УДК 342.721
DOI https://doi.org/10.32782/2524-0374/2024-3/119

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ЩОДО ЕЛЕКТРОННОЇ КОМУНІКАЦІЇ У ПРАКТИЦІ СУДУ ЄС

PROTECTION OF PERSONAL DATA CONCERNING ELECTRONIC COMMUNICATION IN PRACTICE OF THE COURT OF JUSTICE OF THE EUROPEAN UNION

Чванкін С.А., д.ю.н., доцент,
голова
Київський районний суд м. Одеси

Розвиток цифрових технологій у сучасному світі призвів до збільшення втручання в приватне життя людини та кількості порушень прав людини, пов'язаних із приватним життям. Для України актуальність захисту персональних даних в розрізі застосування підходів, що використовуються Судом ЄС, є актуальною з огляду на євроінтеграційні процеси: стаття 15 Угоди про асоціацію з ЄС передбачає співробітництво сторін з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів, зокрема відповідних документів Ради Європи.

У статті проаналізовано ключові рішення Суду ЄС у сфері захисту персональних даних у справах «Digital Rights Ireland and Others», «Tele2 Sverige and Watson and Others», «Privacy International» і «La Quadrature du Net and Others». Враховуючи останню прецедентну практику Суду ЄС у справі «Commissioner of An Garda Síochána and Others» зроблено висновок, що роль Суду ЄС у формуванні єдиного європейського простору захисту даних є ключовою.

Результатом діяльності Суду ЄС є як прямий вплив на регуляцію у даній сфері, що проявляється у скасуванні Судом Директиви 95/46/ЄС Європейського Парламенту і Ради "Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних", так і опосередкований, який проявляється в розробці критеріїв оцінки виправданості втручання у право на приватність, які держави-учасниці мають впровадити у власне національне законодавство та правозастосовну практику.

Вказується, що превентивне збереження даних і доступ до них може бути виправданий лише щодо тяжких злочинів, якщо отримання доступу містить достатні гарантії (необхідність, об'єктивний зв'язок, чіткі та точні правила). Для доступу правоохоронних органів до даних застосовуються додаткові процедурні гарантії, а саме обов'язок сповіщення та попередній розгляд судом або незалежним адміністративним органом.

Натомість для цілей забезпечення національної безпеки Судом допускаються більш жорсткі заходи втручання, які також мають відповідати критеріям необхідності, відповідності, пропорційності та об'єктивному критерію). Було введено кілька винятків, коли загроза національній безпеці є серйозною, справжньою, наявною або передбачуваною.

Ключові слова: персональні дані, електронні комунікації, Суд ЄС.

Development of digital technologies in the modern world has led to growing invasion of privacy and cases of violation of privacy-related human rights. In Ukraine protection of personal data as far as it concerns application of approaches used by the EU Court of Justice is a pressing issue in view of European integration processes: Art. 15 of the European Union - Ukraine Association Agreement stipulates cooperation of the Parties in order to ensure an adequate level of protection of personal data in accordance with the highest European and international standards, including the relevant Council of Europe instruments.

The article contains an analysis of key judgments of the EU Court of Justice in the field of protection of personal data in the cases of Digital Rights Ireland and Others, Tele2 Sverige and Watson and Others, Privacy International, and La Quadrature du Net and Others. Taking into account the latest case law of the EU Court of Justice in the case of Commissioner of An Garda Síochána and Others, it is concluded that the EU Court of Justice plays a key role in creation of the common European space for data protection.

Results of activities of the EU Court of Justice include a direct impact on governance in this sphere, which is demonstrated by repeal of the Directive 95/46/EU of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data by the Court, as well as an indirect influence manifesting itself in development of criteria for assessment of propriety of invasion of privacy, which the member states must implement into their national law and law enforcement practice.

It is noted that preventive storage of data and access thereto may be justified only with regard to grave offences, provided that accessibility includes sufficient guarantees (necessity, objective connection, clear and exact rules). For the purpose of access to data by law-enforcement agencies additional procedural guarantees are applied, in particular, obligation to notify and preliminary proceedings in court or independent administrative authority.

At the same time for the purposes of national security the Court of Justice allows for more severe interventions, which should also meet criteria for relevance, compliance, proportionality and objectivity. A number of exceptions were introduced, when threat to national security is serious, real, present or implied.

Key words: personal data, electronic communications, EU Court of Justice.

Постановка проблеми. Розвиток цифрових технологій у сучасному світі призвів до збільшення втручання в приватне життя людини та кількості порушень прав людини, пов'язаних із приватним життям. Для України актуальність захисту персональних даних в розрізі застосування підходів, що використовуються Судом ЄС, є актуальною з огляду на євроінтеграційні процеси: стаття 15 Угоди про асоціацію з ЄС передбачає співробітництво сторін з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів, зокрема відповідних документів Ради Європи [1].

Аналіз останніх досліджень і публікацій. У своїй статті Б. Якименко проаналізував розвиток інституту захисту персональних даних у світі з метою визначення шляхів адаптації національного законодавства України до чинних стандартів захисту персональних даних ЄС. Згідно з результатами дослідження, інститут захисту персональних даних пройшов значний шлях розвитку від індивідуальних понять і концепцій до структурованого набору законодавчо встановлених стандартів та інструментів на рівні ЄС [2]. Оглядам практики суду ЄС присвячені роботи Д. Місюнайте-Камараускене (Dalia Misiūnaitė-Kamarauskienė) [3], Г. Рудольф та П. Ковач (Grega Rudolf, Polonca Kovač) вказують на відсутність процесуальних положень щодо узгодженого застосування Загального регламенту захисту даних (GDPR), який діє з 2018 року, у кількох аспектах, включаючи визначення сторін процедури та їхні права на захист, зокрема доступ до файлу, права бути почутим і права на оскарження, а також доступ до правового захисту та ін. [4].

Д. Дуіч та Т. Петрашевич (Dunja Duic, Tunjica Petrašević) роблять висновок про нагальну необхідність захисту приватного життя осіб, зокрема їхніх особистих

даних, що неможливо зробити без надійної законодавчої бази. У захисті даних ключова роль відводиться національним судам і судам ЄС, які повинні збалансувати право фізичних осіб на захист персональних даних і недоторканність приватного життя з іншими законними інтересами, такими як національна безпека. Однак дослідники констатують, що позитивних законодавчих зрушень на рівні ЄС ще не було реалізовано, тоді як стандарти переважно відображені в практиці та прецедентному праві Суду ЄС [5, с. 112].

Метою статті є визначення роді Суду ЄС на формування критеріїв допустимого втручання держави у право на особи на приватність у сфері електронних комунікацій.

Виклад основного матеріалу. У 1995 році була прийнята Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних», яка заклала основи захисту персональних даних в ЄС [6]. Визначаючи ключові поняття та принципи, пов'язані з обробкою персональних даних, Директива встановлювала у ст. 17 стандарт безпеки даних, за яким контролер даних зобов'язаний здійснювати відповідні технічні й організаційні заходи для захисту персональних даних від випадкового або незаконного знищення чи випадкової втрати, зміни, несанкціонованого розкриття чи доступу, зокрема, якщо обробка включає передачу даних через мережу, і від усіх інших незаконних форм обробки. Директива визначала суб'єктів відносин з обробки персональних даних, їх права та обов'язки. Однак, як зазначають К. Врублевська-Місюна та В. Тичина, вже за декілька років після прийняття Директива 95/46/ЄС «не могла справлятися з новими викликами, які з'явились разом з новою технологічною індустрією, яка динамічно розвивалась. Персональні дані суб'єктів персональних даних використовувались не тільки для потреб бізнесу. Все більше і більше процесів з обробки даних та невизначеностей виникало у сфері соціальних медіа, що і спричинило неминуче створення нового підходу до захисту персональних даних» [7]. І хоча Директива 95/46/ЄС мала на меті узгодити захист фундаментальних прав щодо персональних даних, а її цілі та принципи і сьогодні залишаються актуальними, це не запобігло фрагментації у здійсненні захисту даних у Європейському Союзі, правовій невизначеності, що було перешкодою для подальшого створення єдиного цифрового ринку ЄС.

Тривалий час корпус законодавства ЄС у сфері електронних комунікаційних складали п'ять основних директив Європейського Парламенту і Ради:

1) Директива 2012/19/ЄС від 7 березня 2002 р. про доступ до електронних комунікаційних мереж, пов'язаних засобів та їх взаємоз'єднання (Директива про доступ);

2) Директива 2002/20/ЄС від 7 березня 2002 р. про авторизацію електронних комунікаційних мереж та послуг (Директива про авторизацію);

3) Директива 2002/21/ЄС від 7 березня 2002 р. про спільні правові рамки для електронних комунікаційних мереж та послуг (Рамкова директива);

4) Директива 2002/22/ЄС від 7 березня 2002 р. про універсальні послуги та права користувачів стосовно електронних мереж зв'язку і послуг (Директива про універсальні послуги);

5) Директива 2002/58/ЄС від 12 липня 2002 р. про обробку персональних даних та захист таємниці сектора електронних комунікацій (Директива про приватність та електронні комунікації).

Перші чотири Директиви з вищеназваних, хоча і бути скасовані з 20 грудня 2020 р. Директивою Європейського Парламенту і Ради (ЄС) 2018/1972 від 11 грудня 2018 р. про запровадження Європейського кодексу електронних комунікацій, все ж не втратили своєї значимості, адже Європейський кодекс електронних комунікацій містить кореляційні таблиці, відповідно до яких посилання на скасовані директиви необхідно тлумачити як покликання на цю Директиву.

Необхідність уніфікації захисту персональних даних обумовило розробку та прийняття Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 р. про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) [8]. Мета Загального регламенту насамперед відображається в тому, що його прийняття забезпечує однакове функціонування наглядових органів на національному рівні, посилюються наглядові повноваження та можливість органів влади накладати штрафи за порушення у сфері захисту персональних даних. Важливість цієї реформи випливає саме з основної мети прийняття Загального регламенту, яка полягає у визначенні кордонів і максимальному захисті даних з наголосом на обробці персональних даних і захисті приватності громадян на території Європейського Союзу, що підвищує загальний правовий захист та безпеку в сучасному інформаційному суспільстві [9, с. 199-200].

Зв'язок між Загальним регламентом про захист даних та Директивою про приватність та електронні комунікації 2002/58/ЄС визначено у ст. 95 Загального регламенту, якою унеможливлено накладення Загальним регламентом додаткових обов'язків з тією ж метою на контролерів, які підлягають конкретним зобов'язанням згідно з Директивою про приватність та електронні комунікації. Як уточнює ст. 173 Загального регламенту, це правило охоплює як обов'язки контролерів, так і права фізичних осіб, які підпадають під дію Директиви 2002/58/ЄС як lex specialis; однак Загальний регламент застосовується до всіх інших питань як lex generalis. У такий спосіб ст. 95 Загального регламенту забезпечує юридичну визначеність щодо положень, що застосовуються до обробки персональних даних у конкретному контексті загальнодоступних електронних комунікаційних послуг у публічних комунікаційних мережах [10, с. 1151].

Останніми роками Суд ЄС у кількох справах виніс рішення щодо збереження персональних даних та доступу до них у сфері електронних комунікацій. Зазначена вище домінуюча роль Суду ЄС проявилася у рішенні від 8 квітня 2014 р. по справі *«Digital Rights Ireland and Others»* (C-293/12 та C-594/12), яким Суд оголосив Директиву 2006/24/ЄС Європейського Парламенту та Ради від 15 березня 2006 р. про збереження даних, створених або оброблених при наданні загальнодоступних послуг електронних повідомлень або громадських мереж зв'язку та про внесення змін до Директиви 2002/58/ЄС (Директива про збереження даних), недійсною на тій підставі, що втручання в право на повагу до приватного життя та на захист персональних даних, визнані Хартією основоположних прав Європейського Союзу, яке є наслідком загального зобов'язання щодо збереження трафіку та даних про місцезнаходження, викладених цією директивою, не обмежувалися тим, що було суворо необхідним. На думку Суду «той факт, що дані зберігаються і згодом можуть використовуватися без повідомлення про це абонента або зареєстрованого користувача, ймовірно, породжують у зацікавлених осіб відчуття того, що їхнє особисте життя є предметом постійного спостереження […] Вимагаючи здійснення збору та зберігання цих даних, а також надаючи відповідним органам влади доступ до них, Директива вкрай серйозно втручається у сферу фундаментальних прав людини та порушує право на повагу особистого життя та захист персональних даних».

По-перше, Скасована Судом Директива 2006/24/ЄС в узагальненому вигляді охоплювала всіх осіб, усі засоби електронного зв'язку та всі дані трафіку без будь-яких диференціацій, обмежень чи винятків у світлі мети боротьби з злочинністю.

По-друге, Директива 2006/24/ЄС не встановлювала жодного об'єктивного критерію, який би гарантував, що компетентні національні органи мають доступ до даних і можуть використовувати їх лише з метою запобігання, виявлення або кримінального переслідування щодо правопорушень, які, з огляду на масштаби та серйозність втручання в основні права особи, можуть вважатися достатньо серйозними, щоб виправдати таке втручання. Навпаки, Директива просто посилалася в узагальненому вигляді на «серйозний злочин», як це визначалося кожною державою-членом у її національному законодавстві. Крім того, Директива не встановлювала процедурних умов, за яких компетентні національні органи могли б отримати доступ до даних і згодом використовувати їх. Зокрема, доступ до даних не ставився в залежність від попереднього розгляду судом або незалежним адміністративним органом.

По-третє, що стосується періоду зберігання даних, Директива встановлювала мінімальний період у шість місяців, не роблячи жодного розрізнення між категоріями зібраних даних, значимістю таких даних для досягнення мети, яка переслідується державою. Максимальний період зберігання було визначено у 24 місяців, але Директива не передбачала об'єктивних критеріїв, на основі яких повинен був визначатися конкретний період зберігання. Суд також зауважив, що Директива 2006/24/ЄС не передбачає достатніх гарантій для забезпечення ефективного захисту даних від ризику зловживання та від будь-якого незаконного доступу та використання даних: Директива дозволяла постачальникам послуг знижувати стандарт захисту даних, враховуючи економічні міркування (наприклад, витрати на впровадження заходів безпеки), та не зобов'язувала до незворотного знищення даних по закінченню терміну їх зберігання [11].

Після даного, доволі радикального для європейського правового простору рішення, національні суди, як вказують Л. Марін та С. Тас (Luisa Marin, Sarah Tas), кілька разів вимагали від Суду ЄС повернутися до своєї попередньої доктрини, що в подальшому змусило Суд у низці подальших справ уточнювати свою точку зору як щодо різних видів даних, так і щодо цілей їх отримання та зберігання [12, с. 5].

Рішенням від 21 грудня 2016 р. у справі *«Tele2 Sverige and Watson and Others»* (С-203/15 і С-698/15) Суд постановив, що стаття 15(1) Директиви 2002/58/ЄС виключає національне законодавство, що передбачає загальне та невибіркове збереження трафіку та даних про місцезнаходження з метою боротьби зі злочинністю. Така позиція була підтримана рішенням Великої палати від 6 жовтня 2020 р., яким Суд підтвердив свою попередню прецедентну практику щодо непропорційного характеру загального та невибіркового збереження трафіку: Суд уточнив, зокрема, обсяг повноважень, які Директива про приватність та електронні комунікації надає державами-членами щодо збереження цих даних з метою захисту національної безпеки та боротьби зі злочинністю. Положення Директиви 2002/58/ЄС слід тлумачити як такі, що виключають національне законодавство щодо безпеки трафіку та даних про місцезнаходження та, зокрема, доступу компетентних національних органів до збережених даних, якщо мета, переслідувана таким доступом, у контексті боротьби зі злочинністю, не обмежується виключно боротьбою з тяжкою злочинністю, якщо доступ не підлягає попередньому перегляду судом або незалежним адміністративним органом, і якщо немає вимог щодо зберігання відповідних даних у межах Європейського Союзу [13].

У рішенні від 2 жовтня 2018 р. у справі *«Ministerio Fiscal»* (С-207/16), яка стосувалася доступу органів державної влади до даних, Суд витлумачив статтю 15(1) Директиви 2002/58/ЄС, вказавши, що доступ державних органів до даних (таких як прізвища, імена та, якщо необхідно, адреси власників) з метою ідентифікації власників SIM-карт, активованих за допомогою викраденого мобільного телефону, тягне за собою втручання в їхні основні права, закріплені в Хартії основоположних прав ЄС. Мета доступу у даній справі була недостатньо серйозною, адже не спричинена розслідуванням тяжкого злочину [14]. Суд ЄС продовжив утверджувати критерій, за яким відповідно до принципу пропорційності серйозне втручання в права особи може бути виправдане у сферах запобігання, розслідування, виявлення та переслідування кримінальних правопорушень лише метою боротьби зі злочинністю, яка має бути визначена як «серйозна». Навпаки, коли втручання, яке тягне за собою такий доступ, не є серйозним, розкриття персональних даних можна виправдати метою запобігання, розслідування, виявлення та судового переслідування «кримінальних злочинів» загалом. Тому, перш за все, слід визначити, чи було втручання в основні права, закріплені в статтях 7 і 8 Хартії, серйозним, а якщо так – співставляти здійснене втручання із тяжкістю злочину, що розслідується.

Рішеннями від 6 жовтня 2020 р. у справі *«Privacy International»* (С-623/17), і *«La Quadrature du Net and Others»* (С-511/18, С-512/18 та С-520/18) [15, 16] Суд ЄС, посилаючись на попередню практику щодо непропорційного характеру загального та невибіркового збереження трафіку та даних про місцезнаходження, уточнив обсяг повноважень, які Директива про приватність та електронні комунікації надає державам-членам щодо збереження цих даних з метою захисту національної безпеки та боротьби зі злочинністю. Невибіркове збирання даних буде правомірним тільки у випадку, коли відповідна держава-член стикається з серйозною загрозою національній безпеці, тобто доведено, що загроза є справжньою (існуючою або передбачуваною), якщо рішення про невибіркове збирання даних підлягає ефективному перегляду або судом, або незалежним адміністративним органом, а строк збирання даних обмежується визначеним періодом, який може бути продовжений, якщо загроза зберігається. Держава повинна забезпечити цільове збереження даних на основі об'єктивних і недискримінаційних факторів, а також надати особам ефективні гарантії проти ризиків зловживання. Оскільки автоматизований аналіз даних про трафік і місцезнаходження обов'язково передбачає певну похибку, будь-який позитивний результат, отриманий після автоматизованої обробки, повинен підлягати індивідуальній повторній перевірці неавтоматизованими засобами, перш ніж буде запроваджено індивідуальний захід, який негативно впливатиме на зацікавлених осіб.

В справі *«Commissioner of An Garda Síochána and Others»* (С-140/20) прохання про винесення попереднього рішення було подано Верховним судом Ірландії у контексті цивільного провадження, порушеного особою, засудженою до довічного ув'язнення за вбивство, скоєне в Ірландії. Ця особа оскаржила сумісність із законодавством ЄС певних положень національного законодавства щодо збереження даних електронних комунікацій [17]. Відповідно до національного закону дані про трафік і місцезнаходження, що стосуються телефонних дзвінків обвинуваченої особи, зберігалися постачальниками електронних комунікаційних послуг і були надані правоохоронним органам. Сумніви національного суду, який звернувся до Суду ЄС за тлумаченням положень ст. 15(1) Директиви 2002/58/ЄС, стосувалися, зокрема, сумісності з Директивою про приватність та електронні комунікації у світлі Хартії загального та невибіркового зберігання цих даних у зв'язку з боротьбою з серйозними злочинами. У своєму рішенні Суд ЄС у складі Великої Палати, підтвердив, що загальне та невибіркове збереження трафіку та даних про місцезнаходження, пов'язаних з електронними комунікаціями, заборонені з метою боротьби з серйозними злочинами та запобігання серйозним загрозам громадській безпеці. Суд дійшов висновку, по-перше, що Директива про приватність та електронні комунікації в світлі Хартії виключає законодавчі положення, які у якості

превентивних заходів передбачають загальне та невибіркове збереження даних про трафік і місцезнаходження з метою боротьби з серйозними злочинами та запобігання серйозним загрозам громадській безпеці. Беручи до уваги переконливий вплив на здійснення основних прав, який може бути результатом збереження цих даних і серйозність втручання, спричиненого таким збереженням, необхідно, щоб це збереження бути винятком, а не правилом у системі, встановленій цією Директивою, таким чином, ці дані не повинні зберігатися систематично та постійно.

Злочин, навіть особливо тяжкий злочин, не можна розглядати так само, як загрозу національній безпеці, оскільки їхнє ототожнення, ймовірно, створить проміжну категорію між національною безпекою та громадською безпекою з метою застосування до них однакових вимог збереження даних. Однак Директива про приватність та електронні комунікації, прочитана у світлі Хартії, не перешкоджає законодавчим заходам, які передбачають цільове збереження даних з метою захисту національної безпеки, боротьби з серйозними злочинами та запобігання серйозним загрозам громадській безпеці.

Отримання даних у місцях, які регулярно приймають дуже велику кількість відвідувачів, або стратегічних місцях (аеропорти, вокзали, морські порти тощо), може дозволити компетентним органам отримати інформацію щодо присутності в цих місцях або географічному районі осіб і робити висновки щодо присутності та діяльності таких осіб в цих місцях або географічних районах з метою боротьби з тяжкою злочинністю. У будь-якому випадку труднощі у наданні детального визначення обставин і умов, за яких може здійснюватися збирання даних, не є причиною для держав-членів перетворювати виняток на правило, законодавчо закріпивши невибіркове збереження трафіку та даних про місцезнаходження.

Суд окремо наголосив, що ані Директива 2002/58/ЄС, ані будь-який інший акт законодавства ЄС не перешкоджає національному законодавству, метою якого є боротьба з серйозними злочинами, перевірку офіційних документів, що встановлюють особу покупця, і реєстрації продавцем цієї інформації (наприклад, під час придбання засобів електронного зв'язку, передплаченої SIM-карти тощо), при цьому продавець зобов'язаний, у разі виникнення такої ситуації, надати доступ до цієї інформацію компетентним національним органам.

Це ж стосується законодавчих заходів, які дозволяють вимагати від постачальників електронних комунікаційних послуг на підставі рішення компетентного органу, яке підлягає ефективному судовому перегляду, щоб протягом певного періоду часу оператори збирали та зберігали трафік і дані про місцезнаходження, якими вони володіють з метою боротьби з тяжкою злочинністю та запобіганню серйозним загрозам громадській безпеці. Лише дії, спрямовані на боротьбу з серйозними злочинами та, тим більше, на захист національної безпеки є такими, що виправдовують таке зберігання, за умови, що заходи та доступ до збережених даних відповідають межам того, що є суворо необхідним.

Суд нагадав, що такий захід зберігання може бути поширений на дані про трафік і місцезнаходження, що стосуються інших осіб, ніж ті, хто підозрюється в плануванні або вчиненні серйозного кримінального правопорушення або дій, що негативно впливають на національну безпеку, за умови, що ці дані можуть на підставі об'єктивних і недискримінаційних факторів, пролити світло на таке правопорушення або дії, що негативно впливають на національну безпеку, наприклад, дані про потерпілого, його соціальні чи професійні зв'язки. Проте далі Суд зазначає, що всі вищезазначені законодавчі заходи повинні забезпечувати, за допомогою чітких і точних правил, що збереження даних, підлягає відповідності застосовним матеріальним і процесуальним умовам і що відповідні особи мають ефективні гарантії проти можливих зловживань. Різні заходи для збереження трафіку та даних про місцезнаходження можуть, за вибором національного законодавчого органу та в межах того, що є суворо необхідним, застосовуватись одночасно.

Що не менш важливо, Суд ЄС вказав на неможливість доступу до даних, зібраних для цілей усунення серйозної загрози національній безпеці, у справах щодо боротьби із серйозними злочинами, адже це суперечитиме ієрархії цілей суспільного інтересу, що може виправдати вжиті заходи втручання у права особи відповідно до Директиви про приватність та електронні комунікації. На думку Суду, це означало б виправдання доступу для мети меншої важливості, ніж та, яка виправдовувала загальне та невибіркове утримання даних, а саме – збереження національної безпеки, що ризикувало б позбавити будь-якої ефективності заборону на загальне та невибіркове утримання з метою боротьби з тяжкими злочинами.

Важливим був висновок Суду ЄС і щодо суб'єкта, який може бути відповідальним на надання доступу до даних: Директива про приватність та електронні комунікації, прочитана у світлі Хартії, виключає національне законодавство, згідно з яким запит на доступ до даних, що зберігаються постачальниками електронних комунікаційних послуг може бути задоволено офіцером поліції підрозділу, створеного у поліцейській службі, який користується ступенем автономії у виконанні своїх обов'язків, і чиї рішення згодом можуть бути предметом судового розгляду. Суд ЄС наголосив, що такий поліцейський не відповідає вимогам незалежності та неупередженості, яким повинен відповідати адміністративний орган, який здійснює попередній розгляд запитів на доступ до даних, оскільки він не має статусу третьої сторони по відношенню до цих органів. Хоча рішення цієї посадової особи може підлягати подальшому судовому перегляду, цей перегляд не може замінити первісного розгляду запиту на доступ, який так само мав би бути незалежним.

Як вказується, бажання Європейського Суду взяти на себе роль захисника фундаментальних цифрових прав громадян спонукало його до розробки сміливої сукупності прецедентного права, спрямованого на обмеження втручання держав-членів, а також третіх країн, у права на конфіденційність і захист персональних даних, закріплених в Статті 7 і 8 Хартії основних прав [18].

Висновки. Роль Суду ЄС у формуванні єдиного європейського простору захисту даних є ключовою: Суд використовує наявні важелі регуляції європейського законодавства: від скасування Директиви 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних», яка заклала основи захисту персональних даних в ЄС, до розробки критеріїв збирання та збереження даних у боротьбі зі злочинністю та забезпеченні національної безпеки. Коли мова йде про боротьбу зі злочинністю, Суд неодноразово заявляв, що загальне та невибіркове збереження даних не відповідає законодавству ЄС. Превентивне цільове збереження даних і доступ до них може бути виправданий лише щодо тяжких злочинів, якщо отримання доступу містить достатні гарантії (необхідність, об'єктивний зв'язок, чіткі та точні правила). Для доступу правоохоронних органів до даних застосовуються додаткові процедурні гарантії, а саме обов'язок сповіщення та попередній розгляд судом або незалежним адміністративним органом.

Для цілей національної безпеки, Суд із посиланням на Директиву 2002/58/ЄС знижує стандарт, допустивши більш жорсткі заходи втручання, але все ще застосовуючи суворий тест перевірки. Було введено кілька винятків, коли загроза національній безпеці є серйозною, справжньою, наявною або передбачуваною.

Крім того, прецедентне право Суду опосередковано впливає і на законодавчу базу країн-учасниць ЄС та практику застосування чинного законодавства з огляду на критерії допустимого втручання, що використовуються Судом ЄС.

ЛІТЕРАТУРА

1. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони : Угода; Україна від 27.06.2014 // База даних «*Законодавство України*» / *Верховна Рада України*. URL: https://zakon.rada.gov.ua/go/984_011.

2. Yakymenko B. Formation of the institute of personal data protection and experience of its implementation in the countries of the EU. *Scientific Journal of the National Academy of Internal Affairs.* 2023. 28(4), 68-79. https://doi.org/10.56215/naia-herald/4.2023.68.

3. Dalia Misiūnaitė-Kamarauskienė. Recent Case-law of the Court of Justice of the European Union Regarding the Fundamental Rights to Respect for Private and Family Life and to Protection of Personal Data. *Jurisprudence. 2014.* 21(4):1233. DOI: 10.13165/JUR-14-21-4-15.

4. Grega Rudolf, Polonca Kovač. Procedural Challenges of Cross-border Cooperation and Consistency in Personal Data Protection in the EU. NISPAcee Journal of Public Administration and Policy. 2023. 16(2). P. 143-170. DOI: 10.2478/nispa-2023-0017.

5. Dunja Duic, Tunjica Petrašević. Data protection and cybersecurity : case-law of two european courts. *Conference: International Scientific Conference on International, EU and Comparative Law Issues "Law in the Age of Modern Technologies".* 2023. P. 94-118. DOI: 10.25234/eclic/28259.

6. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individual swith regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Communities.* 1995. NoL281/1. p. 0031 – 0050. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:1995:281:FULL&from=BG.

7. Врублевська-Місюна К., Тичина В. Міжнародно-правові стандарти захисту інформації про особу. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2022. № 74. Том 2. С. 149-154. DOI: https://doi.org/10.24144/2307-3322.2022.74.58.

8. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 4 May 2016. P. 1–88. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679/

9. Boban M. Digital single market and EU data protection reform with regard to the processing of personal data as the challenge of the modern world. *16th International Scientific Conference on Economic and Social Development "The Legal Challenges of Modern World": Book of Proceedings*/ Primorac, Ž.; Bussoli, C.; Recke, N. (ur.). Varaždin; Split; Koprivnica: Development and Entrepreneurship Agency; Faculty of Law; University North, Koprivnica, 2016, P. 191– 202. URL: https://www.bib.irb.hr:8443/904724.

10. Vagelis Papakonstantinou, Paul De Hert. Article 95 GDPR (Relationship with Directive 2002/58/EC): Commentary. General Data Protection Regulation: Article-by-Article Commentary. Baden-Baden : Nomos Verlagsgesellschaft, 2023. P. 1150-1155.

11. Judgment in Joined Cases C-293/12 and C-594/12 «Digital Rights Ireland and Seitlinger and Others» (ECLI:EU:C:2014:238). URL: https://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=558433.

12. Marin L., Tas S. Once upon a time... Digital Rights Ireland: The never-ending saga of data retention in the EU. European University Institute, 2023. 29 p. URL: https://cadmus.eui.eu/handle/1814/76276 .

13. Judgment of the Court (Grand Chamber) of 21 December 2016. «Tele2 Sverige AB v Postoch telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others» (C-203/15, ECLI:EU:C:2016:970). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62015CJ0203.

14. Judgment of the Court (Grand Chamber) of 2 October 2018 «Ministerio Fiscal» (C-207/16, ECLI:EU:C:2018:788). URL: https://curia.europa.eu/juris/ document/document.jsf?text=&docid=206332&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=563441.

15. Judgment of the Court (Grand Chamber) of 6 October 2020. «Privacy International» (C-623/17, EU:C:2020:790). URL: https://curia.europa.eu/juris/document/document.jsf?text=&docid=232083&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=1217012.

16. Judgment of the Court (Grand Chamber) of 6 October 2020. «La Quadrature du Net» (In Joined Cases C-511/18, C-512/18 and C-520/18, EU:C:2020:791). URL: https://curia.europa.eu/juris/document/document.jsf? text=&docid=232084&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=1216457.

17. Judgment of the Court (Grand Chamber) of 5 April 2022. «Commissioner of An Garda Síochána and Others» (C-140/20, EU:C:2022:258). URL: http://curia.europa.eu/juris/documents.jsf?language=EN&critereEcli= ECLI:EU:C:2022:258.

18. Teyssedre Julie. Strictly regulated retention and access regimes for metadata: Commissioner of An Garda Síochána. *Common Market Law Review*. 2023. 60. Issue 2. P. 569-588. DOI: https://doi.org/10.54648/cola2023032.