МІЖНАРОДНЕ ПРАВО ПРАВ ЛЮДИНИ

УДК 341
DOI https://doi.org/10.32841/ILA.2020.24.10

БІЛА-КИСЕЛЬОВА А. А.,
кандидат юридичних наук,
суддя
Білозерського районного суду Херсонської області,
сертифікований тренер
Національної школи суддів України

ПРАВО НА НЕДОТОРКАННІСТЬ ПРИВАТНОГО ЖИТТЯ В КОНТЕКСТІ ЦИФРОВИХ КОМУНІКАЦІЙ: РЕКОМЕНДАЦІЇ МІЖНАРОДНИХ ІНСТИТУЦІЙ ТА ПРАКТИКА ЄСПЛ

Анотація. У статті висвітлено проблемні питання, пов'язані з правом на недоторканність приватного життя в контексті цифрових комунікацій.

Автор звертає увагу на те, що новітні інформаційні технології дають змогу проводити віртуальне стеження (переслідування, збір інформації), що може привести до порушення недоторканності приватного життя задля дискредитації жертви та/чи підбурювання до інших порушень або зловживань щодо неї.

Проаналізовано законодавство іноземних країн (США, Швеції, Болгарії, Нідерландів, Румунії) у питаннях стеження за «об'єктами спостереження», а також щодо втручання в право на недоторканність приватного життя.

У дослідженні приділяється увага Міжнародному пакту про громадянські і політичні права, Конвенції про захист прав людини і основоположних свобод, а також вивчаються документи Комітету ООН із прав людини та Резолюцій Генеральної Асамблеї ООН.

Аналіз міжнародних документів та вивчення практики ЄСПЛ дає змогу зробити висновок про те, що держави зобов'язані забезпечити свою роботу таким чином, щоб державні органи або посадові особи утримувалися від будь-якого свавільного втручання у право на недоторканність приватного життя. Це стосується й контексту цифрових комунікацій. Крім того, право на недоторканність приватного життя має гарантувати утримання від будь-якого втручання (зазіхань), незалежно від того, чи такі дії здійснюються державними органами, чи фізичними та юридичними особами. Доцільно переглянути процедури,

практики та законодавство, які стосуються відстеження комунікацій, їх перехоплення і збору особистих даних (включаючи масове відстеження, перехоплення та збір).

Що стосується використання матеріалів, отриманих у процесі стеження, вилучення документації (інформації, даних), які були отримані в результаті незаконного втручання у приватне життя, то вони не можуть бути прийнятними у провадженні проти цієї особи, що кореспондується з практикою ЄСПЛ у розрізі позиції: «використання доказів, здобутих із порушенням прав людини або внутрішнього законодавства, робить судовий процес несправедливим».

Ключові слова: віртуальний простір, стеження, об'єкти спостереження, права людини, приватне життя, ЄСПЛ, міжнародні стандарти, цифрові комунікації, цифрові технології.

Постановка проблеми. Відповідно до статті 17 МПГПП, «ніхто не може зазнавати безпідставного чи незаконного втручання в його особисте і сімейне життя, недоторканність житла чи таємницю його кореспонденції або незаконних посягань на його честь і репутацію» та «кожний має право на захист законом від такого втручання або посягань». Право на повагу до особистого і сімейного життя також гарантується статтею 8 (1) ЄКПЛ [1, 2].

Стаття 8 ЄКПЛ, на відміну від МПГПП, безпосередньо не згадує честь і репутацію публічних осіб чи громадян, але у своїх рішеннях Європейський суд із прав людини зазначав, що за деяких обставин право на захист репутації підпадає під статтю 8 Конвенції як складова частина права на недоторканність приватного життя (справа «Шові та інші проти Франції», заява № 64915/01, рішення від 29 червня 2004 р., п. 70.) [1, 2, 3].

У справі «Караке проти Угорщини» (заява № 39311/05, рішення від 28 квітня 2009 р.) ЄСПЛ зазначив, що «репутація розглядалася як індивідуальне право лише в деяких окремих випадках, здебільшого тоді, коли стверджувані факти мали настільки серйозний образливий характер, що їх публікація неминуче чинила безпосередній вплив на особисте життя заявника» (п. 23) [4].

Крім того, стаття 8 (2) ЄКПЛ вказує, що будь-яке втручання органів державної влади у приватне життя має здійснюватися згідно із законом і бути необхідним у демократичному суспільстві на одній із перелічених у Конвенції підстав [2].

Комітет ООН із прав людини підкреслив, що, відповідно до вимог захисту від незаконного втручання, «втручання, яке дозволяється державами, може відбуватися тільки на основі закону, який у свою чергу має відповідати положенням, цілям і завданням Пакту». Що стосується **поняття свавільності**, то Комітет відзначив необхідність «забезпечити, щоб навіть втручання, яке допускається законом, відповідало положенням, цілям і завданням Пакту і в будь-якому разі було обґрунтованим за конкретних обставин (Комітет ООН із прав людини, Коментар загального порядку № 16 щодо статті 17, пункти 3, 4) [5].

Крім того, у своїх рішеннях Комітет підкреслював, що **вимога розумності** означає **пропорційність будь-якого** втручання переслідуваній цілі та його необхідність у кожному конкретному випадку (справа «Антоніус Корнеліс Ван Гюлст проти Нідерландів», повідомлення № 903/1999, UN Doc. CCPR/C/82/D/903/1999, від 15 листопада 2004, п. 7.6.; справа «Тоонен проти Австралії», повідомлення № 488/1992, UN Doc. CCPR/C/50/D/488/1992, від 31 березня 1994 р., п. 8.3.) [6].

У Коментарі загального порядку Комітет підкреслив, що навіть щодо втручання, яке відповідає Пакту, у відповідному законодавстві мають докладно визначатися конкретні обставини, за яких таке **втручання є припустимим**. Рішення про санкціонування такого припустимого втручання має ухвалюватися лише органом, передбаченим законом, і лише залежно від обставин у конкретному випадку (Коментар загального порядку № 16, пп. 7 і 8). Європейський суд із прав людини заявив, що стаття 8 (2) ЄКПЛ, якою передбачаються виключення з права, гарантованого Конвенцією, підлягає вузькому тлумаченню і що необхідність втручання в конкретному випадку має бути переконливо встановлена (справа «Клас та інші проти Федеративної Республіки Німеччина», 1978 р., п. 42, і справа «Функе проти Франції», 1993 р, п. 55) [5, 7, 8].

Крім того, ЄСПЛ зазначив, що він має упевнитися в тому, що існують достатні та ефективні гарантії проти зловживань будь-якою запровадженою системою спостереження (рішення у справі «Клас проти Федеративної Республіки Німеччина», п. 50) [7].

Не можна не погодитися з тим, що одна з найвідоміших проблем у сфері приватного життя стосується збору та опрацювання персональних даних з боку державних структур. Цілями такої діяльності може бути як боротьба з тероризмом, недопущення громадських заворушень, так і покращення у сфері надання послуг (інші підстави). При цьому способами отримання даних є: збір із відкритих джерел, офіційні звернення до розпорядників, прямий доступ до серверів, перехоплення інформації, використання третіх осіб для отримання доступу. Така діяльність породжує сумніви щодо її відповідності чинним міжнародним стандартам.

Як у разі з іншими правами, котрі можуть бути обмежені за певних суворо визначених умов, держави мають забезпечити, щоб будь-яке втручання в право на недоторканність приватного життя суворо відповідало принципам законності, необхідності та пропорційності. Це стосується й недоторканності в розрізі спілкування у віртуальному просторі.

Новітні інформаційні технології дають змогу проводити віртуальне стеження (переслідування, збір інформації) та порушення недоторканності приватного життя (зламування електронної пошти та інших електронних додатків, зняття інформації з приватних електронних додатків) задля дискредитації жертви та/чи підбурювання до інших порушень або зловживань щодо неї.

Аналіз останніх досліджень і публікацій. Дослідженням прав і свобод людини та вивченню міжнародних стандартів щодо захисту прав людини займаються науковці та судді Т.О. Анцупова, М.І. Дерев'янко, О.Р. Кібенко, П.М. Рабінович, В.В. Мицик та інші. Водночас право на недоторканність приватного життя в контексті цифрових технологій потребує додаткового вивчення. Саме тому ця тема актуальна нині.

Метою статті є аналіз міжнародних документів щодо права на повагу до особистого і приватного життя; вивчення документів Комітету ООН із прав людини, Резолюцій Генеральної Асамблеї ООН; дослідження практики ЄСПЛ у питаннях втручання у приватне життя; надання інформації про міжнародні стандарти в галузі прав людини щодо незаконного втручання в приватне життя.

Виклад основного матеріалу. Ефективний захист від незаконного і свавільного втручання в особисте життя має особливе значення тому, що повага до права на приватне життя є важливою для здійснення права на захист прав людини.

Так, наприклад, Генеральна Асамблея ООН визнала, що здійснення права на недоторканність приватного життя має велике значення для реалізації права на свободу вираження поглядів та права безперешкодно дотримуватися власних переконань і, таким чином, є однією з підвалин демократичного суспільства (Резолюція Генеральної Асамблеї ООН 68/167 «Право на недоторканність особистого життя в цифрову еру», UN Doc. A/ RES/68/167, від 18 грудня 2013 р., преамбула) [9].

Водночас люди все більше наражаються на ризик стати об'єктами незаконного, свавільного втручання в їхнє приватне життя. Вони часто повідомляють про випадки протиправного контролю і спостереження за їхньою роботою та приватним життям з боку служб безпеки, в тому числі у формі прослуховування телефонів та відстеження комунікацій в Інтернеті (Права людини і безпековий сектор: круглий стіл із правозахисниками, організований Бюро Комісара Ради Європи з прав людини, Київ, 30–31 травня 2013 р., CommDH(2013)17, від 17 вересня 2013 р.,пп. 14 і 49.) [6].

У деяких випадках йдеться про незаконне використання інформації у зв'язку з протиправним контролем і спостереженням та з метою дискредитації їх особисто або у зв'язку з їхньою роботою.

Комісар Ради Європи ыз прав людини неодноразово нагадував про пов'язані з Інтернетом загрози для прав людини.

Так, відповідно до четвертої щоквартальної доповіді про діяльність у 2013 р. Нільса Муйжніекса (візит до Азербайджану 22–24 травня 2013 р.,), Комісара Ради Європи з прав людини (за період з 1 жовтня по 31 грудня 2013 р.), CommDH (2014)3, від 12 лютого 2014 р., «є інформація від різних співрозмовників, що в Азербайджані органи безпеки здійснюють моніторинг активності в Інтернеті або відстежують дані користувачів. Зокрема, деякі зі співрозмовників Комісара повідомили, що під час допитів органи

влади посилалися на їх матеріали у Фейсбуці або показували їм повідомлення з їх приватної електронної пошти» [6].

Дійсно, проблеми, які виникають у зв'язку з цифровими інформаційно-комунікаційними технологіями, викликають усе більшу стурбованість міжнародного співтовариства. Про це свідчить Резолюція 2013 р. про Право на недоторканність особистого життя в еру цифрових технологій. Генеральна Асамблея ООН звернула увагу на те, що «швидкі темпи технологічного розвитку дозволяють людям у всьому світі користуватися новими інформаційними та комунікаційними технологіями і водночас посилюють спроможність урядів, компаній та фізичних осіб відстежувати, перехоплювати і збирати інформацію, що може порушувати чи обмежувати права людини» [9].

Крім того, Комітет міністрів Ради Європи зазначив, що «обробка даних в інформаційному суспільстві, яка здійснюється без необхідних гарантій та заходів безпеки, може викликати серйозні занепокоєння щодо прав людини. Законодавство, яке дозволяє широкосяжне спостереження за громадянами, може бути визнане таким, що суперечить праву на недоторканність особистого життя. Такі можливості та практика чинять стримувальний вплив на участь громадян у суспільному, культурному та політичному житті та можуть у більш довгостроковій перспективі чинити шкідливий вплив на демократію; порушувати право на конфеденційність; загрожувати свободі передання та отримання інформації» (Декларація Комітету міністрів про ризики для основоположних прав людини, пов'язані з цифровими технологіями спостереження і стеження, від 11 червня 2013 р., п. 2) [10].

Нові методи спостереження і проникнення в комп'ютерні системи для виявлення вразливих місць тих осіб, які є об'єктами спостереження, задля підриву їхнього авторитету та репутації являють собою додаткову загрозу, оскільки такі засоби можуть використовуватися в цілях дискредитації, наприклад, опозиційних політиків, суддів, адвокатів, активістів правозахисного руху або журналістів.

Крім того, відстеження геолокації може бути використано для переслідування жінок та зробить їх більш вразливими до зловживань та насильства, пов'язаних із гендером (п. 6 Декларації Комітету міністрів про ризики для основоположних прав людини, пов'язані з цифровими технологіями спостереження і стеження) [10].

Так, спеціальний доповідач ООН із питання про право на свободу переконань і свободу вираження поглядів висловив занепокоєння з приводу того факту, що в багатьох країнах, включаючи держави-учасниці ОБСЄ, національні розвідувальні служби автоматично звільняються від вимоги діяти на підставі судових санкцій [6]. Закон США «Про стеження в рамках закордонної розвідувальної діяльності» уповноважує Агентство національної безпеки перехоплювати комунікації без судової санкції, а закони Німеччини та Швеції допускають прослуховування та перехоплення без наявності ордеру.

У своїх Заключних зауваженнях щодо Швеції від 2009 р. Комітет із прав людини також зазначив, що Закон «Про радіоперехоплення розвідданих у ході оборонних операцій» надає виконавчій владі широкі повноваження у сфері стеження за електронними комунікаціями, і рекомендував «державі-учасниці вжити всіх необхідних заходів для того, щоб уникнути зловживань під час збору, зберігання або використання особистих даних, не використовувати їх у цілях, які суперечать Пакту, і забезпечити їх відповідність зобов'язанням, передбаченим у статті 17 Пакту. Для цього держава-учасниця має гарантувати, що обробка і збір інформації підлягатимуть перевірці та нагляду з боку незалежного органу, з необхідними гарантіями неупередженості та ефективності» (CCPR/C/SWE/ CO/6, від 7 травня 2009 р., п. 18.) [5].

У своїх Заключних зауваженнях щодо США від 26 березня 2014 р. Комітет ООН із прав людини висловив стурбованість із приводу стеження за комунікаціями, яке проводиться Агентством національної безпеки (АНБ), і зазначив, що система нагляду за діяльністю АНБ не в змозі захистити права тих, за ким таке стеження було встановлено, тоді як останні не мають доступу до ефективних засобів правового захисту в разі зловживань. Комітет закликав державу-учасницю забезпечити, щоби її заходи зі стеження повною мірою відповідали її зобов'язаннями за Пактом, у тому числі за статтею 17, зокрема, щоб будь-яке втручання відбувалося «відповідно до законів, які 1) є загальнодоступними; 2) містять положення, які забезпечують відповідність збору комунікаційних даних, доступу до них або їх використання конкретним законним цілям; 3) є досить точними і детально визначають умови, за яких будь-яке подібне втручання є припустимим, порядок отримання дозволу, категорії осіб, щодо яких може вестися спостереження, граничні строки ведення спостереження, порядок використання і зберігання отриманих даних; 4) передбачають ефективні гарантії проти зловживання» (UN Doc. CCPR/C/USA/CO/4, п. 22) [5].

Таким чином, за відсутності належного законодавства та правових стандартів щодо забезпечення конфіденційності, безпеки й анонімності комунікацій будь-яка людина не може бути впевнена, що держави не контролюватимуть її спілкування. Без надійних механізмів правового захисту будь-яка особа може зазнавати безпідставного стеження за своїм життям.

Законодавство має передбачати можливість відстеження державою комунікацій лише за виняткових обставин і тільки під наглядом незалежного судового органу.

У рішенні по справі «Асоціація за європейську інтеграцію та права людини й Екімджиєв проти Болгарії» (заява № 62540/00, рішення від 28 червня 2007 р., п. 76) ЄСПЛ зазначив: «законодавство дозволило владі значну свободу дій щодо збору інформації шляхом стеження та її подальшого використання». ЄСПЛ нагадав, що законодавство має встановлювати мінімальні гарантії проти зловживань, зокрема «характер правопорушень,

які можуть спричинити до наказу про перехоплення інформації; визначення категорій осіб, спілкування яких підлягає відстеженню; граничні терміни тривалості такого відстеження; порядок вивчення, використання і зберігання отриманих даних; запобіжні заходи під час передачі таких даних іншим сторонам; обставини, за яких отримані дані або записи можуть або мають бути знищені» [11].

Крім того, ЄСПЛ підкреслив необхідність «адекватних та ефективних гарантій проти зловживань» у контексті негласного стеження, в тому числі щодо «характеру, масштабів та тривалості можливих заходів стеження, підстав, потрібних для їх застосування, органів влади, уповноважених санкціонувати та здійснювати такі заходи і наглядати за ними, і типу засобів правового захисту, передбачених національним законодавством» (справа «Ліберті проти Сполученого Королівства», заява № 58243/00, рішення від 1 липня 2008 р.) [12].

У справі «Ліберті проти Сполученого Королівства» ЄСПЛ ухвалив, що держава порушила статтю 8 ЄКПЛ, оскільки не вважав, що «в той час національне законодавство не визначало з достатньою ясністю, яка забезпечувала би адекватний захист від зловживання повноваженнями, ті межі або той спосіб здійснення вельми широких дискреційних повноважень, якими було наділено державу для перехоплення і вивчення зовнішніх комунікацій. Зокрема, воно не встановлювало, як того вимагає практика Суду, в доступній для широкого загалу формі будь-яку процедуру відбору перехоплюваних матеріалів для їх вивчення, передання, зберігання і знищення» (п. 69).

На нашу думку, кожний має бути наділений установленим у законі правом бути сповіщеним про те, що його комунікації відстежуються, або що держава отримувала доступ до його комунікаційних даних; особи мають сповіщатися про закінчення стеження одразу після його завершення, щоб мати гарантовану можливість домагатися відшкодування збитку. Така думка повністю узгоджується з практикою ЄСПЛ, відповідно до якої органи влади мають позитивне зобов'язання забезпечити наявність ефективної та доступної процедури, яка дозволятиме окремим особам в розумні строки отримати доступ до своїх особистих досьє, котрі зберігаються державними органами (справа «Араламбіе проти Румунії», заява № 21737/03) [13].

Висновки. Аналіз міжнародних документів та вивчення практики ЄСПЛ дає змогу зробити висновок про те, що держави зобов'язані забезпечити свою роботу таким чином, щоб державні органи або посадові особи утримувалися від будь-якого незаконного або свавільного втручання у право на недоторканність приватного життя. Це стосується й контексту цифрових комунікацій. Крім того, право на недоторканність приватного життя має гарантувати утримання від будь-якого втручання і таких зазіхань, незалежно від того, чи вони здійснюються державними органами, чи фізичними або юридичними особами. Держави мають криміналізувати незаконне стеження з боку державних або приватних суб'єктів. Доцільно

переглянути процедури, практики та законодавство, які стосуються відстеження комунікацій, їх перехоплення і збору особистих даних (включаючи масове відстеження, перехоплення та збір).

Що стосується використання матеріалів, отриманих у процесі стеження, вилучення документації (інформації, даних), які були отримані в результаті незаконного або свавільного втручання у приватне життя, то вони не можуть бути прийнятними у провадженні проти цієї особи, що кореспондується з практикою ЄСПЛ у розрізі позиції, що «використання доказів, здобутих із порушенням прав людини або внутрішнього законодавства, робить судовий процес несправедливим».

Література:

1. Міжнародний пакт про громадянські і політичні права URL: https://zakon.rada.gov.ua/laws/show/995_043#Text
2. Конвенція про захист прав людини і основоположних свобод URL: https://zakon.rada.gov.ua/laws/show/995_004#Text
3. Справа «Шові та інші проти Франції» URL: https://www.echr.coe.int/Documents/Guide_Art_17_UKR.pdf
4. Справа «Караке проти Угорщини» URL: http://search.ligazakon.ua/l_doc2.nsf/link1/SO5961.html
5. Комітет з прав людини ООН (офіційний сайт) URL: https://www.ohchr.org/RU/HRBodies/CCPR/Pages/CCPRIndex.aspx
6. Керівні принципи щодо захисту правозахисників URL: https://www.osce.org/files/f/documents/d/d/150476.pdf
7. Справа «Клас та інші проти Федеративної Республіки Німеччина» URL: https://zakon.rada.gov.ua/laws/show/980_093#Text
8. Справа «Функе проти Франції» URL: https://zakon.rada.gov.ua/laws/show/980_154#Text
9. Резолюция Генеральной Асамблеи ООН 68/167 «Право на неприкосновенность личной жизни в цифровой век» URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G14/068/73/PDF/G1406873.pdf?OpenElement
10. Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies (11 червня 2013р.) URL: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168068460d
11. Справа «Асоціація за європейську інтеграцію та права людини і Екімджиєв проти Болгарії» URL: http://khpg.org/index.php?id=1317624595
12. Справа «Ліберті проти Сполученого Королівства» URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-181074%22]}
13. Справа «Араламбіе проти Румунії» URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-95302%22]}

Bila-Kyseleva A. The right to the privacy in the context of digital communications: recommendations of international institutions and practice of the ECHR

Summary. The article highlights the issues related to the right to privacy in the context of digital communications.

The author draws attention to the fact that the latest information technologies allow virtual surveillance (harassment, collection of information) and violation of privacy in order to discredit the victim and / or incite other violations or abuses against her.

The legislation of foreign countries (USA, Sweden, Bulgaria, the Netherlands, Romania) on the issues of surveillance of «objects of observation», as well as on interference with the right to privacy was analyzed

The study focuses on the International Covenant on Civil and Political Rights, the Convention for the Protection of Human Rights and Fundamental Freedoms, as well as documents of the UN Human Rights Committee and UN General Assembly Resolutions.

An analysis of international documents and a study of the case law of the ECHR leads to the conclusion that states are obliged to ensure their work in such a way that public authorities or officials refrain from any illegal or arbitrary interference with the right to privacy. This also applies to the context of digital communications. In addition, the right to privacy must guarantee refraining from any interference and such encroachments, whether carried out by public authorities or natural or legal persons, as States must criminalize unlawful surveillance by public or private entities.

It is advisable to review the procedures, practices and legislation relating to the tracking of communications, their interception and the collection of personal data (including mass tracking, interception and collection).

As for the use of materials obtained during surveillance, seizure of documentation (information, data), which were obtained as a result of illegal or arbitrary invasion of privacy, they can not be acceptable in proceedings against this person, which corresponds to the practice of the ECtHR in terms of positions: «the use of evidence obtained in violation of human rights or domestic law makes the trial unfair».

Key words: cyberspace, surveillance, «objects of observation», human rights, privacy, ECHR, international standards, digital communications, digital technologies.