодавства процедур перехоплення кабельних електронних комунікацій (інтернет-трафіку, електронної пошти, тощо), збору та автоматизованої обробки метаданих, а також зберігання та аналізу великих масивів цифрової інформації в інтересах зовнішньої розвідки та національної безпеки.

Суд дійшов висновку, що загалом законодавство містить певні гарантії від можливих зловживань з боку органів влади, зокрема, відповідний закон забороняв обробку персональних даних лише на основі інформації про расу або етнічне походження особи, політичні, релігійні чи філософські переконання, членство в профспілці, стан здоров'я або сексуальну орієнтацію. Водночас, Суд зазначив, що закон не вимагав врахування інтересів конфіденційності відповідної особи при прийнятті рішення про обмін інформацією, що є серйозною прогалиною у національному законодавчому режимі перехоплення комунікацій, яку він має враховувати при оцінці сумісності цього режиму зі статтею 8 Конвенції (п. 330).

Крім того, Суд дійшов висновку про те, що механізм подальшого контролю не забезпечував реальної ефективності, зокрема, зацікавлені особи не мали права отримувати відповіді на скарги щодо фактів перехоплення, що могло породжувати у них обгрунтоване побоювання, що їх права були свавільно обмежені.

У підсумку Суд виснував, що основні характеристики шведського режиму масового перехоплення відповідають вимогам Конвенції щодо якості закону, і вважає, що в тому вигляді, в якому цей режим функціонував на момент його розгляду Палатою, він у більшості своїх аспектів залишався в межах того, що є «необхідним у демократичному суспільстві». Але водночас дійшов висновку, що виявлені недоліки не є належним чином компенсованими наявними гарантіями, а отже, шведський режим масового перехоплення виходить за межі дискреції, наданої органам держави-відповідача у цій сфері [3].

Безумовно, одним із найбільш фундаментальних рішень ЄСПЛ у контексті масового цифрового спостереження на сьогодні є справа «Big Brother Watch and Others v. United Kingdom» [4]. У ній заявники ставили питання про відповідність Конвенції трьох взаємопов'язаних режимів спостереження у Сполученому Королівстві: 1) масове перехоплення електронних комунікацій; 2) отримання комунікаційних даних від провайдерів; 3) обмін розвідувальними даними з іноземними спецслужбами.

Так само як і в попередніх рішеннях, ЄСПЛ визнав порушення ст. 8 Конвенції у цій справі через відсутність попереднього судового контролю і відсутність чітких правил щодо відбору інтернет-трафіку, застосування пошукових селекторів, зберігання та знищення цифрових даних. У цій справі Суд окремо наголосив, що метадані здатні так само реконструювати приватне життя особи, а отже щодо них мають поширюватися такі самі гарантії, як і для контенту.

Водночас, на відміну від інших справ, ЄСПЛ у справі «Big Brother Watch and Others v. United Kingdom» вперше розглянув питання відповідності Конвенції процедури обміну інформацією з іноземними спецслужбами. Суд дійшов висновку, що загалом такі дії є сумісними із гарантіями Кон-

венції, але за умови наявності достатніх правил перевірки та контролю за таким обміном інформації, який відповідно до британського законодавства був формальним. Власне у зв'язку із цим Суд констатував порушення ст. 8 Конвенції.

У контексті оцінки якості законодавства, яке регламентує втручання держави у сферу цифрового спілкування, ЄСПЛ і надалі послідовно наголошував на необхідності існування дієвих і достатніх гарантій від свавільного втручання з боку органів влади. Вказана проблематика була предметом розгляду, зокрема, у справі «Екімджієв та інші проти Болгарії» [5].

У цьому рішенні Суд дійшов висновку про порушення статті 8 Конвенції, зазначивши, що хоча нормативне регулювання збереження телекомунікаційних даних та доступу до них зазнало суттєвого вдосконалення після рішення Конституційного суду Болгарії 2015 року, ухваленого з урахуванням позиції Суду ЄС у справі Digital Rights Ireland та інші, відповідне законодавство у практичному вимірі все ще не забезпечує мінімальних гарантій, необхідних для запобігання свавілля та зловживанням.

Зокрема, ЄСПЛ вказав, що: 1) процедура надання дозволу на доступ до збережених даних не гарантує, що таке втручання здійснюватиметься виключно за умов його необхідності у демократичному суспільстві; 2) законодавство не встановлює чітко визначених строків зберігання та обов'язкового знищення даних після їх використання у кримінальному провадженні; 3) відсутні публічно доступні та достатньо чіткі правила щодо порядку зберігання, доступу, аналізу, використання, передачі та знищення телекомунікаційних даних органами державної влади; 4) чинний механізм нагляду не забезпечує ефективної та незалежної перевірки можливих зловживань; 5) процедура повідомлення осіб про втручання у їхнє приватне життя є надмірно обмеженою; 6) національне право не гарантує наявності ефективних засобів правового захисту.

Таким чином, Суд констатував, що сукупність зазначених недоліків свідчить про невідповідність болгарської моделі доступу до даних зв'язку вимогам статті 8 Конвенції щодо передбачуваності правового регулювання та належного захисту від свавільного втручання.

Висновки. Проведений аналіз практики ЄСПЛ свідчить про формування цілісної та послідовної системи стандартів захисту права на повагу до приватного життя у кіберпросторі, яка ґрунтується на положеннях статті 8 Конвенції та принципі верховенства права. Суд, застосовуючи динамічне тлумачення Конвенції, адаптує класичні підходи до оцінки втручання у приватне життя до умов цифровізації, визнаючи, що електронні комунікації, метадані та інші цифрові сліди особи здатні розкривати різні аспекти її приватного та сімейного життя не меншою мірою, ніж традиційні форми кореспонденції.

У аналізованих рішеннях ЄСПЛ послідовно наголошує, що сама наявність законодавчого режиму, який допускає таємне або масове втручання у цифрове спілкування, вже може становити втручання у право на повагу до приватного життя. Вирішальним при цьому є формальна наявність правового регулювання, а його «якість», що передбачає достатню чіткість, передбачуваність та наявність ефективних гарантій від свавілля.

Зокрема, узагальнений аналіз справ дозволяє стверджувати, що мінімальними гарантіями відповідності практики масового кіберспостереження вимогам ст. 8 Конвенції є: 1) чітке законодавче визначення категорій осіб та даних щодо яких можливе перехоплення 2) наявність попереднього судового контролю на спостереження або ефективного подальшого контролю 3) нормативне формулювання критеріїв, за якими вирішується питання про ініціювання перехоплення 4) обмеження строків зберігання та наявність чіткого порядку знищення інформації.

ЛІТЕРАТУРА

1. Roman Zakharov v. Russia: Judgement of European Court Human Rights (Application № 47143/06), 04 December 2015. URL: <https://hudoc.echr.coe.int/fre?i=001-159324>
2. Szabó and Vissy v. Hungary: Judgement of European Court Human Rights (Application № 37138/14), 12 January 2016. URL: <https://hudoc.echr.coe.int/eng?i=001-160020>
3. Centrum för Rättvisa v. Sweden: Judgement of European Court Human Rights (Application № 35252/08), 25 May 2021. URL: <https://hudoc.echr.coe.int/fre?i=001-210278>
4. Big Brother Watch and others v. The United Kingdom: Judgement of European Court Human Rights (Application № 58170/13, 62322/14, 24960/15), 25 May 2021. URL: <https://hudoc.echr.coe.int/fre?i=001-210077>
5. Ekiimdzhiyev and Others v. Bulgaria: Judgement of European Court Human Rights (Application № 70078/12), 11 January 2022. URL: <https://hudoc.echr.coe.int/eng?i=001-214673>