Спільна інформаційна довідка

Масове спостереження[1]
Практика ЄСПЛ та Суду справедливості Європейського Союзу (СЄС)

(Останнє оновлення: 28.02.2025)

Ця інформаційна довідка підготовлена Секретаріатом Європейського суду з прав людини («ЄСПЛ»)[2] та Агентством Європейського Союзу з питань основоположних прав людини в рамках спільної роботи з метою висвітлення судової практики в окремих сферах, де взаємодіють право Європейського Союзу (ЄС) та Європейська конвенція з прав людини («ЄКПЛ» або «Конвенція»).

I. Масове спостереження

Зважаючи на останні технологічні та соціальні зміни у сфері електронних комунікацій, ЄСПЛ та СЄС були покликані розглянути ризики для прав людини, пов'язані з режимом масового спостереження, а саме системами, що дозволяють великомасштабний технічний збір інформації[3] в електронних комунікаціях.

Сьогодні, у дедалі більш цифрову епоху, комунікація здебільшого відбувається у цифровій формі та передається по всесвітнім телекомунікаційним мережам, використовуючи комбінацію найшвидших та найдешевших шляхів без будь-якого значущого врахування національних кордонів. Тому спостереження, не спрямоване безпосередньо на окремих осіб, має спроможність дуже широкого охоплення як всередині, так і за межами території Держави, яка здійснює спостереження.[4]

Режими масового спостереження можуть функціонувати шляхом отримання доступу до інформації та зберігання великих обсягів даних, одержаних від носіїв інтернет-комунікацій (так зване масове перехоплення)[5]. Від постачальників послуг електронних комунікацій («ППЕК») також можуть вимагати здійснювати загальне збереження комунікацій користувачів та

[1] Для цілей цієї інформаційної довідки загальний термін «масове спостереження» розуміється як «загальне спостереження за комунікаціями». Термінологія більш детально розглядається у звіті Агентства ЄС з питань основоположних прав за 2017 рік на с. 29 *«Спостереження з боку служб розвідки: гарантії основоположних прав та засоби правового захисту в ЄС – Том II: перспективи галузі та оновлення законодавства»*. Див. також звіт *Агентства ЄС з питань основоположних прав «Спостереження з боку служб розвідки: гарантії основоположних прав та засоби правового захисту в ЄС – оновлення 2023 року / Агентство Європейського Союзу з основоположних прав*.

[2] Зміст цієї інформаційної довідки не є обов'язковим для Суду. Цей переклад виконано Верховним Судом (Україна) та опубліковано за домовленістю з Радою Європи та Європейським судом з прав людини.

[3] Термін «інформація» використовується для охоплення невибіркового перехоплення інформації в контексті кримінального провадження, а не лише інформації, зібраної розвідувальними службами.

[4] Рішення ЄСПЛ у справі *«Біг Бразер Вотч та інші проти Сполученого Королівства» (Big Brother Watch and Others v. the United Kingdom)* [ВП], №№ 58170/13 та 2 інші, § 322, 25 травня 2021 року; та *«Центр справедливості проти Швеції» (Centrum för rättvisa v. Sweden)* [ВП], № 35252/08, § 236, 25 травня 2021 року.

[5] Див., наприклад, рішення ЄСПЛ у справах *«Біг Бразер Вотч» (Big Brother Watch)*, цитоване вище, § 15, і загалом судову практику, описану нижче в пункті А.

пов’язаних із ними даних[6] і надавати національним органам доступ до цих даних або безпосередньо та необмежено[7], або на підставі цільових запитів[8].

Масове спостереження може бути спрямоване на зміст електронних комунікацій та/або пов'язаних із ними комунікаційних даних, включаючи персональні дані абонентів та зареєстрованих користувачів, а також дані про трафік та місцезнаходження. Заволодіння комунікаційними даними не становить менше втручання, ніж заволодіння змістом, оскільки дані про трафік та місцезнаходження, взяті в сукупності, можуть дозволити зробити дуже точні висновки щодо приватного життя людей, включаючи їхні звички, постійні або тимчасові місця проживання, щоденні пересування, їхню діяльність, особисті стосунки та соціальне оточення[9]. Що стосується змісту електронних комунікацій, особливий перелік питань може виникнути, коли масове перехоплення, зберігання та доступ до змісту включають спроби національних органів розшифрувати зашифровані електронні повідомлення.[10]

II. Масове спостереження у практиці Суду справедливості ЄС

Перш за все Суд справедливості ЄС розглядав режими масового спостереження з точки зору захисту персональних даних та права на приватність, що гарантуються Директивою про приватність та електронні комунікації[11] та Загальним регламентом захисту даних (GDPR)[12], у світлі основоположних прав, гарантованих статтями 7 (повага до приватного та сімейного життя), 8 (захист персональних даних) та 11 (свобода вираження поглядів) Хартії основоположних прав ЄС (далі – «Хартія»). [13]

В окремих випадках, пов'язаних із функціонуванням режимів масового спостереження, СЄС також надавав роз'яснення щодо тлумачення інших правових інструментів ЄС, у світлі вищезазначених основоположних прав, зокрема у контексті судового співробітництва у кримінальних справах та Європейського ордеру на проведення розслідування[14] або боротьби зі зловживаннями на ринку.[15]

---

[6] Див., наприклад, рішення ЄСПЛ у справі *«Подчасов проти Росії» (Podchasov v. Russia)*, № 33696/19, 13 лютого 2024 року, і загалом судову практику, описану нижче в пункті B.

[7] Див., наприклад, рішення ЄСПЛ у справі *«П'єтрак і Бичавська-Синярська та інші проти Польщі» (Pietrzak and Bychawska-Siniarska and Others v. Poland)*, №№ 72038/17 та 25237/18, 28 травня 2024 року.

[8] Див., наприклад, рішення ЄСПЛ у справі *«Бен Файза проти Франції» (Ben Faiza v. France)*, № 31446/12, 8 лютого 2018 року, та *«Шкоберне проти Словенії» (Škoberne v. Slovenia)*, № 19920/20, 15 лютого 2024 року; рішення СЄС від 2 березня 2021 року, *Прокуратура (Prokuratuur)*, C-746/18, EU:C:2021:152, рішення від 5 квітня 2022 року, *«Комісар Ґарда Сіхани та інші» (Commissioner of An Garda Síochána e.a.)*, C-140/20, EU:C:2022:258, рішення від 17 листопада 2022 року, *«Спеціалізована прокуратура» (Spetsializirana prokuratura)*, C-350/21, EU:C:2022:896.

[9] Рішення СЄС від 8 квітня 2014 року, *«Діджитал Райтс Айрленд та інші» (Digital Rights Ireland e.a.)*, C-293/12 та C-594/12, EU:C:2014:238, § 27; ЄСПЛ, *«Біг Бразер Вотч» (Big Brother Watch)*, цитоване вище, § 342.

[10] Рішення СЄС від 30 квітня 2024 року, *«M.N. (ІнкроЧат)» (M.N. (EncroChat))* C-670/22, EU:C:2024:372; ЄСПЛ, *Подчасов проти Росії (Podchasov v. Russia)*, цитоване вище.

[11] Директива 2002/58/ЄС Європейського Парламенту і Ради від 12 липня 2022 року про обробку персональних даних і захист приватності у сфері електронних комунікацій.

[12] Регламент (ЄС) 2016/679 Європейського Парламенту і Ради від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС.

[13] Зверніться до судової практики СЄС, описаної нижче в розділах C.1 та C.2.

[14] Директива 2014/41/ЄС Європейського Парламенту і Ради від 3 квітня 2014 року про Європейський ордер на проведення розслідування у кримінальних справах; див. СЄС, *«M.N. (ІнкроЧат)» (M.N. (EncroChat))*, цитоване вище.

[15] Директива 2003/6/ЄС Європейського Парламенту і Ради від 28 січня 2003 року про інсайдерську діяльність та маніпулювання ринком («Директива про зловживання на ринку») та Регламент (ЄС)

III. Масове спостереження у практиці ЄСПЛ

Здебільшого ЄСПЛ розглядав режими масового спостереження з точки зору права на повагу до приватного життя[16] і кореспонденції (стаття 8 ЄКПЛ) та права на свободу вираження поглядів (стаття 10 ЄКПЛ) стосовно захисту комунікації журналістів.

У контексті статті 8 ЄКПЛ, спираючись на свою практику щодо режимів таємного спостереження, що дозволяють цілеспрямовані заходи спостереження[17], ЄСПЛ підтвердив, що в особливому контексті таємних заходів спостереження «передбачуваність» означає зрозумілість національного законодавства для надання громадянам адекватної вказівки на обставини чи умови, за яких органи державної влади уповноважені вдаватися до будь-яких подібних заходів, а також з достатньою чіткістю має вказувати на обсяг свободи розсуду та спосіб її використання, щоб забезпечити особі адекватний захист від свавілля[18].

Суд також підтвердив, що доцільно розглядати в сукупності вимоги «згідно із законом» та «необхідність» тоді, коли законодавство, що дозволяє таємне спостереження, оскаржується в ЄСПЛ. Національне законодавство має бути не лише доступним та передбачуваним у своєму застосуванні, воно також має забезпечувати застосування таємних заходів спостереження лише тоді, коли це «необхідно в демократичному суспільстві», зокрема, шляхом забезпечення адекватних та ефективних гарантій проти зловживань[19].

Щодо гарантій, які мають бути властиві режиму масового спостереження, що відповідає вимогам Конвенції, ЄСПЛ вважав за необхідне розробити та адаптувати гарантії, викладені у попередній практиці Суду щодо режимів цільового перехоплення, до особливостей масового перехоплення повідомлень[20] та загального зберігання й доступу до змісту повідомлень[21].

У контексті статті 10 ЄКПЛ, Суд спирався на свою практику щодо обшуків житла або робочого місця журналіста, адаптуючи матеріальні та процесуальні гарантії, передбачені в ній, до контексту масового перехоплення[22] та загального зберігання даних[23]. Суд розрізнив, зокрема, гарантії, що повинні бути передбачені для режиму масового спостереження, який відповідає Конвенції, у випадках, коли втручання у свободу вираження поглядів журналістів є навмисним, від випадків, коли комунікація журналістів або пов'язана з нею інформація не були спеціально

№ 596/2014 Європейського Парламенту і Ради від 16 квітня 2014 року про зловживання на ринку («Регламент про зловживання на ринку»); див. рішення СЄС від 20 вересня 2022 року, *«ВД і СР» (VD and SR)*, C-339/20 та C-397/20, EU:C:2022:703.

[16] Оцінюючи втручання у право на повагу до приватного життя внаслідок масового спостереження, Суд також посилався на інші правові документи Ради Європи, такі як Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних 1981 року та Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних від 8 листопада 2001 року; Рекомендація Комітету міністрів (№ R (95) 4 щодо захисту персональних даних у сфері телекомунікаційних послуг (прийнята 7 лютого 1995 року) та Звіт Європейської комісії «За демократію через право» про демократичний нагляд за агентствами радіоелектронної розвідки 2015 року.

[17] Див., наприклад, рішення ЄСПЛ у справі *«Роман Захаров проти Росії» (Roman Zakharov v. Russia)* [ВП], № 47143/06, §§ 227-234, ЄСПЛ 2015, та іншу судову практику, на яку там посилаються.

[18] Див., наприклад, рішення ЄСПЛ у справі *«Біг Бразер Вотч» (Big Brother Watch)*, цитоване вище, § 333.

[19] *Ibid.*, § 334.

[20] Рішення ЄСПЛ у справі *«Біг Бразер Вотч» (Big Brother Watch)*, цитоване вище, §§ 340-347; *«Центр справедливості проти Швеції» (Centrum för rättvisa v. Sweden)*, цитоване вище, §§ 254-261.

[21] Рішення ЄСПЛ у справі *«Екімджієв та інші проти Болгарії» (Ekimdzhiev and Others v. Bulgaria)*, № 70078/12, §§ 394-395, 11 січня 2022 року.

[22] Рішення ЄСПЛ у справі *«Біг Бразер Вотч» (Big Brother Watch)*, цитоване вище, §§ 447-450.

[23] Рішення ЄСПЛ у справі *«Біг Бразер Вотч» (Big Brother Watch)*, цитоване вище, §§ 524-525 та 528.

відібрані для перевірки, за умови, що на етапі такої перевірки стає очевидним, що зміст комунікації містить конфіденційні журналістські матеріали.[24]

IV. Практика Суду справедливості ЄС (СЄС) та ЄСПЛ щодо масового спостереження

A. Режими масового перехоплення

Рішення СЄС від 6 жовтня 2020 року, *«Прайвесі Інтернешенел» (Privacy International)*, C-623/17, EU:C:2020:790

Фактичні обставини справи – На початку 2015 року стало відомо про існування практики заволодіння та використання великих обсягів комунікаційних даних різними органами безпеки та розвідки Великобританії. Згідно з оскаржуваним режимом, Державний секретар міг вимагати від постачальників послуг електронних комунікацій, якщо він вважав це необхідним в інтересах національної безпеки або відносин з іноземним урядом, передавати великі обсяги комунікаційних даних (включаючи дані про трафік і місцезнаходження, а також інформацію, що стосується використовуваних послуг) органам безпеки та розвідки. Таке розкриття даних стосувалося всіх користувачів засобів електронної комунікації. Після передачі ці дані зберігалися органами безпеки та розвідки й залишалися доступними для цілей діяльності цих органів, як і інші бази даних, що підтримуються цими органами. Зокрема, отримані таким чином дані підлягали масовій автоматизованій обробці та аналізу, могли перевірятися перехресно з іншими базами даних, що містять різні категорії великих обсягів персональних даних, або розголошуватися поза межами цих органів чи третім країнам. Такі операції не потребували попереднього дозволу суду або іншого незалежного адміністративного органу і не передбачали повідомлення зацікавлених осіб про проведення щодо них такої операції.

Неурядова організація «Прайвесі Інтернешенел» (Privacy International) подала позов до Трибуналу з питань слідчих повноважень (Investigatory Powers Tribunal) (далі – Трибунал) оскаржуючи законність цих практик. Трибунал встановив, що ці режими, вже після їхнього визнання, відповідали статті 8 ЄКПЛ. Однак за результатом розгляду справи *Tele2 Sverige ma Watson ma інші* СЄС визначив наступні чотири вимоги, що виходять за межі вимог статті 8 ЄКПЛ: обмеження нецільового доступу до великих обсягів даних; необхідність попереднього дозволу (крім випадків належним чином встановленої надзвичайної ситуації) перед отриманням доступу до даних; положення про подальше повідомлення зацікавлених осіб; збереження всіх даних в межах ЄС.

30 жовтня 2017 року Трибунал звернувся до СЄС із запитом про ухвалення попереднього рішення для з'ясування в якому обсязі вимоги зі справи Watson можуть застосовуватися у випадках, коли методи масового заволодіння даними та автоматизованої обробки необхідні для захисту національної безпеки.

Право – СЄС встановив, що національне законодавство, яке дозволяє державному органу вимагати від ППЕК поширення даних про трафік і місцезнаходження органам безпеки та розвідки з метою захисту національної безпеки, підпадає під дію Директиви про приватність та електронні комунікації. Тлумачення цієї Директиви має враховувати права, гарантовані статтями 7, 8 та 11 Хартії. Обмеження щодо здійснення цих прав мають бути передбачені законом, поважати зміст таких прав і бути пропорційними, необхідними та відповідати загальному інтересу, визнаному ЄС, або необхідності захисту прав і свобод інших осіб. Крім того, обмеження захисту персональних даних повинні застосовуватися лише в тій мірі, в якій

[24] Рішення ЄСПЛ у справі *«Біг Бразер Вотч» (Big Brother Watch)*, цитоване вище, § 447.

це є суворо необхідним. Для дотримання вимоги пропорційності законодавство має встановлювати чіткі та зрозумілі правила, що регулюють обсяг і застосування відповідного заходу, і встановлювати мінімальні гарантії ефективного захисту від ризику зловживань для осіб, чиї персональні дані зазнали впливу.

На думку СЄС, національне законодавство, яке вимагає від ППЕК розкривати дані про трафік і місцезнаходження органам безпеки та розвідки за допомогою загальної та невибіркової передачі даних, що зачіпає всіх осіб, які користуються послугами електронної комунікації, перевищує межі того, що є суворо необхідним, і не може вважатися обґрунтованим, як цього вимагає Директива про приватність та електронні комунікації у світлі Хартії.

Рішення ЄСПЛ у справі *«Біг Бразер Вотч та інші проти Сполученого Королівства» (Big Brother Watch and Others v. the United Kingdom)* [ВП], №№ 58170/13 та 2 інших, 25 травня 2021 року

Фактичні обставини справи – Ця справа стосувалася сумісності зі статтями 8 та 10 ЄКПЛ режиму таємного спостереження у Великобританії, що діяв на 7 листопада 2017 року та регулював:
I) масове перехоплення змісту комунікаційних даних та пов'язаної з ними інформації;
II) отримання розвідувальних даних від іноземних розвідувальних служб;
III) отримання комунікаційних даних від постачальників послуг електронних комунікацій.

Право – **Щодо I), Стаття 8 ЄКПЛ:** заявники скаржилися, що масове перехоплення транскордонних комунікацій службами розвідки порушує статтю 8.

Щодо наявності втручання ЄСПЛ розглядав масове перехоплення комунікацій як поступовий процес, в якому ступінь втручання у права особи за статтею 8 збільшувався в міру просування процесу відповідно до чотирьох етапів:
a) перехоплення та початкове зберігання комунікацій і пов'язаних із ними комунікаційних даних;
b) застосування конкретних селекторів до збережених комунікацій/пов'язаних із ними комунікаційних даних;
c) вивчення відібраних комунікацій/пов'язаних із ними комунікаційних даних аналітиками; та
d) подальше зберігання даних і використання «кінцевого продукту», включаючи обмін даними з третіми сторонами.

Хоча первинне перехоплення з подальшим негайним видаленням частини комунікацій не становило значного втручання, ступінь втручання у права особи за статтею 8 збільшувався в міру просування процесу масового перехоплення.

Щодо відповідних принципів, застосовних до справ про масове перехоплення, ЄСПЛ посилався на свою попередню практику щодо режимів цільового перехоплення, щоб заявити, що Держави користуються широкою свободою розсуду при вирішенні того, який тип режиму перехоплення є необхідним для захисту національної безпеки та інших важливих національних інтересів від серйозних зовнішніх загроз. Утім, при функціонуванні такої системи свобода розсуду має бути вужчою, і має бути присутня низка гарантій. Суд вважав, що гарантії, визначені в контексті режимів цільового перехоплення, повинні бути адаптовані для відображення конкретних особливостей режиму масового перехоплення, і, зокрема, зростаючих ступенів втручання у права осіб за статтею 8 у міру того, як операція проходить через етапи, визначені вище.

Оцінюючи, чи діяли Держави в межах своєї свободи розсуду, ЄСПЛ розглянув у сукупності вимоги «згідно із законом» та «необхідність» й провів глобальну оцінку того, чи чітко визначає національна правова база:

1) підстави, на яких може бути дозволено масове перехоплення;
2) обставини, за яких можуть бути перехоплені комунікації особи;
3) процедуру, якої необхідно дотримуватися для надання дозволу на перехоплення;
4) процедури, яких необхідно дотримуватися для відбору, вивчення та використання матеріалів перехоплення;
5) запобіжні заходи, яких необхідно вживати при передачі матеріалів іншим сторонам;
6) обмеження тривалості перехоплення, зберігання матеріалів перехоплення та обставини, за яких такі матеріали можуть бути стерті та знищені;
7) процедури та умови нагляду незалежним органом за дотриманням вищезазначених гарантій та його повноваження щодо усунення недотримання;
8) процедури незалежного *ex post facto* перегляду такого дотримання та повноваження, надані компетентному органу, щодо усунення випадків недотримання.

Щодо запобіжних заходів, яких необхідно вживати при передачі матеріалів перехоплення іншим сторонам, ЄСПЛ зазначив, що передача іноземним Державам або міжнародним організаціям повинна обмежуватися матеріалами, зібраними та збереженими у спосіб, що відповідає Конвенції, і має підпадати під додаткові гарантії, що стосуються самої передачі. Перш за все обставини, за яких така передача може відбутися, повинні бути чітко викладені у національному законодавстві. По-друге, Держава, що передає, повинна забезпечити, щоб Держава, що приймає, при обробці даних вжила гарантії, що здатні запобігти зловживанню чи непропорційному втручанню. Зокрема, Держава, що приймає, повинна гарантувати безпечне зберігання матеріалів та обмежити їх подальше розголошення. Це не обов'язково означає, що Держава, яка приймає, повинна мати аналогічний захист до того, що має Держава, яка передає; також це не обов'язково вимагає підтвердження гарантій перед кожною передачею. По-третє, посилені гарантії будуть необхідні для передачі матеріалів, що потребують особливої конфіденційності, таких як конфіденційні журналістські матеріали. Крім того, передача матеріалів іноземним партнерам по розвідці також повинна підлягати незалежному контролю.

Щодо запобіжних заходів, яких необхідно вживати для отримання пов'язаних комунікаційних даних за допомогою масового перехоплення, ЄСПЛ зазначив, що ці дані можуть бути проаналізовані та досліджені таким чином, щоб створити детальну картину про особу за допомогою мапування соціальних мереж, відстеження місцезнаходження особи, відстеження її переглядів в Інтернеті, мапування шаблонів комунікації та розуміння того, з ким взаємодіяла особа. Суд вважав, що перехоплення, зберігання та пошук цих даних повинні бути проаналізовані з посиланням на ті самі гарантії, що застосовуються до змісту комунікацій, навіть коли правові норми, що регулюють їх обробку, не обов'язково повинні бути ідентичними в усіх відношеннях з тими, що регулюють поводження зі змістом.

Застосовуючи такі принципи до цієї справи, ЄСПЛ дійшов висновку, що режим таємного спостереження у Великобританії, незважаючи на його гарантії, не містив достатніх «наскрізних» гарантій для забезпечення адекватних й ефективних гарантій проти свавілля та ризику зловживань. Він виявив наступні недоліки в режимі: відсутність надання незалежного дозволу на спостереження, невключення категорій селекторів до заяви на отримання ордеру та відсутність попереднього національного дозволу для селекторів, пов'язаних із особою. Такі недоліки стосувалися не лише перехоплення змісту комунікацій, але й перехоплення пов'язаних комунікаційних даних. Хоча Уповноважений з питань перехоплення комунікацій («IC») забезпечував незалежний та ефективний нагляд за режимом, а IPT пропонував надійний засіб судового захисту будь-кому, хто підозрював, що його/її комунікації були перехоплені службами розвідки, ці важливі гарантії були недостатніми для того, щоб збалансувати недоліки, зазначені вище.

Щодо I), Стаття 10: заявники скаржилися, що режим масового перехоплення порушує статтю 10, оскільки він має стримувальний вплив на свободу спілкування журналістів.

ЄСПЛ розрізнив навмисний доступ служб розвідки до конфіденційних журналістських матеріалів через свідоме використання селекторів або пошукових термінів, пов'язаних із журналістом чи новинною організацією, та ненавмисний доступ як «побічний продукт» операції масового перехоплення. У першому сценарії ЄСПЛ вважав, що втручання має бути пропорційним тому, що спричинене обшуком будинку або робочого місця журналіста, і заявив, що селектори або пошукові терміни повинні бути дозволені суддею або іншим незалежним та неупередженим органом, наділеним повноваженнями визначати, чи воно «виправдане першочерговою вимогою в інтересах суспільства», і, зокрема, чи достатньо було б менш нав'язливого заходу для задоволення першочергового інтересу суспільства. У другому сценарії ЄСПЛ вважав, що ступінь втручання в журналістські комунікації та/або джерела неможливо передбачити на початку. Так, на етапі надання дозволу суддя або інший незалежний орган не зможе оцінити обґрунтованість втручання. Однак ЄСПЛ також вважав, що через технологічний розвиток нецільове спостереження має здатність до широкого охоплення. Тому, оскільки вивчення аналітиком журналістських комунікацій або пов'язаних із ними комунікаційних даних може призвести до ідентифікації джерела, ЄСПЛ вважав необхідним, щоб національне законодавство містило надійні гарантії щодо зберігання, вивчення, використання, подальшої передачі та знищення таких конфіденційних матеріалів. Крім того, якщо і колись стане очевидним, що комунікації або пов'язані з ними комунікаційні дані містять конфіденційні журналістські матеріали, їхнє подальше зберігання та вивчення аналітиком має бути можливим лише за наявності дозволу судді або іншого незалежного та неупередженого органу, наділеного повноваженнями визначати, чи є продовження зберігання та вивчення «виправданим першочерговою вимогою в інтересах суспільства».

Застосовуючи зазначені принципи до цієї справи, ЄСПЛ дійшов висновку, що правова база Великобританії щодо зберігання, подальшої передачі та знищення конфіденційних журналістських матеріалів забезпечувала належні гарантії. Однак вона не усунула недоліки, виявлені ЄСПЛ під час аналізу цього режиму за статтею 8, і не задовольнила вимогу про те, щоб використання селекторів або пошукових термінів (які, як відомо, пов'язані з журналістом) було дозволено суддею або іншим незалежним і неупередженим органом, наділеним повноваженнями визначати, чи є воно «виправдане першочерговою вимогою в інтересах суспільства», і чи достатньо було б менш інтрузивного заходу для задоволення першочергового інтересу суспільства. Крім того, не існувало достатніх гарантій того, що коли стане зрозуміло, що невідібрані для вивчення через навмисне використання селектора або пошукового терміну (який, як відомо, пов'язаний із журналістом) комунікаційні дані тим не менш містять конфіденційні журналістські матеріали, які мають зберігатися та вивчатися аналітиком лише за наявності дозволу судді або іншого незалежного й неупередженого органу ухвалення рішень, наділеного повноваженнями визначати, чи є їхнє подальше зберігання та вивчення «виправданим першочерговою вимогою в інтересах суспільства».

Щодо II), Стаття 8: Заявники скаржилися в основному на отримання національними органами влади запитуваних матеріалів перехоплення від іноземних розвідувальних служб.

ЄСПЛ вважав, що у випадках, коли запит на матеріали перехоплення надходить до Держави, що не є Договірною Стороною, запит повинен мати підстави згідно до національного права, і це право має бути доступним для зацікавленої особи та передбачуваним щодо його наслідків. Також необхідно мати чіткі детальні правила, які дають громадянам належну вказівку щодо обставин і умов, за яких органи влади уповноважені робити такий запит, і які забезпечують ефективні гарантії проти використання цих повноважень для обходу національного законодавства та/або зобов'язань Держав за ЄКПЛ.

Після отримання матеріалів перехоплення ЄСПЛ вважав, що Держава, яка приймає, повинна мати належні гарантії для їх вивчення, використання та зберігання, їх подальшої передачі та їх видалення й знищення. Крім того, будь-який режим, що дозволяє службам розвідки запитувати перехоплення або матеріали перехоплення у Держав, що не є Договірними Сторонами, або безпосередньо отримувати доступ до таких матеріалів, повинен підлягати незалежному нагляду, і також повинна бути можливість незалежного *ex post facto* перегляду.

Застосовуючи зазначені принципи до цієї справи, ЄСПЛ дійшов висновку, що в правовій базі Великобританії існували чіткі детальні правила, які давали громадянам адекватне розуміння обставин та умов, за яких влада була уповноважена звертатися із запитом до іноземної розвідувальної служби; національне законодавство містило ефективні гарантії проти використання таких запитів для обходу національного законодавства та/або ЄКПЛ; Великобританія мала належні гарантії для вивчення, використання, зберігання, подальшої передачі, видалення та знищення матеріалів; і режим підлягав незалежному нагляду з боку Уповноваженого з питань перехоплення комунікацій (IC Commissioner), а також існувала можливість *ex post facto* перегляду з боку Трибуналу з питань слідчих повноважень (IPT).

Щодо II), Стаття 10: Заявники скаржилися, що режим обміну розвідувальними даними порушив їхні права за статтею 10. ЄСПЛ вважав, що цей аргумент не викликає окремих питань, окрім тих, що випливають зі статті 8.

Щодо III): будь ласка, зверніться до пункту C нижче.

Висновок – Порушення статей 8 та 10 ЄКПЛ щодо масового перехоплення. Відсутність порушення статей 8 та 10 ЄКПЛ щодо отримання розвідувальних даних від іноземних служб.

Рішення ЄСПЛ у справі *«Центр справедливості проти Швеції» (Centrum för rättvisa v. Sweden)* [ВП], № 35252/08, 25 травня 2021 року

Фактичні обставини справи – Ця справа стосувалася сумісності зі статтею 8 режиму радіоелектронної розвідки Швеції, що діяв у травні 2018 року, зокрема масового перехоплення транскордонних комунікацій, включаючи зміст і пов'язані комунікаційні дані.

Заявник скаржився на те, що національне законодавство та практика масового перехоплення комунікацій порушують статтю 8 ЄКПЛ.

Право – Застосовуючи принципи, викладені у вищезгаданому рішенні у справі *Big Brother Watch*, ЄСПЛ відмітив, що основні характеристики шведського режиму масового перехоплення відповідали вимогам ЄКПЛ щодо доступності та передбачуваності закону, і вважав, що функціонування цього режиму здебільшого залишалося в межах «необхідного в демократичному суспільстві». Однак він виявив три недоліки: відсутність чіткого правила щодо знищення перехоплених матеріалів, які не містять персональних даних; відсутність вимоги у відповідному законодавстві про те, щоб при ухваленні рішення про передачу розвідувальних матеріалів іноземним партнерам враховувалися інтереси конфіденційності окремих осіб; та відсутність ефективного *ex post facto* перегляду.

Висновок – порушення статті 8 ЄКПЛ.

Рішення ЄСПЛ у справі *«Відер та Ґварньєрі проти Сполученого Королівства» (Wieder and Guarnieri v. the United Kingdom),* №№ 64371/16 та 64407/16, 12 вересня 2023 року

Фактичні обставини справи – Заявники, фізичні особи, які проживають за межами Держави-відповідача, скаржилися на несумісність зі статтею 8 ЄКПЛ режиму масового перехоплення інформації у Великобританії.

Право – Головним правовим питанням у цій справі було те, чи підпадають особи, які перебувають за межами Договірної Держави, під її територіальну юрисдикцію, для цілей скарги за цією нормою, якщо їхні електронні комунікації були (або ж існував ризик того, що будуть) перехоплені, обшукані та досліджені розвідувальними службами цієї Держави.

Враховуючи, що втручання у приватність комунікацій очевидно відбувається там, де ці комунікації перехоплюються, обшукуються, досліджуються та використовуються, і що в результаті праву на приватність також завдається шкода, ЄСПЛ постановив: втручання в права заявників за статтею 8 підпадає під територіальну юрисдикцію Держави-відповідача.

Щодо суті скарги, ЄСПЛ посилався на висновки, викладені у вищезгаданій справі *Big Brother Watch*.

Висновок – порушення статті 8 ЄКПЛ.

Рішення СЄС від 30 квітня 2024 року, *«M.N. (ІнкроЧат)» (M.N. (EncroChat))*, C-670/22, EU:C:2024:372

Фактичні обставини справи – У контексті розслідування, проведеного французькою владою, з'ясувалося, що обвинувачені особи використовували зашифровані мобільні телефони, які працювали за ліцензією «EncroChat», для вчинення злочинів, переважно пов'язаних з незаконним обігом наркотиків. Ці мобільні телефони мали спеціальне програмне забезпечення та модифіковане обладнання, що забезпечувало наскрізне зашифроване спілкування, яке не могло бути перехоплене звичайними слідчими засобами («сервіс EncroChat»). З дозволу судді навесні 2020 року на сервер було завантажено троянську програму, яка звідти через імітоване оновлення була встановлена на ці мобільні телефони. Загалом із 66 134 зареєстрованих користувачів, за повідомленнями 32 477 користувачів у 122 країнах постраждали від цієї програми, включаючи приблизно 4600 користувачів у Німеччині. Представники французької та нідерландської влади повідомили представників влади інших Держав-членів про своє розслідування. Представники німецької влади висловили зацікавленість у даних німецьких користувачів. Німецька кримінальна поліція оголосила про початок розслідування щодо всіх невідомих користувачів сервісу «EncroChat» за підозрою в участі в організованому незаконному обігу значних обсягів наркотичних засобів та у створенні злочинної організації. 2 червня 2020 року прокуратура Франкфурта звернулася до французької влади з попереднім Європейським ордером на виконання слідчих дій (EIO) з проханням надати дозвіл на використання даних сервісу «EncroChat» у кримінальному провадженні.

У контексті кримінального провадження, розпочатого щодо M.H., національний суд звернувся до СЄС із запитом про ухвалення попереднього рішення щодо кількох процесуальних та матеріальних аспектів сумісності цих Європейських ордерів на виконання слідчих дій із правом ЄС, включаючи питання про те, чи стаття 6(1) Директиви про Європейський ордер на виконання слідчих дій перешкоджає прокурору видавати такі ордери для передачі доказів, які вже знаходяться у розпорядженні компетентних органів Держави, що виконує ордер, якщо ці докази були отримані внаслідок перехоплення відповідними органами на території Держави, що видала ордер, телекомунікацій усіх користувачів мобільних телефонів, які через спеціальне програмне забезпечення та модифіковане обладнання забезпечували наскрізне зашифроване спілкування.

Право – СЄС постановив, що законність відповідних Європейських ордерів на виконання слідчих дій підпадає під ті самі умови, які могли б застосовуватися до передачі таких даних у суто національній ситуації в Державі, що видала ордер. Отже, якщо згідно з законодавством Держави, що видала ордер, така передача підлягала наявності конкретних доказів того, що обвинувачена особа вчинила серйозні злочини, або якщо докази у формі відповідних даних були допустимими, видача Європейських ордерів на виконання слідчих дій підпадала під усі ці умови. Натомість стаття 6(1)(b) Директиви про Європейський ордер на виконання слідчих дій не вимагала (зокрема, в ситуації, подібній до тієї, що розглядається в основному провадженні, де відповідні дані були зібрані компетентними органами Держави, що виконує ордер на території Держави, що його видала та в її інтересах), щоб видача Європейських ордерів на виконання слідчих дій для передачі доказів, які вже знаходяться у розпорядженні компетентних органів Держави, що виконує ордер, підпадала під ті самі матеріальні умови, що застосовувалися в Державі, що його видала, стосовно збору цих доказів.

У зв'язку з цим СЄС зазначив, що Європейський ордер на виконання слідчих дій є інструментом, що підпадає під сферу дії судового співробітництва у кримінальних справах, заснованого на принципі взаємного визнання судових рішень і презумпції того, що інші Держави-члени дотримуються права ЄС та, зокрема, основоположних прав. Тому орган, що видає Європейський ордер на виконання слідчих дій, не уповноважений переглядати законність окремої процедури, за допомогою якої Держава, що виконує ордер, зібрала докази, що підлягають передачі.

СЄС також нагадав, що згідно зі статтею 14(1) Директиви 2014/41 Держави-члени повинні забезпечити застосування засобів правового захисту, еквівалентних тим, які доступні у подібній національній справі до слідчого заходу, що стосується Європейського ордеру на виконання слідчих дій, і в цьому контексті компетентний суд повинен перевірити, чи виконані умови для видачі Європейського ордеру на виконання слідчих дій, а саме чи є він необхідним і пропорційним для цілей кримінального провадження, розпочатого в Державі, що його видала, і чи могли б бути призначені слідчі заходи, зазначені в ордері, за тих самих умов у подібній національній справі.

Наприкінці СЄС постановив, що у кримінальному провадженні щодо особи, підозрюваної у вчиненні кримінальних правопорушень, національні кримінальні суди зобов'язані ігнорувати інформацію та докази, отримані за допомогою Європейського ордеру на виконання слідчих дій, якщо ця особа не має можливості ефективно коментувати їх, а вони, ймовірно, матимуть вагомий вплив на встановлення фактичних обставин справи.

Рішення ЄСПЛ у справі *«А.Л. та Е.Дж.проти Франції» (A.L. and E.J. v. France)* (ухв.), **№№ 44715/20 та 47930/21, 24 вересня 2024 року**

Фактичні обставини справи – Заяви стосуються збору французькою владою даних щодо користувачів зашифрованих мобільних телефонів, які працювали за ліцензією «EncroChat», та їх передачі правоохоронним органам Великобританії. Щодо заявників були розпочаті кримінальні провадження у Великобританії, в яких їх звинувачували у використанні EncroChat. Заявники посилалися на статтю 8 окремо та у поєднанні зі статтею 13, а також на статтю 6 Конвенції.

Право – Спираючись на принципи, сформульовані у вищезгаданій справі *Відер та Ґварньєрі* (*Wieder and Guarnieri)*, ЄСПЛ постановив, що збір, зберігання та передача даних органам влади Великобританії відбулися у Франції, і тому втручання у права заявників за статтею 8 підпадає під територіальну юрисдикцію Держави-відповідача. ЄСПЛ зазначив, що цей висновок узгоджується з практикою Суду справедливості ЄС (справа *M.N. (EncroChat)*), згідно з яким принцип взаємного визнання судових рішень перешкоджав органу, який видав Європейський

ордер на виконання слідчих дій, переглянути законність окремої процедури, за допомогою якої Держава, що виконує ордер, зібрала докази, що підлягали передачі.

Щодо вичерпання національних засобів правового захисту ЄСПЛ вважав, що ні той факт, що заявники проживали за межами території Франції, ні той факт, що вони не обрали підпорядкування юрисдикції цієї Держави, не звільняв їх від обов'язку вичерпати наявні національні засоби правового захисту. ЄСПЛ встановив, що у національній правовій системі існують положення, які імплементують статтю 14 Директиви 2014/41, згідно з якою Держави-члени повинні забезпечити до слідчого заходу, якого стосується ордер, застосування засобів правового захисту, які є еквівалентними тим, що доступні у подібній національній справі. Окрім того, Суд зазначив, що ці положення узгоджуються з практикою Суду справедливості ЄС, згідно з якою Держави-члени зобов'язані забезпечити повагу до права на ефективний засіб правового захисту, закріпленого у статті 47 Хартії, у контексті процедури видачі та виконання Європейського ордера на проведення розслідування. Оскільки згідно з національним законодавством особа, щодо якої проводиться розслідування, могла оскаржити включення до матеріалів кримінального провадження доказів, отриманих в окремому провадженні, зокрема посилаючись на порушення прав, гарантованих Конвенцією, цей засіб правового захисту був також відкритий для заявників, які могли б домагатися скасування запровадженого ордером заходу на тих самих умовах і таким же чином, як і особа, щодо якої проводиться розслідування у Франції, включаючи посилання на статтю 8 Конвенції.

Дійшовши висновку про те, що заявники мали у своєму розпорядженні ефективний засіб правового захисту, ЄСПЛ також зазначив, що згідно зі статтею 14(7) Директиви 2014/41 Держава, що видала ордер, повинна була врахувати факт успішного оскарження ордеру. Тому, оскільки кримінальне провадження щодо заявників ще тривало, суди Великобританії були б зобов'язані врахувати можливий сприятливий результат провадження у французьких судах.

Висновок – неприйнятність скарг за статтею 8 Конвенції через невичерпання національних засобів правового захисту; неприйнятність скарг за статтями 6 та 13 Конвенції як явно необґрунтованих.

B. Обов'язки постачальників послуг електронних комунікацій щодо зберігання даних та цільового доступу національними органами влади

B. 1. Дані абонента

Рішення СЄС від 2 жовтня 2018 року, *Прокуратура (Ministerio Fiscal)*, C-207/16, EU:C:2018:788

Фактичні обставини справи – Іспанська поліція в ході розслідування крадіжки гаманця та мобільного телефону звернулася до слідчого судді з клопотанням надати їм доступ до даних, що ідентифікують користувачів телефонних номерів, що були активовані викраденим телефоном протягом дванадцяти днів після крадіжки. Слідчий суддя відхилив клопотання, зокрема, на тій підставі, що дії, які стали підставою для кримінального розслідування, не становили «серйозного» злочину.

Згодом запитуючий суд звернувся до СЄС за роз'ясненнями щодо встановлення порогу серйозності, за якого втручання в основоположні права може вважатися обґрунтованим.

Право – СЄС постановив, що статтю 15(1) Директиви про приватність та електронні комунікації у світлі статей 7 та 8 Хартії слід тлумачити таким чином: доступ державних органів до даних з метою ідентифікації власників SIM-карток (прізвища, імена та, за потреби, адреси власників),

активованих у викраденому мобільному телефоні, становив втручання в їхні основоположні права, що не було достатньо серйозним для обмеження такого доступу у сфері запобігання, розслідування, виявлення та переслідування кримінальних правопорушень, з причини боротьби з тяжкими злочинами. Зокрема, Суд зазначив, що відповідно до принципу пропорційності, серйозне втручання може бути обґрунтоване у сферах запобігання, розслідування, виявлення та переслідування кримінальних правопорушень лише метою боротьби зі злочинами, що визначаються як «тяжкі». Натомість, коли спричинене таким доступом втручання не було серйозним, такий доступ міг бути обґрунтованим метою запобігання, розслідування, виявлення та переслідування кримінальних правопорушень загалом. Суд не вважав доступ до даних, які були предметом запиту, особливо серйозним втручанням, оскільки він лише дозволяв пов'язати SIM-картки, активовані протягом певного періоду у викраденому мобільному телефоні з ідентифікацією їхніх власників. Без зіставлення цих даних з комунікаційними даними SIM-карток та даними про місцезнаходження, ці дані не дозволяли встановити дату, час, тривалість та одержувачів комунікацій, за допомогою відповідних SIM-карток, а також місця, де відбувалися ці комунікації, або частоту цих комунікацій з конкретними особами протягом певного періоду. Тому ці дані не дозволяли зробити точних висновків щодо приватного життя відповідних осіб.

Рішення ЄСПЛ у справі *«Брейер проти Німеччини» (Breyer v. Germany)*, № 50001/12, 30 січня 2020 року

Фактичні обставини справи – Заявники скаржилися за статтею 8 ЄКПЛ (право на повагу до приватного та сімейного життя) на те, що їхні деякі персональні дані, як користувачів передплачених SIM-карток (номер телефону, ім'я та адреса, дата народження та дата укладення договору), зберігалися їхніми відповідними ППЕК відповідно до юридичного зобов'язання, що діяло станом на 1 січня 2008 року.

Право – ЄСПЛ нагадав свою усталену практику щодо втручання у право на приватне життя за статтею 8 внаслідок зберігання, обробки та використання персональних даних (включаючи справу *«Бен Файза проти Франції» (Ben Faiza v. France)*, № 31446/12, 8 лютого 2018 року).

Щодо обґрунтування втручання ЄСПЛ встановив, що оскаржуване зберігання мало підґрунтя у національному законодавстві, яке було достатньо чітким та передбачуваним. Крім того, тривалість та технічний аспект зберігання були чітко визначені. Щодо того, чи було втручання необхідним у демократичному суспільстві, ЄСПЛ визнав, що попередня реєстрація абонентів мобільного зв'язку значно спрощувала та прискорювала розслідування правоохоронними органами і таким чином могла сприяти ефективному забезпеченню правопорядку та запобіганню заворушенням або злочинам. Він також підтвердив, що в контексті національної безпеки органи влади мають певну свободу розсуду при виборі засобів для досягнення законної мети. Суд також зазначив, що серед Держав-членів немає консенсусу щодо зберігання інформації про абонентів передплачених SIM-карток. Враховуючи таку свободу розсуду, зобов'язання зберігати інформацію про абонентів було, загалом, адекватною відповіддю на зміни в поведінці комунікації та засобах телекомунікації. Оцінюючи пропорційність оскаржуваного юридичного зобов'язання, ЄСПЛ відрізнив цю справу від тих, де зберігалася дуже особиста інформація (наприклад, справа *Ben Faiza*, згадана вище), і, посилаючись також на рішення Суду справедливості ЄС у справі *Ministerio fiscal*, згаданій вище, встановив, що втручання було обмеженим за своїм характером.

ЄСПЛ також зазначив, що, хоча заявники скаржилися лише на зберігання їхніх персональних даних, він не міг розглядати пропорційність втручання без ретельної оцінки майбутнього можливого доступу до цієї інформації та її використання. Він вважав, що доступ до даних був обмежений певним колом органів влади (або чітко перелічених, і доступ у цьому випадку дозволявся через централізовану та автоматизовану процедуру; або визначених через

виконувані ними завдання, і в цьому випадку дозвіл на доступ надавався шляхом звернення з письмовим запитом). Крім того, доступ підлягав низці гарантій: лише Федеральне мережеве агентство або відповідний ППЕК могли розголошувати дані; доступ був обмежений необхідними даними; ця вимога необхідності забезпечувалася загальним зобов'язанням відповідних органів, що вилучали інформацію, без зайвої затримки видаляти будь-які дані, які їм не були потрібні; у контексті розслідування правопорушень мала існувати щонайменше первинна підозра. Що стосується можливостей перегляду та нагляду за запитами про надання інформації, то ЄСПЛ відрізнив цю справу від попередніх рішень, що стосувалися різних втручань у статтю 8. Суд вважав, що такі гарантії слід розглядати як важливий, але не вирішальний елемент в оцінці пропорційності з огляду на обмежений набір даних. На думку Суду, відповідна правова база пропонувала достатні гарантії, оскільки кожне вилучення інформації та відповідні відомості щодо її вилучення фіксувалися з метою нагляду за захистом даних, який здійснювався спеціальними незалежними органами, і будь-хто, хто вважав, що його права були порушені, міг подати скаргу.

Висновок – відсутність порушення статті 8 ЄКПЛ.

B. 2. Дані про трафік і місцезнаходження

Рішення СЄС від 08 квітня 2014 року, *«Діджитал Райтс Айрленд та інші» (Digital Rights Ireland e.a.)*, C-293/12 та C 594/12, EU:C:2014:238

Фактичні обставини справи – Справу було розпочато на підставі двох звернень за попереднім рішенням щодо дійсності Директиви про збереження даних, поданих у контексті національних проваджень, у яких законність національних законодавчих та адміністративних заходів щодо збереження даних, отриманих з електронних комунікацій, було оскаржено всупереч конституційним правам і правам ЄС на захист даних.

Право – СЄС постановив, що зобов'язання ППЕК зберігати дані, що стосуються приватного життя і комунікацій, а також подальший доступ до цих даних національних органів влади, становили втручання в права, гарантовані статтями 7 і 8 Хартії. Втручання було визнано особливо серйозним і таким, що може створити для відповідних осіб відчуття, що їхнє приватне життя є об'єктом постійного нагляду.

СЄС постановив, що оцінка пропорційності включає аналіз: (i) доцільності та (ii) необхідності оскаржуваних заходів з огляду на їхні цілі. Спираючись також на принципи, викладені в практиці ЄСПЛ щодо меж свободи розсуду, СЄС постановив, що обсяг дискреційних повноважень законодавчого органу ЄС може бути обмежений низкою факторів, зокрема, відповідною сферою, природою права, про яке йдеться, характером і ступенем втручання та метою, яку переслідує це втручання, і що в цій справі обсяг дискреційних повноважень було звужено через важливість захисту персональних даних та серйозність втручання.

Попри те, що оскаржувані заходи могли вважатися доцільними з огляду на зростаючу важливість засобів електронного зв'язку та їхнє використання як цінного інструменту в рамках кримінальних розслідувань, СЄС вважає, що Директива про збереження даних не обмежувалася лише тим, що було суворо необхідним для досягнення її цілей, з наступних причин.

По-перше, вона охоплювала в узагальненому вигляді всіх осіб і всі засоби електронного зв'язку, а також всі дані про трафік без будь-якого розрізнення, обмеження або винятку з огляду на мету боротьби з тяжкими злочинами. Вона не обмежувалася даними, що стосуються певного періоду часу та/або певної географічної зони, і застосовувалася навіть до осіб, щодо яких не було жодних доказів, які б вказували на те, що їхня поведінка може бути пов'язана з тяжкими злочинами.

По-друге, вона не містила матеріальних і процесуальних умов, що регулювали б доступ компетентних національних органів влади до даних та їхнє подальше використання. Просто посилаючись в цілому на тяжкі злочини, як їх визначає кожна Держава-член у своєму національному законодавстві, Директива не встановила жодного об'єктивного критерію, за допомогою якого можна було б визначити, які злочини вважаються достатньо серйозними, щоб виправдати таке широке втручання в основоположні права, закріплені в статтях 7 і 8 Хартії. Крім того, доступ компетентних національних органів влади до збережених даних не залежав від попереднього розгляду, проведеного судом або незалежним адміністративним органом, рішення якого мало на меті обмежити доступ до даних та їхнє використання лише тим, що було суворо необхідним.

По-третє, вона вимагала, щоб усі дані зберігалися протягом щонайменше шести місяців, без будь-якого розрізнення між категоріями даних на основі їхньої можливої користі для досягнення поставленої мети або залежно від відповідних осіб. СЄС дійшов висновку, що Директива спричинила широкомасштабне й особливо серйозне втручання в основоположні права, закріплені в статтях 7 і 8 Хартії. Водночас таке втручання не було чітко визначено, щоб гарантувати, що воно дійсно обмежувалося тим, що було суворо необхідним. СЄС також зазначив, що директива не передбачала достатніх гарантій за допомогою технічних та організаційних заходів для забезпечення ефективного захисту збережених даних від ризику зловживань, а також від будь-якого незаконного доступу та використання. Вона не забезпечувала незворотного знищення даних після закінчення строку їхнього зберігання, а також не вимагала, щоб ці дані зберігалися в межах ЄС.

Рішення СЄС від 21 грудня 2016 року, *«Теле2 Сверіге і Ватсон та інші» (Tele2 Sverige and Watson and Others)*, C-203/15 та C-698/15, EU:C:2016:970

Фактичні обставини справи – Справу було розпочато на підставі двох звернень за попереднім рішенням щодо сумісності з правом ЄС національного законодавства, яке передбачало загальне збереження всіх даних про трафік і місцезнаходження для цілей боротьби зі злочинністю.

Право – СЄС постановив, що пункт 1 статті 15 Директиви про приватність та електронні комунікації з огляду на статті 7, 8 і 11 та пункт 1 статті 52 Хартії варто тлумачити як такий, що виключає національне законодавство, яке:

1) з метою боротьби зі злочинністю передбачає загальне і невибіркове збереження даних про трафік і місцезнаходження всіх користувачів, пов'язаних з усіма засобами електронного зв'язку.

Зокрема, СЄС послався на згадану вище справу *«Діджитал Райтс Айрленд та інші» (Digital Rights Ireland e.a.)*, і вказав, що зберігання даних має обмежуватися тим, що є суворо необхідним з огляду на категорії даних, засоби зв'язку та осіб, яких вони стосуються, і прийнятий період зберігання. Для того, щоб задовольнити ці вимоги, національне законодавство повинно, по-перше, встановлювати чіткі та зрозумілі правила, що регулюють сферу застосування таких заходів щодо зберігання даних та встановлюють мінімальні гарантії. По-друге, воно повинно передбачати суттєві умови для зберігання даних, щоб підтримувати зв'язок між даними, що підлягають зберіганню, та метою, яку переслідують;

2) регулює захист і безпеку даних про трафік та місцезнаходження і, зокрема, доступ компетентних національних органів влади до збережених даних, якщо (i) мета, яку переслідує такий доступ в контексті боротьби зі злочинністю, не обмежується виключно боротьбою з тяжкими злочинами, (ii) доступ до даних не підлягає попередньому розгляду судом або незалежним адміністративним органом, і (iii) немає вимоги, що відповідні дані повинні зберігатися в межах ЄС.

Рішення ЄСПЛ у справі *«Бен Файза проти Франції» (Ben Faiza v. France)*, № 31446/12, 8 лютого 2018 року

Фактичні обставини справи – Справа стосувалася сумісності зі статтею 8 ЄКПЛ доступу судової поліції на підставі дозволу прокурора до даних про трафік і місцезнаходження, що зберігаються ППЕК.

Право – ЄСПЛ вважав, що доступ національних органів влади до даних про трафік і місцезнаходження становив втручання у право заявника, передбачене статтею 8.

Стосовно обґрунтування втручання ЄСПЛ вважає, що доступ до даних мав правову основу в національному законодавстві і був передбачуваним. Стосовно гарантій проти свавілля ЄСПЛ зазначив, що судова поліція могла мати доступ до комунікаційних даних після отримання дозволу прокурора. Крім того, такий доступ підлягав судовому перегляду *ex post facto* в контексті кримінального провадження щодо відповідної особи, де судді могли оцінити його законність. У разі визнання доступу незаконним, судді могли виключити відповідні докази з провадження. ЄСПЛ також зазначив, що гарантії, передбачені щодо доступу до комунікаційних даних, є менш суворими, ніж гарантії, встановлені щодо геолокації в режимі реального часу. Утім, Суд вважає, що така диференціація виправдана менш серйозним характером втручання.

Стосовно того, чи було втручання необхідним у демократичному суспільстві, ЄСПЛ вважає, що воно було необхідним для ліквідації масштабної операції з незаконного обігу наркотиків. Крім того, отриману інформацію було використано у кримінальному провадженні, де заявник користувався ефективним контролем, як того вимагає верховенство права, і міг обмежити оскаржуване втручання до того, що було необхідним у демократичному суспільстві.

Висновок – відсутність порушення статті 8 ЄКПЛ.

Рішення СЄС від 16 липня 2020 року, *«Фейсбук Ірландія та Шремс» (Facebook Ireland and Schrems)*, C-311/18, EU:C:2020:559

Фактичні обставини справи – Після рішення СЄС від 6 жовтня 2015 року у справі *«Шремс» (Schrems)*, C-362/14, EU:C:2015:650), яким було визнано недійсним рішення про «безпечну гавань», згідно з яким Європейська комісія вважала, що Сполучені Штати забезпечили належний рівень захисту переданих персональних даних, пан Шремс знову оскаржив передачу його даних компанією «Фейсбук Ірландія» (Facebook Ireland) до Сполучених Штатів та зберігання його даних на серверах, розташованих у цій країні. Він скаржився на те, що законодавство Сполучених Штатів вимагає від компанії «Фейсбук Інк» (Facebook Inc). надавати передані їй персональні дані певним органам влади Сполучених Штатів, таким як Агентство національної безпеки та Федеральне бюро розслідувань. Пан Шремс стверджував, що оскільки ці дані використовувалися в контексті різних програм моніторингу у спосіб, несумісний зі статтями 7, 8 і 47 Хартії, рішення 2010/87/ЄС не може виправдати передачу цих даних до Сполучених Штатів.

Національний суд направив до СЄС низку запитань для отримання попереднього рішення, зокрема, чи застосовується право ЄС до передачі даних від приватної компанії в ЄС до приватної компанії в третій країні; якщо так, то яким чином необхідно оцінювати рівень захисту, наданий у третій країні; і чи відповідає рівень захисту, наданий Сполученими Штатами, суті прав, гарантованих статтею 47 Хартії.

Право – СЄС постановив, що положення Загального регламенту захисту даних застосовуються до передачі персональних даних у комерційних цілях суб'єктом господарювання, заснованим у Державі-члені, іншому суб'єкту господарювання, заснованому в третій країні, незалежно від

того, чи підлягають ці дані обробці органами влади третьої країни під час такої передачі або після неї для цілей громадської безпеки, оборони та державної безпеки. Крім того, відповідні гарантії, законні права й ефективні засоби правового захисту, передбачені регламентом, повинні були забезпечити суб'єктам даних, чиї персональні дані передаються до третьої країни відповідно до стандартних положень про захист даних, рівень захисту, еквівалентний тому, що гарантується в межах ЄС. З цією метою оцінка рівня захисту, що надається в контексті такої передачі, повинна враховувати як договірні положення, узгоджені між контролером або процесором, заснованим у ЄС, і одержувачем, заснованим у відповідній третій країні, так і відповідні аспекти правової системи цієї третьої країни стосовно будь-якого доступу органів державної влади цієї третьої країни до переданих персональних даних.

Крім того, за відсутності дійсного рішення Комісії про належний рівень захисту, компетентний наглядовий орган влади повинен був призупинити або заборонити передачу даних до третьої країни, якщо, на думку цього наглядового органу і з огляду на всі обставини цієї передачі, стандартні положення про захист даних, прийняті Комісією, не були або не могли бути дотримані в цій третій країні, а захист даних, що передаються (як того вимагає законодавство ЄС), не міг бути забезпечений іншими способами.

Для того, щоб Комісія ухвалила рішення про належний рівень захисту, їй потрібно було встановити, що третя країна, про яку йдеться, забезпечила своїм національним законодавством або міжнародними зобов'язаннями рівень захисту основоположних прав, що був еквівалентний тому, який гарантується в правовому порядку ЄС. На думку СЄС, рішення про «безпечну гавань» було недійсним. Відповідне положення не вказувало на існування будь-яких обмежень повноважень, що надавалися для здійснення програм спостереження в цілях зовнішньої розвідки, або гарантій для осіб, які не є громадянами США і потенційно могли бути об'єктом цих програм. За цих обставин воно не могло забезпечити рівень захисту, еквівалентний тому, що гарантується Хартією. Крім того, стосовно програм моніторингу було очевидно, що цей наказ не надавав прав, що могли б бути застосовані проти органів влади Сполучених Штатів в американських судах.

Рішення СЄС від 6 жовтня 2020 року, *«Ла Квадратюр дю Нет та інші» (La Quadrature du Net and Others)*, C-511/18, C-512/18 та C-520/18, EU:C:2020:791

Фактичні обставини справи – Справу було розпочато на підставі трьох звернень за попереднім рішенням про застосування Директиви про приватність та електронні комунікації до національного законодавства, що створює для ППЕК зобов'язання, яке вимагає від них:

(i) загального та невибіркового зберігання даних про трафік та місцезнаходження з метою захисту національної безпеки та боротьби з тероризмом;

(ii) запровадження у своїх мережах заходів, що дозволяють здійснювати автоматизований аналіз і збір даних про трафік та місцезнаходження в режимі реального часу, а також збір технічних даних про місцезнаходження використовуваного кінцевого (термінального) обладнання в режимі реального часу.

Право – СЄС підкреслив, що мета захисту національної безпеки ще не була предметом спеціального розгляду СЄС у його рішеннях, що тлумачать Директиву про приватність та електронні комунікації. Він підтвердив, що, попри те, що ця Директива у світлі Хартії виключає законодавчі заходи, що передбачають загальне та невибіркове зберігання даних про трафік і місцезнаходження, якщо Держава-член ЄС зіткнулася з серйозною загрозою національній безпеці, яка є реальною, наявною або передбачуваною, не існує жодних перешкод для вжиття законодавчих заходів, що вимагають від ППЕК збереження даних про трафік і місцезнаходження протягом періоду, обмеженого суворою необхідністю, який може бути продовжений, якщо загроза не зникне. У цьому випадку рішення про введення такої вказівки

повинно підлягати ефективному перегляду або судом, або незалежним адміністративним органом, рішення якого є обов'язковим до виконання, з метою перевірки наявності однієї з цих ситуацій і дотримання умов і гарантій, що повинні бути встановлені. З метою боротьби з тяжкими злочинами і запобігання серйозним загрозам громадській безпеці, Держава-член могла також передбачити (з обмеженнями в часі та згідно з вимогою суворої необхідності) цільове зберігання даних про трафік і місцезнаходження на основі об'єктивних та недискримінаційних факторів відповідно до категорій відповідних осіб або з використанням географічного критерію, або IP-адреси, присвоєної джерелу інтернет-з'єднання. Держава-член також може здійснювати загальне і невибіркове зберігання даних, що стосуються цивільної ідентичності користувачів засобів електронних комунікацій, без встановлення конкретного строку зберігання цих даних.

Крім того, Директива про приватність та електронні комунікації, що розглядається у світлі Хартії, не перешкоджає існуванню національних правових норм, що вимагають від ППЕК вдаватися, по-перше, до автоматизованого аналізу та збору даних про трафік і місцезнаходження в режимі реального часу, а по-друге, до збору в режимі реального часу технічних даних про місцезнаходження використовуваного кінцевого (термінального) обладнання, якщо це обмежується ситуаціями, коли Держава-член стикається з серйозною загрозою національній безпеці, яка є реальною, наявною або передбачуваною, і якщо використання такого аналізу може бути предметом ефективного розгляду судом або незалежним адміністративним органом, рішення якого є обов'язковим до виконання; а також, якщо доступ до збору даних про трафік і місцезнаходження в режимі реального часу обмежувався особами, щодо яких існували вагомі підстави підозрювати, що вони причетні до терористичної діяльності, і підлягав попередньому розгляду або судом, або незалежним адміністративним органом, рішення якого було обов'язковим до виконання.

Рішення СЄС від 2 березня 2021 року, *Прокуратура (Prokuratuur)*, C-746/18, EU:C:2021:152

Фактичні обставини справи – Справу було розпочато на підставі звернення за попереднім рішенням про застосування Директиви про приватність та електронні комунікації до національного законодавства, що дозволяє доступ до даних, збережених ППЕК, у контексті кримінального провадження.

Право – СЄС повторив, що пункт 1 статті 15 Директиви про приватність та електронні комунікації дозволяє доступ до збережених даних про трафік або місцезнаходження з метою боротьби зі злочинністю лише тоді, коли йдеться про тяжкі злочини або серйозні загрози громадській безпеці, незалежно від тривалості періоду, щодо якого запитується доступ, а також кількості або характеру даних, наявних щодо цього періоду.

СЄС також постановив, що повноваження розглядати запити на доступ до інформації не можуть бути надані прокуратурі, оскільки завдання останньої щодо керівництва досудовим розслідуванням і здійснення кримінального переслідування можуть вплинути на її незалежність *vis-à-vis* сторін кримінального провадження.

Рішення ЄСПЛ у справі *«Біг Бразер Вотч та інші проти Сполученого Королівства» (Big Brother Watch and Others v. the United Kingdom)* [ВП], згадане вище

Фактичні обставини справи – Будь ласка, ознайомтесь з відповідною інформацією в пункті B вище.

Право – Заявники скаржилися на те, що режим отримання комунікаційних даних від ППЕК був несумісним з їхніми правами, передбаченими статтями 8 і 10 ЄКПЛ. Щодо обох скарг Велика Палата підтримала висновки Палати:

Щодо статті 8, то на момент розгляду справи Палатою тривало національне провадження щодо нового законодавства, яке регулює зберігання комунікаційних даних ППЕК. У ході цього провадження Уряд Великої Британії визнав, що відповідна нормативно-правова база не відповідає праву ЄС, і, відповідно, національні судді визнали її несумісною з основними правами, гарантованими законодавством ЄС.

Враховуючи пріоритет права ЄС над правом Великої Британії на той час, а також поступку Уряду в національному провадженні, ЄСПЛ постановив, що національне законодавство вимагає, щоб будь-який механізм, який дозволяє органам влади отримувати доступ до даних, що зберігаються ППЕК, обмежував доступ метою боротьби з «тяжкими злочинами», і щоб такий доступ підлягав попередньому перегляду судом або незалежним адміністративним органом. Оскільки режим, що існував до цього, мав ті ж самі недоліки, що й наступний режим отримання даних, ЄСПЛ постановив, що він не може бути визнаний таким, що відповідає закону в розумінні статті 8 ЄКПЛ.

Щодо статті 10 ЄСПЛ визнав, що оскаржуваний режим отримання даних передбачав посилений захист у випадку, коли дані запитувалися з метою ідентифікації журналістських джерел. Водночас ці положення не застосовувалися в кожному випадку, коли надходив запит на комунікаційні дані журналіста або коли існувала можливість такого побічного втручання. Крім того, у справах про доступ до комунікаційних даних журналіста не було спеціальних положень, які б обмежували доступ з метою боротьби з «тяжкими злочинами». Отже, ЄСПЛ вважав, що режим отримання даних не відповідав закону в розумінні статті 10 ЄКПЛ.

Висновок – Порушення статей 8 і 10 ЄКПЛ щодо порядку отримання комунікаційних даних від ППЕК.

Рішення ЄСПЛ у справі *«Екімджієв та інші проти Болгарії» (Ekimdzhiev and Others v. Bulgaria)*, № 70078/12, 11 січня 2022 року

Фактичні обставини справи – Справа стосувалася відповідності статті 8 законодавства Болгарії та практики щодо зберігання і доступу до комунікаційних даних. Заявники, два адвокати та дві неурядові організації, стверджували, що характер їхньої діяльності покладає на них ризик доступу до їхніх комунікаційних даних з боку органів влади.

Право – Заявники скаржилися на те, що система зберігання та подальшого доступу до комунікаційних даних (абонентські дані, дані про трафік і місцезнаходження) не відповідала вимогам статті 8 ЄКПЛ.

Спираючись на свою попередню практику (*«Брейер» (Breyer), «Центр справедливості» (Centrum för rättvisa)* та *«Біг Бразер Вотч» (Big Brother Watch)*, згадані вище), ЄСПЛ постановив, що:

(a) саме лише зберігання цих даних становило втручання у право відповідних заявників на повагу до приватного життя та кореспонденції, а також право на повагу до кореспонденції організацій-заявників;

(b) доступ органів влади до збережених комунікаційних даних становив подальше втручання у статтю 8.

Стосовно того, чи було втручання обґрунтоване, ЄСПЛ, спираючись на згадані вище справи *«Центр справедливості» (Centrum för rättvisa)* та *«Біг Бразер Вотч»*, вважав, що отримання цих даних шляхом масового перехоплення може становити таке ж втручання, що й масове отримання змісту повідомлень. Тому слід застосовувати ті ж самі гарантії, що й до змісту. ЄСПЛ також зазначив, що загальне зберігання комунікаційних даних ППЕК і доступ до них органів влади в окремих випадках має супроводжуватися, *mutatis mutandis*, тими ж гарантіями, що й

таємне спостереження (він послався, зокрема, на справу *«Роман Захаров» (Roman Zakharov)*, згадану вище).

Застосовуючи ці принципи до справи, що розглядається, та оцінюючи низку елементів (доступність закону; рівень захисту збережених даних, гарантований ППЕК; аналіз підстав, на яких органи влади можуть отримати доступ до збережених даних; процедури отримання доступу; тривалість зберігання та використання отриманих даних, що в подальшому не використовувалися в кримінальному провадженні; а також розглядаючи процедури зберігання, доступу, вивчення, використання, передачі та знищення даних, до яких отримали доступ органи влади; механізми нагляду; повідомлення зацікавлених осіб; засоби правового захисту), ЄСПЛ дійшов висновку, що правова база, про яку йдеться, не відповідає мінімальним гарантіям проти свавілля та зловживань, що вимагаються статтею 8 ЄКПЛ, у наступних аспектах:

(а) процедура отримання дозволу не може забезпечити, щоб органи влади отримували доступ до збережених комунікаційних даних лише тоді, коли це «необхідно в демократичному суспільстві»;

(б) не було встановлено чітких часових обмежень для знищення даних, до яких органи влади отримали доступ у ході кримінального провадження;

(в) не існувало загальнодоступних правил щодо зберігання, доступу, вивчення, використання, передачі та знищення комунікаційних даних, до яких мають доступ органи влади;

(г) система нагляду видається нездатною ефективно перевіряти наявність зловживань;

(ґ) механізми повідомлення були надто обмеженими; і

(д) не було ефективних засобів правового захисту.

Висновок – порушення статті 8 ЄКПЛ щодо системи зберігання та доступу до комунікаційних даних.

Рішення СЄС від 5 квітня 2022 року, *«Комісар Ґарда Сіхани та інші» (Commissioner of An Garda Síochána e.a.)*, C-140/20, EU:C:2022:258

Фактичні обставини справи – Справу було розпочато на підставі звернення для ухвалення попереднього рішення про застосування Директиви про приватність та електронні комунікації до національного законодавства, що дозволяє доступ до даних, які зберігаються ППЕК у контексті кримінального провадження.

Право – СЄС підтвердив свою усталену практику, згідно з якою право ЄС виключає національне законодавство, що передбачає загальне та невибіркове збереження даних про трафік і місцезнаходження, пов'язаних з електронними комунікаціями, як превентивний захід з метою боротьби з тяжкими злочинами і запобігання серйозним загрозам громадській безпеці. Однак він вважає, що право ЄС не виключає:

– цілеспрямоване зберігання даних про трафік і місцезнаходження протягом обмеженого періоду часу, обумовленого об'єктивними й недискримінаційними факторами;

– загальне та невибіркове зберігання IP-адрес, присвоєних джерелу інтернет-з'єднання, протягом обмеженого періоду часу;

– загальне та невибіркове зберігання даних щодо цивільної ідентичності користувачів систем електронних комунікацій; і

– звернення до вказівок, що вимагають від ППЕК, згідно з рішенням компетентного органу влади, що підлягає ефективному судовому контролю, здійснювати протягом певного періоду

часу оперативне зберігання даних про трафік і місцезнаходження, що перебувають у володінні цих ППЕК, за умови, що ці заходи за допомогою чітких і зрозумілих правил забезпечують, що зберігання даних, про які йде мова, підлягає дотриманню застосовних матеріальних і процесуальних умов, і що відповідні особи мають ефективні гарантії проти ризиків зловживань.

Крім того, СЄС вважає, що право ЄС виключає національне законодавство, згідно з яким централізована обробка запитів на доступ до даних, що зберігаються ППЕК, виданих поліцією в контексті розслідування або притягнення до відповідальності за тяжкі кримінальні правопорушення, є обов'язком поліцейського за сприяння підрозділу, створеного в рамках поліцейської служби, що має певну автономію у виконанні своїх обов'язків, і чиї рішення згодом можуть підлягати судовому перегляду.

Рішення СЄС від 20 вересня 2022 року, *«СпейсНет і Телеком Дойчланд» (SpaceNet et Telekom Deutschland)*, C-793/19 та C-794/19, EU:C:2022:702

Фактичні обставини справи – Справу було розпочато на підставі двох звернень за попереднім рішенням про застосування Директиви про приватність та електронні комунікації до національного законодавства, що зобов'язує ППЕК зберігати в загальному та невибірковому порядку більшу частину даних про трафік і місцезнаходження кінцевих користувачів цих послуг (включно з даними, що стосуються відвіданих вебсайтів і даних з електронних поштових служб), встановлюючи строк зберігання в кілька тижнів та норми, що покликані забезпечити ефективний захист збережених даних від ризиків зловживань і від будь-якого незаконного доступу до цих даних.

Право – СЄС підтвердив свою усталену практику проти загального й невибіркового зберігання даних про трафік і місцезнаходження з метою боротьби з тяжкими злочинами або запобігання серйозним загрозам громадській безпеці (див. *«Ла Квадратюр дю Нет» (La Quadrature du Net)* і *«Комісар Ґарда Сіхани» (Commissioner of An Garda Síochána)*, обидві справи згадані вище). Він встановив, що національне законодавство, про яке йдеться у цій справі, не відповідає праву ЄС, незважаючи на наявність гарантій і коротший строк зберігання даних, ніж у попередніх справах. СЄС також постановив, що зберігання цих даних і доступ до них є окремими втручаннями в основоположні права суб'єктів даних, які потребують окремого обґрунтування, і що таким чином національне законодавство, яке забезпечує повне дотримання умов, що випливають із судової практики щодо доступу до збережених даних, за своєю природою не може обмежити або навіть виправити серйозне втручання у права суб'єктів даних, яке може виникнути в результаті загального зберігання цих даних.

Рішення СЄС від 20 вересня 2022 року, *«ВД і СР» (VD and SR)*, C-339/20 та C-397/20, EU:C:2022:703

Фактичні обставини справи – Справу було розпочато на підставі двох звернень для ухвалення попереднього рішення щодо тлумачення положень ЄС про зловживання на ринку в поєднанні з пунктом 1 статті 15 Директиви про приватність та електронні комунікації. Звернення були подані в контексті кримінальних проваджень стосовно ВД (VD) і СР (SR) щодо інсайдерської торгівлі, приховування інсайдерської торгівлі, пособництва та підбурювання, корупції і відмивання грошей.

Право – СЄС постановив, що Директива про зловживання на ринку та Регламент про зловживання на ринку, розглянуті в поєднанні з Директивою про приватність та електронні комунікації і з огляду на статті 7, 8 та 11 Хартії, не дають дозволу на загальне та невибіркове

зберігання даних про трафік ППЕК протягом одного року з дня, коли ці дані було отримано, з метою боротьби з правопорушеннями, пов'язаними зі зловживанням на ринку.

СЄС також постановив, що право ЄС виключає національне законодавство, яке обмежує тимчасові наслідки визнання недійсності, що вимагається за національним правом щодо його положень, які, по-перше, вимагають від ППЕК зберігати загальні та невибіркові дані про трафік і, по-друге, дозволяють передавати ці дані компетентному фінансовому органу без попереднього дозволу суду або незалежного адміністративного органу, оскільки ці положення є несумісними з пунктом 1 статті 15 Директиви про приватність та електронні комунікації, розглянутої у світлі Хартії. Допустимість доказів, отриманих відповідно до положень національного законодавства, несумісних з правом ЄС, згідно з принципом процесуальної автономії Держав-членів, є питанням національного права, за умови дотримання, *inter alia*, принципів еквівалентності та ефективності.

Рішення СЄС від 17 листопада 2022 року, *«Спеціалізована прокуратура» (Spetsializirana prokuratura)*, C-350/21, EU:C:2022:896

Фактичні обставини справи – Справу було розпочато на підставі звернення до Суду за попереднім рішенням щодо застосування Директиви про приватність та електронні комунікації з огляду на статті 7, 8, 11 і 52 Хартії до національного законодавства, яке:

(i) зобов'язує ППЕК зберігати в загальному і невибірковому порядку всі дані про трафік і місцезнаходження кінцевих користувачів цих послуг з метою боротьби з тяжкими злочинами, встановлюючи строк зберігання в шість місяців і норми, покликані забезпечити певні гарантії;

(ii) не обмежує доступ до цих даних лише тим, що є суворо необхідним, і не надає особам право бути поінформованими (у випадку, якщо ця інформація не перешкоджає кримінальному провадженню), а також право на засіб правового захисту від незаконного доступу.

Право – СЄС підтвердив свою усталену практику щодо заборони загального й невибіркового зберігання даних про трафік і місцезнаходження з метою боротьби з тяжкими злочинами (див. *«Ла Квадратюр дю Нет» (La Quadrature du Net)* і *«Комісар Ґарда Сіхани» (Commissioner of An Garda Síochána)*, обидві справи згадані вище). Він встановив, що національне законодавство, про яке йдеться в цій справі, не відповідає праву ЄС, незважаючи на наявність гарантій і шестимісячного строку зберігання даних. Стосовно процесуальних гарантій щодо незаконного доступу СЄС постановив, що дозволу, виданого національним судом, самого по собі недостатнього для того, аби забезпечити ефективний захист суб'єктів даних від ризиків зловживань і незаконного доступу до їхніх даних, якщо, як у цій справі, національне законодавство передбачає, що такий дозвіл надається виключно на підставі запиту національних органів влади, відповідальних за проведення кримінальних розслідувань, без заслуховування зацікавлених осіб, а отже, без того, щоб суд, який має право видавати такий дозвіл, мав змогу взяти до уваги будь-які заперечення з боку цих осіб.

Рішення ЄСПЛ у справі *«Шкоберне проти Словенії» (Škoberne v. Slovenia)*, № 19920/20, 15 лютого 2024 року

Фактичні обставини справи – Дані про трафік і місцезнаходження заявника, що зберігалися ППЕК протягом чотирнадцяти місяців у рамках системного заходу, було отримано правоохоронними органами на підставі судових рішень, що ґрунтувалися на підозрі в причетності заявника до хабарництва. Справа стосується сумісності зі статтею 8 ЄКПЛ законодавства, що дозволяє зберігати телекомунікаційні дані заявника та використовувати їх органами влади в провадженні щодо нього.

Право – Оцінюючи, чи є режим зберігання даних необхідним у демократичному суспільстві, ЄСПЛ розглянув (i) рівень втручання; (ii) широту меж свободи розсуду та (iii) чи був досягнутий «справедливий баланс».

Стосовно пункту (i) ЄСПЛ провів розмежування між цією справою і згаданою вище справою *«Брейер» (Breyer)* зазначивши, що в цій справі втручання було більш серйозним, оскільки воно поширювалося на комунікаційні дані.

Стосовно пункту (ii) ЄСПЛ, посилаючись на свою попередню практику, повторив, що боротьба зі злочинністю, підтримка громадської безпеки та захист громадян є «нагальними суспільними потребами», і що національні органи влади користуються певною свободою розсуду при виборі засобів для досягнення такої законної мети. Однак межі цієї свободи розсуду, як правило, будуть вужчими, якщо, як у цій справі, право, про яке йдеться, має вирішальне значення для ефективного здійснення особою особистих або ключових прав, або якщо втручання є далекосяжним.

Стосовно пункту (iii) ЄСПЛ вважав, що гарантії, які застосовуються до загального зберігання комунікаційних даних ППЕК і доступу до них органів влади в окремих випадках, повинні бути такими ж, *mutatis mutandis*, як і гарантії, що стосуються таємного спостереження.

Він встановив, що оскаржувана нормативно-правова база не містить положень, які б обмежували обсяг і застосування цього заходу тим, що є необхідним для досягнення цілей, задля яких телекомунікаційні дані підлягали зберіганню. Також спираючись на згадане вище рішення СЄС у справі *«Діджитал Райтс Айрленд» (Digital Rights Ireland)* ЄСПЛ встановив, що національне законодавство повинно визначати сферу застосування відповідного заходу і передбачати відповідні процедури для його запровадження та/або перегляду необхідності його запровадження з метою недопущення виходу за межі того, що є необхідним. Просте обмеження строку зберігання даних чотирнадцятьма місяцями не може спростувати цей висновок. ЄСПЛ також вважав, що той факт, що режим зберігання даних був визнаний недійсним СЄС і Конституційним Судом після надання доступу до відповідних даних, не може означати, що він відповідав вимогам статті 8 на той момент.

ЄСПЛ також зазначив, що, незважаючи на те, що заявник чітко стверджував, що його комунікаційні дані було збережено з порушенням його права на приватне життя, національні суди обмежили свою оцінку виключно підставами, на яких було видано дозвіл на доступ до збережених даних – попри те, що ці підстави не оскаржувалися заявником. ЄСПЛ підкреслив, що хоча доступ до його даних супроводжувався певними гарантіями (такими як судовий нагляд), цих гарантій, незважаючи на те, що вони становили один із критеріїв, яких слід було дотримуватися, самих по собі було недостатньо для того, щоб зробити режим зберігання даних таким, що відповідає вимогам статті 8 ЄКПЛ. ЄСПЛ також посилався на згадане вище рішення СЄС у справі *«СпейсНет і Телеком Дойчланд» (SpaceNet і Telekom Deutschland)*.

Стосовно збору та використання даних заявника в національному провадженні ЄСПЛ, посилаючись на згадане вище рішення СЄС у справі *«Комісар Ґарда Сіхани та інші» (Commissioner of An Garda Síochána e.a.)*, постановив, що коли зберігання комунікаційних даних визнано таким, що порушує статтю 8, оскільки воно не відповідає вимогам «якості закону» та/або принципу пропорційності, доступ до таких даних, як і їх подальша обробка та зберігання органами влади, не може з тієї ж причини бути сумісним зі статтею 8.

Висновок – порушення статті 8 ЄКПЛ.

Рішення ЄСПЛ у справі *«П'єтрак і Бичавська-Синярська та інші проти Польщі» (Pietrzak and Bychawska-Siniarska and Others v. Poland)*, №№ 72038/17 та 25237/18, 28 травня 2024 року

Фактичні обставини справи – Справа стосувалася відповідності польського режиму таємного спостереження, що регулює зберігання та обробку комунікаційних даних, зі статтею 8[25]. Заявники скаржилися не на те, що над ними фактично велося спостереження, а на ризик впровадження щодо них таких заходів.

Заявники скаржилися на те, що система зберігання та подальшого доступу до комунікаційних даних (даних про трафік і місцезнаходження, а також даних, пов'язаних з пошуковими запитами в Інтернеті) не відповідала вимогам статті 8 ЄКПЛ.

Право – Посилаючись на згадану вище справу *«Екімджієв» (Ekimdzhiev)* ЄСПЛ постановив, що зберігання та подальший доступ до комунікаційних даних є окремими втручаннями у статтю 8, і що загальне зберігання комунікаційних даних ППЕК і доступ до них органів влади в окремих випадках має супроводжуватися, *mutatis mutandis*, тими ж гарантіями, що й таємне спостереження.

ЄСПЛ провів розмежування між цією справою і згаданою вище справою *«Екімджієв» (Ekimdzhiev)*, зазначивши, що оскаржуваний режим дозволяв національним органам влади мати постійний, прямий і необмежений доступ до комунікаційних даних без будь-яких втручань з боку ППЕК, яким навіть не було про це відомо. У цій справі втручання було визнано дуже серйозним. Крім того, попри те, що згадана вище справа *«Екімджієв» (Ekimdzhiev)* стосувалася режиму зберігання комунікаційних даних, подібного тому, що розглядається в цій справі, ЄСПЛ не вирішував, чи відповідає такий режим вимогам статті 8, а зосередився на гарантіях, пов'язаних із доступом до зібраних даних та їхнім зберіганням.

Спираючись також на практику СЄС (згадані вище рішення у справах *«Діджитал Райтс Айрленд та інші» (Digital Rights Ireland e.a)*, *«Прайвесі Інтернешенал» (Privacy International)*, *«Комісар Ґарда Сіхани та інші» (Commissioner of An Garda Síochána e.a.)*, а також рішення у справі *«Ла Квадратюр дю Нет та інші» (La Quadrature du Net e.a.)*[26]), ЄСПЛ встановив, що оскаржуваний режим передбачав загальне та невибіркове зберігання комунікаційних даних всіх користувачів послуг комунікацій, що впливало на осіб, які не перебували, навіть опосередковано, у ситуації, яка могла б призвести до порушення кримінального провадження. Крім того, цей режим надавав поліції та спецслужбам доступ з будь-якою метою, що була б пов'язана з виконанням їхніх посадових обов'язків. За таких обставин гарантій проти можливих зловживань, включно із судовим переглядом *ex post facto*, було недостатньо для приведення оскаржуваного режиму у відповідність до вимог статті 8.

Висновок – порушення статті 8 ЄКПЛ щодо системи зберігання та доступу до комунікаційних даних.

[25] Заявники також скаржилися за цією ж статтею на оперативний контроль у контексті діяльності поліції та заходи таємного спостереження, вжиті в контексті боротьби з тероризмом, за допомогою засобів, що включають підслуховування, запис змісту телефонних розмов або кореспонденції, що здійснювалися за допомогою телекомунікаційних та цифрових мереж зв'язку. Цю частину рішення не буде проаналізовано, оскільки оскаржувана система, що дозволяє вживати цілеспрямовані заходи спостереження, виходить за рамки цієї інформаційної довідки.

[26] Рішення СЄС від 06 жовтня 2020 року, *«Ла Квадратюр дю Нет та інші» (La Quadrature du Net and Others)*, C-511/18, C-512/18 та C-520/18, ЄС:C:2020:791.

B. 3. Зміст комунікацій

Рішення ЄСПЛ у справі *«Подчасов проти Росії» (Podchasov v. Russia)*, № 33696/19, 13 лютого 2024 року

Фактичні обставини справи – Заявник, користувач соціальної мережі «Телеграм» (Telegram), скаржився на відповідність статті 8 ЄКПЛ законодавчої вимоги до «організаторів інтернет-комунікацій» (Internet communication organisers – «ICO») зберігати всі комунікаційні дані протягом одного року, а також зміст усіх комунікацій протягом шести місяців, і надавати ці дані правоохоронним органам або службам безпеки у передбачених законом випадках разом з інформацією, необхідною для розшифровки електронних повідомлень, якщо вони були зашифровані.

Право – ЄСПЛ, посилаючись на свою попередню практику (*«Брейер» (Breyer)*, *«Екімджієв» (Ekimdzhiev)*, і *«Роман Захаров» (Roman Zakharov)*, всі згадані вище), постановив, що безперервне зберігання інтернет-комунікацій заявника та пов'язаних з ними комунікаційних даних у соціальній мережі «Телеграм» і потенційний доступ органів влади до цих даних становило втручання у права заявника за статтею 8 Конвенції. Стосовно зобов'язання, покладеного на «Телеграм», надати органам влади ключі шифрування для того, щоб вони могли розшифровувати наскрізні зашифровані повідомлення, ЄСПЛ підтримав аргумент заявника про те, що технічно неможливо надати органам влади ключі шифрування, пов'язані з конкретними користувачами цієї соціальної мережі, без впливу на всіх користувачів їхніх послуг. Відповідно, ЄСПЛ визнав, що на заявника також вплинуло це законодавче положення.

ЄСПЛ постановив, що, попри те, що цю справу слід розглядати насамперед з точки зору зберігання персональних даних заявника (подібно до справ *«Брейер» (Breyer)* і *«Екімджієв» (Ekimdzhiev)*, згаданих вище), її також слід розглядати, де це доречно, з врахуванням його практики щодо таємного спостереження (*«Роман Захаров» (Roman Zakharov)*, *«Біг Бразер Вотч» (Big Brother Watch)*, згадані вище).

Стосовно зберігання інтернет-комунікацій і комунікаційних даних, ЄСПЛ підкреслив широкомасштабність зберігання даних, що передбачалася оскаржуваним законодавством, яке охоплює зміст усіх інтернет-комунікацій та пов'язаних із ними комунікацій стосовно всіх користувачів інтернет-комунікацій, навіть за відсутності обґрунтованої підозри у причетності до злочинної діяльності або діяльності, що загрожує національній безпеці, або будь-яких інших підстав вважати, що збереження даних може сприяти боротьбі з тяжкими злочинами або захисту національної безпеки, без будь-якого обмеження сфери застосування цього заходу з точки зору територіального або часового застосування чи категорій осіб, чиї персональні дані можуть бути збережені. Він встановив, що втручання було надзвичайно широким і серйозним.

Стосовно потенційного доступу до збережених даних з метою цілеспрямованого таємного спостереження ЄСПЛ встановив, що національне законодавство не зобов'язує правоохоронні органи пред'являти ППЕК дозвіл, наданий судом, перед отриманням доступу до комунікацій особи. Крім того, інтернет-компанії повинні були встановити обладнання, яке надавало службам безпеки прямий доступ до збережених даних і забезпечувало їм технічну можливість обійти процедуру отримання такого дозволу й отримати доступ до збережених інтернет-комунікацій і комунікаційних даних без попереднього дозволу суду. ЄСПЛ також повторив свої висновки щодо відсутності належних і достатніх гарантій проти зловживань у згаданій вище справі *«Роман Захаров» (Roman Zakharov)*, де той самий правовий режим розглядався в контексті перехоплення мобільних телефонних комунікацій.

Наприкінці стосовно законодавчої вимоги розшифровувати комунікації ЄСПЛ визнав її непропорційною переслідуваним законним цілям, оскільки, незважаючи на те, що він

погодився, що шифрування може використовуватися злочинцями, оспорюване положення ризикує послабити механізм шифрування для всіх користувачів.

Висновок – порушення статті 8 ЄКПЛ.