УДК 341.242.2:004.738.5
DOI

ПРАВОВЕ РЕГУЛЮВАННЯ В ЄС ДОСТУПУ ДО ІНФОРМАЦІЇ В ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ МЕРЕЖАХ

Прокопченко С. В.,
головний науковий співробітник
Українського науково-дослідного інституту спеціальної техніки
та судових експертиз Служби безпеки України
ORCID ID: 0000-0002-8338-4876
lodrins@gmail.com

У статті здійснено комплексний аналіз еволюції нормативно-правового регулювання доступу правоохоронних органів держав-членів Європейського Союзу до даних електронних комунікацій. Об'єктом дослідження є ключові нормативно-правові акти ЄС, серед яких: Резолюція № 96/C329/01 «Про законне перехоплення телекомунікацій», Конвенція Ради ЄС № 994_238 про взаємодопомогу в кримінальних справах, Директива № 96/C329/01 (ENFOPOL), Директива 2006/24/ЕС про зберігання даних, а також Директива (ЄС) 2018/1972/ЄС (Європейський кодекс електронних комунікацій).

Метою дослідження є виявлення трансформації підходів Європейського Союзу до забезпечення балансу між інтересами національної безпеки та дотриманням основоположних прав людини, зокрема права на приватність та захист персональних даних. Проаналізовано правові підстави, обсяг та межі здійснення законного перехоплення електронних повідомлень, запровадження обов'язку провайдерів щодо зберігання трафіку даних, а також ключові виклики у процесі імплементації цих норм на національному рівні.

Особливу увагу приділено аналізу рішення Суду Європейського Союзу у справі Digital Rights Ireland (2014), яке призвело до визнання Директиви 2006/24/ЕС такою, що не відповідає Хартії основних прав ЄС. На цьому тлі розглянуто концептуальне перезавантаження підходів до збереження даних у контексті нового нормативного середовища, окресленого положеннями Директиви 2018/1972. Стаття формує пропозиції щодо можливостей адаптації європейських підходів у законодавство України в контексті гармонізації із правом ЄС та в умовах сучасних безпекових викликів, включаючи протидію міжнародному тероризму та військової агресії.

Висновки. ЄС пройшов еволюційний шлях від безпекового централізму до демократичного компромісу, орієнтованого на верховенство права та основоположні свободи. Система доступу до даних стала більш прозорою, підзвітною, орієнтованою на ризик, а не на масовість, що становить орієнтиром для України на шляху імплементації європейських стандартів у сфері електронних комунікацій та прав людини.

Ключові слова: ENFOPOL, законне перехоплення, електронні комунікаційні мережі, правоохоронні запити, збереження даних, приватність, Європейський Союз, національна безпека, Суд ЄС.

Постановка проблеми. Розвиток електронних комунікаційних мереж призвів до трансформації правових підходів до регулювання доступу до інформації в цифровому середовищі. У Європейському Союзі поступове зростання ролі електронної комунікації в повсякденному житті, бізнесі та державному управлінні зумовило необхідність комплексного врегулювання питань конфіденційності, безпеки, доступу до даних і правового статусу провайдерів.

Водночас, розширення технологічних можливостей державних органів у сфері нагляду та забезпечення безпеки викликало занепокоєння щодо потенційного порушення прав людини, зокрема права на приватність, захист персональних даних і свободу вираження поглядів. Судова практика Європейського суду з прав людини (ЄСПЛ) та Суду ЄС неодноразово підкреслювала, що втручання в комунікаційні права має бути законним, пропорційним і виправданим цілями, визначеними в демократичному суспільстві.

Відповідно, виникає необхідність дослідити, яким чином сучасне правове поле ЄС – зокрема через Резолюцію № 96/С329/01 «Про законне перехоплення телекомунікацій» , Конвенцію Ради ЄС № 994_238, Директиву № 994_234 “Про оперативні запити правоохоронних органів стосовно телекомунікаційних мереж загального користування та послуг зв’язку (ENFOPOL)”, Регламент 2016/679 (GDPR), Директиву 2018/1972/ЄС (Європейський кодекс електронних комунікацій) та рішення ЄСПЛ – формує баланс між правами суб’єктів інформаційного суспільства та інтересами національної безпеки, боротьби з кіберзлочинністю та тероризмом.

Крім того, постає потреба у розгляді правової визначеності та прозорості механізмів доступу держав до даних у мережах електронної комунікації, зокрема метаданих, даних локації, змісту повідомлень і способів законного перехоплення, а також умов міжнародної співпраці.

Таким чином, на сьогодні є актуальним розгляд питання щодо еволюції правового регулювання в ЄС доступу до інформації в електронних комунікаційних мережах без порушення при цьому фундаментальних прав громадян**,** а також які підходи можуть бути адаптовані для українського законодавства в умовах цифровізації та викликів до національної безпеки.

Аналіз публікацій. Питання перехоплення інформації у електронних комунікаційних мережах досліджували В. Степанов, С. Грищенко, С. Кокіза. Аналіз нормативно-правових актів та нормативних документів ЄС щодо перехоплення інформації в електронних комунікаційних мережах в контексті підготовки технічного регламенту єдиної системи технічних засобів здійснили С. Кокіза та В. Степанов (Кокіза, Степанов, 2021). В статі В. Степанова та С. Грищенка (Степанов, Грищенко, 2019) здійснено порівняння підходу, на якому базуються загальні технічні вимоги до законного перехоплення інформації в Україні, з підходами, що визначені у світових нормативних документах (стандартах ETSI, рекомендаціях, специфікаціях тощо) зазначеної сфери.

Мета статті – дослідити еволюцію підходів ЄС щодо забезпечення балансу між національною безпекою та основоположними правами людини, зокрема правом на приватність та захист персональних даних, під час перехоплення інформації у електронних комунікаційних мережах.

Виклад основного матеріалу. У 1990-х роках швидкий розвиток телекомунікаційних технологій створив нові виклики для правоохоронних органів ЄС. Зокрема, можливість злочинців використовувати новітні комунікаційні технології для координації своєї діяльності викликала стурбованість у сфері національної та громадської безпеки.

Зростання використання цифрових технологій та мобільного зв’язку ускладнювало процес перехоплення комунікацій з боку правоохоронних органів. Одночасно з цим країни-члени ЄС мали різні підходи до законного перехоплення, що ускладнювало співпрацю в межах Союзу. Правоохоронна діяльність, напроти, потребувала спільних узгоджених технічних стандартів для забезпечення ефективного перехоплення незалежно від країни.

Ради ЄС резолюцією від 17 січня 1995 року № 96/С329/01 “Про законне перехоплення телекомунікацій” встановила принципи та вимоги щодо перехоплення телекомунікацій на території ЄС. Основною її метою є забезпечення законного перехоплення відповідно до національного законодавства кожної країни-члена з дотриманням фундаментальних прав людини.

Основними принципами та вимогами розглянутої Резолюція Ради ЄС, що стала правовою базою ЄС у сфері перехоплення телекомунікацій та захисту даних, є:

– гармонізація стандартів: встановлення мінімальних технічних вимог для телекомунікаційних операторів щодо забезпечення перехоплення;

– спільна відповідальність: країни-члени зобов’язані співпрацювати у створенні єдиних вимог та забезпечувати дотримання прав людини;

– пропорційність та законність: перехоплення має здійснюватися виключно в рамках закону, з урахуванням принципу пропорційності та захисту особистих даних;

– технічні можливості: постачальники телекомунікаційних послуг повинні забезпечувати технічні можливості для законного перехоплення.

– Позитивним аспектом резолюції стало:

– встановлення єдиної політики щодо перехоплення, яка зменшує ризики порушення прав людини;

– забезпечення оперативній діяльності правоохоронних органів;

– створення правовій основи для транскордонного співробітництва.

До недоліків резолюції відносять ризик зловживання: відсутність чітких механізмів контролю може призвести до незаконного використання перехоплення.

Резолюція від 17.01.1995 № 96/С329/01 стала основою для розробки подальших нормативних актів у сфері законного перехоплення телекомунікацій в ЄС, а саме:

– директиви про захист даних № 95/46/ЄС, що встановила основні принципи захисту персональних даних у ЄС та вплинула на практики перехоплення телекомунікацій;

– регламенту про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних № 2016/679/ЄС, введений у дію в 2018 році, який посилив вимоги щодо захисту персональних даних, що також стосується практик перехоплення телекомунікацій, та який має пряме застосування у всіх державах-членах ЄС, без потреби національної імплементації.

Наступним важливим міжнародно-правовим документом, що регулює механізми взаємодопомоги в кримінальних справах між державами-членами ЄС стала Конвенція Ради ЄС від 29.05.2000 № 994_238 (Convention). Її прийняття зумовлене необхідністю удосконалення системи співробітництва у сфері кримінального судочинства, адаптації правових механізмів до сучасних викликів та забезпечення ефективного розслідування злочинів у межах ЄС.

Основними чинниками, що зумовили розробку та прийняття Конвенції, стали:

– необхідність покращення правової співпраці між державами-членами ЄС, оскільки до її прийняття взаємодія у сфері кримінального судочинства регулювалася окремими двосторонніми угодами або нормами Європейської конвенції про взаємну допомогу у кримінальних справах 1959 року. Удосконалення цих механізмів було необхідним для прискорення процесів співпраці та усунення бюрократичних перешкод;

– адаптація до сучасних загроз (організована злочинність, тероризм, кіберзлочинність, корупція);

– гармонізація з базовими нормами міжнародного права та захисту прав людини, якими є положення Європейської конвенції про захист прав людини та основоположних свобод 1950 року, що гарантує дотримання принципів справедливого судочинства, права на приватність та захист персональних даних у процесі міжнародного правового співробітництва.

Основними положеннями Конвенції передбачено:

– розширення сфер співпраці – запропоновано нові форми взаємодії, такі як спільні слідчі групи, контрольовані поставки та негласні операції, що дозволяє ефективніше боротися з транснаціональною злочинністю;

– прямі контакти між судовими органами, що сприяє встановленню прямих зв'язків між компетентними органами держав-членів, що зменшує бюрократичні перепони та прискорює процес обміну інформацією;

– використання сучасних технологій, а саме можливість використання відео- та телеконференцій для допиту свідків та експертів, що підвищує оперативність та знижує витрати на проведення процесуальних дій;

– захист персональних даних та забезпечення конфіденційності при обміні інформацією між державами-членами в рамках кримінальних розслідувань.

Впровадження положень Конвенції вимагало від держав-членів адаптації національного законодавства щодо:

– гармонізації процедур: проведення уніфікації процесуальних норм для забезпечення ефективної співпраці та взаємного визнання рішень;

– забезпечення прав людини: гарантування дотримання фундаментальних прав та свобод особи під час здійснення міжнародної співпраці.

Для забезпечення балансу між потребами кримінального розслідування та захистом прав людини в розділі III "Перехоплення телекомунікацій" зазначеної Конвенції визначено наступні вимоги до механізму перехоплення даних на території ЄС:

– компетентним органом може бути суд або інший спеціально уповноважений орган, який здійснює кримінальне розслідування, але якщо судові органи не мають компетенції у певній сфері, інші державні органи можуть виконувати ці функції відповідно до законодавства країни;

– кожна країна може звернутися до іншої держави-члена щодо негайного перехоплення, запису та подальшої передачі даних із запитом, який має містити інформацію щодо: органу, що подає запит; правові підстави перехоплення; ідентифікаційних даних особи, яка є суб'єктом перехоплення; кримінального діяння, що розслідується; очікувану тривалість перехоплення;

– якщо телекомунікаційна мережа проходить через шлюз у державі-члені, але не є безпосередньо доступною для перехоплення в іншій державі-члені, доступ до комунікацій забезпечується через постачальника послуг у державі, де розташовано шлюз, при цьому держави-члени зобов'язані надати компетентним органам право здійснювати таке перехоплення без залучення іншої держави;

– якщо держава-член перехоплює комунікації особи, яка перебуває в іншій державі, вона повинна повідомити відповідний орган цієї країни. Якщо через 96 годин повідомлена держава дозволяє перехоплення – воно продовжується, у випадку вимоги припинити перехоплення – держава, що здійснювала його, повинна припинити або знищити отримані дані.

Крім того, держави-члени можуть укладати додаткові угоди, які полегшують взаємодію та впроваджують нові технічні рішення для законного перехоплення телекомунікацій.

Ця Конвенція відповідає стандартам Європейської конвенції про права людини, яка гарантує право на повагу до приватного життя та конфіденційність комунікацій, водночас забезпечує співпрацю між країнами ЄС у кримінальних розслідуваннях. Вона стала першим міжнародно-правовим інструментом ЄС, який передбачав правила перехоплення на запит іншої держави-члена та запровадила механізм прямої міждержавної співпраці без погодження через центральні органи.

Одночасно з цим залишається необхідність вдосконалювати механізми контролю та підзвітності, щоб запобігати зловживанням у сфері масового стеження та незаконного збору даних.

З метою зміцнення співпраці між правоохоронними органами держав-членів ЄС у сфері боротьби з організованою злочинністю, тероризмом і кіберзлочинністю в рамках Ради ЄС була створена на робоча група, яка у 1995 році отримала офіційну назву ENFOPOL (скорочення від “Enforcement Police” – “Поліцейське правозастосування”).

У 1998–2001 роках ENFOPOL стає ключовою платформою для обговорення питань телекомунікаційного контролю та оперативного доступу до даних. Група працювала над гармонізацією європейських стандартів у сфері цифрового моніторингу, включаючи доступ до телекомунікаційних даних. Її робота згодом вплинула на директиви щодо збереження даних і безпеки електронних комунікацій у ЄС. Саме за результатом її роботи з представниками телекомунікаційної індустрії, а також після обговорень та узгоджень тексту, Радою ЄС у 2001 році офіційно прийнята директива № 994/234 «Про оперативні запити правоохоронних органів стосовно телекомунікаційних мереж загального користування та послуг зв’язку (ENFOPOL)», яку створено за рекомендаціями ЄС щодо взаємодії постачальників послуг з правоохоронними органами.

Сфера дії документу охоплює всі види телекомунікацій: фіксований зв’язок (PSTN, ISDN), мобільний зв’язок (GSM, UMTS, CDMA), супутниковий зв’язок (S-PCS), пакетна передача даних (GPRS, xDSL, Інтернет). Тобто оперативна інформація для правоохоронних органів може бути запитана з будь-якої інфраструктури передачі даних, включно з VoIP, VPN, e-mail, мобільних додатками тощо. Запитувана інформація включає адреси, кредитні картки, каталожні імена – що може виходити за межі необхідного, якщо не обґрунтовано конкретною кримінальною справою.

Санкціоноване для правоохоронних органів перехоплення інформації можливе лише за умови, якщо визначено конкретний абонент спостереження (ідентифікаційна ознака), межі втручання та термін дії санкції, що дає їм право:

– отримати усі передані або майбутні дані, що асоціюються з ідентифікаційною ознакою абонента спостереження;

– використовувати ідентифікаційні ознаки комунікації: номер кінцевого (термінального) обладнання, IP-адресу, e-mail, IMSI, IMEI, логін, MAC-адресу тощо;

– мати відокремлений доступ до потоків інформації (у разі одночасних з’єднань).

Доступ незалежно від статусу користувача послуг включає: тимчасові користувачі (роумінг, UPT, Wi-Fi), виклики через третіх постачальників послуг, зв’язок через голосову пошту, переадресацію. Це дозволяє відстежувати дії, що маскуються через технічні засоби уникнення ідентифікації.

Правоохоронці прагнуть не лише “перехопити дзвінок”, а відтворити логіку дій, контакти, переміщення, способи маскування активності користувача послуг. Тому інформація про з’єднання містить наступні типи даних:

– статус готовності (онлайн, активне підключення);

– вхідні/вихідні спроби з’єднання;

– сигнали набору, перенаправлення, конференції;

– час, тривалість, початок/кінець;

– переадресовані номери/кінцевий пункт;

– геолокація, навіть логічна (наприклад, точка входу в мережу);

– активовані додаткові послуги (SMS, MMS, Voicemail).

Важливим аспектом при цьому є дотримання принципу законності щодо недопустимості отримувати дані, які не належать до ідентифікованої ознаки абонента спостереження (навіть якщо є технічна можливість це зробити).

Директива описує також технічні та організаційні вимоги правоохоронних органів до постачальників послуг щодо перехоплення інформації в телекомунікаційних мережах. Йдеться про:

– таємність перехоплення інформації (абонент спостереження не повинен знати про факт перехоплення інформації);

– захист інформації про сам процес перехоплення інформації, ідентифікацію суб’єкта перехоплення та запис активації;

– обробку одночасних запитів;

– шифрування.

Цей документ не обмежується конкретними технологіями, що дозволяє його застосування до сучасних цифрових сервісів, включно з месенджерами Telegram, Signal та WhatsApp, хмарними сервісами тощо. Одночасно з тим, щоб технічні можливості постачальників послуг не перетворилися в безконтрольний доступ, потрібна юридична підстава та перевірка пропорційності втручання.

Директива Ради ЄС № 994/234 є нормативний опис функціональних вимог, що стали основою для стандарту ETSI TS 101 671, та які необхідно імплементувати згідно із законами кожної окремої держави для захисту національної безпеки та запобіганню злочинам.

З подальшим розвитком цифрових технологій та зростанням використання електронних комунікацій виникла потреба в оновленні законодавства для забезпечення належного рівня конфіденційності та захисту персональних даних. Директива 95/46/ЄС [37}(Директива про захист даних) від 1995 року вже не охоплювала всі аспекти, пов'язані з новими технологіями, такими як електронна пошта, SMS та інші форми електронних комунікацій. Тому для впорядкування цих питань Європейським Парламентом та Радою ЄС 12.07.2002 прийнято Директиву 2002/58/ЄС «Про обробку персональних даних та захист конфіденційності в секторі електронних комунікацій», яка доповнила Директиву 95/46/ЄС специфічними правилами щодо обробки персональних даних та захисту конфіденційності в секторі електронних комунікацій.

Правила, закладанні в документі, базуються на основних принципах:

1. Відображення парадигми «цифрового ризик-менеджменту», коли правові інститути адаптуються до викликів цифрового середовища. Акцент робиться на балансі між інноваціями та правами людини, що є ключовим постулатом у сучасному європейському праві.
2. Формування концепції «технології, орієнтовані на приватність» (Privacy by Design), в ній акцент на анонімність підкреслює необхідність інтеграції технічних рішень у правову практику.
3. Субсидіарність («не чини згори того, що краще вирішується знизу») та розмежування компетенцій з одночасним визнання потенційного конфлікту між безпекою та приватністю, який вирішується через принцип пропорційності.
4. Технологічна конкретизація юридичних понять та трансформація договірного права в умовах цифровізації.
5. Розрізнення понять "broadcast communication" (трансляційна комунікація) та "personalized communication" (персоналізована комунікація), які визначають межі приватності.
6. Формування основи для "cookie-згоди" та інших онлайн-інтерфейсів, що виводить питання згоди у площину UX-дизайну, поведінкової економіки та права.
7. Створення підгрунття кібергігієни та відповідального провайдингу.

Крім того, у зазначеній Директиві встановлено наступні основні вимоги щодо:

– тимчасового автоматичного зберігання даних (без порушення конфіденційності), необхідних виключно для передачі інформаційних повідомлень, що відповідає принципам мінімізації даних;

– запису інформаційних повідомлень у законних комерційних цілях з дотриманням прозорості та обмеження терміну їх зберігання;

– введення кешування, технічної обробки даних, мінімізації з дотриманням пріоритетів щодо технічної необхідності та захисту персональних даних;

– наявності згоди на обробку персональних даних, якщо додаткова послуга вимагає специфічної обробки даних, а також якщо технічно можливо ідентифікувати користувача послуг (фізичну або юридичну особу);

– відповідності договорів з третіми сторонами (наприклад, агентських) нормам захисту персональних даних, зокрема Директиві 95/46/ЄС (користувачі повинні бути проінформовані про передачу даних трафіку або геолокації);

– впровадження анонімних форм оплати (телефонні картки, часткове маскування номерів), оскільки прозорість білінгових рахунків може загрожувати приватності;

– анонімності для абонентів вразливих груп при ідентифікації номерів (провайдери повинні інформувати користувачів про доступні опції щодо ідентифікації);

– обробки даних геолокації лише з окремої згоди абонента (абонент має право легким образом тимчасово відмовитись від такої обробки);

– можливості виключень з правил конфіденційності у випадках злочинних дій або для служб екстреної допомоги;

– забезпечення за запитом абонента захисту від повторних дзвінків та небажаних звернень;

– надання користувачам права визначати дані щодо публікації у довідниках абонентів і в якому вигляді;

– можливості надсилання небажаних повідомлень (спаму) лише за умови попередньої згоди з користувачем послуг (телефон, факс, e-mail, SMS) під час наявності опції безкоштовної відмови, а також наявності технічних рішень для контролю його згоди;

– наявності визначених умов для прямого маркетингу з правом відмови в межах наявних клієнтських відносин;

– можливості здійснення голосових маркетингових дзвінків лише у разі відповідності цієї дії національному законодавству;

– заборони на використання фальшивих ідентифікаторів під час відправлення маркетингових повідомлень.

Директива від 12.07.2002 № 2002/58/ЄС стала важливим кроком у забезпеченні конфіденційності та захисту персональних даних в епоху цифрових технологій, встановивши основні принципи та вимоги для електронних комунікацій, які згодом були розширені та уточнені новими законодавчими актами ЄС.

Після терористичних атак у США 11 вересня 2001 року та в Європі (Мадрид, 2004; Лондон, 2005) зросла потреба у посиленні заходів безпеки. Це призвело до обговорення необхідності збереження телекомунікаційних даних для запобігання та розслідування серйозних злочинів та офіційного прийняття в березні 2006 року Директиви 2006/24/ЄС Європейського Парламенту та Ради ЄС, відомої як Директива про збереження даних (Data Retention Directive).

Зазначена Директива зобов'язувала постачальників послуг електронних комунікаційних зберігати певні дані протягом періоду не менше шести місяців та не більше двох років з дати повідомлення для забезпечення їх доступності з метою розслідування, виявлення та судового переслідування тяжких злочинів, як це визначено кожною державою-членом у своєму національному законодавстві. Вона застосовувалася до даних про трафік та місцезнаходження, а також до пов'язаних даних, необхідних для ідентифікації абонента або зареєстрованого користувача послуг, але не поширювалася на зміст електронних повідомлень. Обов'язок збереження даних також мав відношення до даних про невдалій спробі дзвінків, коли ці дані генеруються або обробляються.

Проте 8 квітня 2014 року Суд ЄС у справі Digital Rights Ireland (C-293/12 та C-594/12) (Adam Juszczak, Elisa Sason, 2021) визнав Директиву 2006/24/ЕС недійсною. Суд ЄС постановив, що Директива порушує основні права на повагу до приватного життя та захист персональних даних, гарантовані Хартією основних прав ЄС, а саме:

– загальне та невибіркове зберігання даних не обмежується лише тим, що є строго необхідним;

– відсутність чітких правил щодо доступу до даних не забезпечує достатніх гарантій проти зловживань.

Це рішення стало прецедентом для перегляду законодавства щодо законного перехоплення та зберігання даних у країнах-членах ЄС. Після визнання Директиви недійсною, багато країн ЄС переглянули свої національні закони щодо законного перехоплення та зберігання даних. Деякі країни, як-то Німеччина та Румунія, скасували відповідні закони або внесли суттєві зміни для забезпечення відповідності вимогам Суду ЄС.

Ключовим документом, що реформувала та консолідувала правову базу ЄС у сфері електронних комунікацій стала Директива 2018/1972/ЄС, відома як Європейський кодекс електронних комунікацій (European Electronic Communications Code, EECC), яка прийнята Європейським Парламентом та Радою 11.12.2018 з подальшим імплементуванням її положень державами-члени ЄС.

EECC об'єднала та замінила чотири основні директиви: 2002/19/ЄС (директива про доступ), 2002/20/ЄС (директива про авторизацію), 2002/21/ЄС (рамкова директива), 2002/22/ЄС (директива про універсальні послуги). Це дозволило створити єдиний, узгоджений правовий акт, що регулює електронні комунікації в ЄС.

EECC встановлює базові визначення, що забезпечують чітке розмежування між різними елементами електронних комунікацій та є критично важливим для правильного застосування нормативно-правових вимог і забезпечення прав користувачів, а саме:

– електронна комунікаційна мережа: системи передачі сигналів, включаючи обладнання для комутації або маршрутизації обладнання та інші ресурси, що дозволяють передачу сигналів за допомогою дротів, радіо, оптичних або інших електромагнітних засобів;

– електронна комунікаційна послуга: платна послуга зазвичай, що повністю або переважно складається з передачі сигналів через електронні комунікаційні мережі, включаючи телекомунікаційні та інтернет-послуги;

– номер ресурсу: номер, що використовується для ідентифікації кінцевих точок у мережі, наприклад, телефонний номер або IP-адреса;

– користувач: фізична або юридична особа, яка використовує або запитує публічно доступну електронну комунікаційну послугу;

– кінцеве обладнання: обладнання, призначене для підключення безпосередньо або опосередковано до інтерфейсів публічних електронних комунікаційних мереж, наприклад, телефони, модеми, маршрутизатори.

Директива визначає чіткі вимоги до національних регуляторних органів, зокрема:

– гарантування їх незалежності та політичної нейтральності;

– призначення керівників на термін не менше трьох років;

– забезпечення участі в діяльності Органу європейських регуляторів електронних комунікацій (BEREC).

Одночасно ЕЕСС посилює права користувачів, включаючи:

– обмеження цін на внутрішньоєвропейські дзвінки та SMS;

– право на зміну оператора без додаткових витрат;

– обов'язок операторів надавати інформацію про умови контрактів;

– ведення системи публічних оповіщень у разі надзвичайних ситуацій.

ЕЕСС підкреслює важливість захисту конфіденційності електронних комунікацій, але допускає обмеження цього права відповідно до статті 15 Директиви 2002/58/ЄС.

Висновки. Європейський Союз пройшов трансформаційний шлях від безпекового централізму до моделі правового регулювання, заснованої на дотриманні прав людини, верховенстві права та демократичних принципах. Це відобразилось у зменшенні практик масового збору даних, посиленні інституційного контролю за доступом до комунікацій, а також у впровадженні системи незалежного судового нагляду. Застосування ризик-орієнтованого підходу у сфері доступу до електронної інформації стало не лише нормою, а й критерієм ефективності системи цифрової безпеки. В умовах євроінтеграції та реформування сектору електронних комунікацій Україні доцільно адаптувати положення європейського права, особливо у сфері регламентації діяльності СБУ, НАБУ, кіберполіції та інших суб'єктів доступу до трафіку і даних. Варто прийняти законодавчий акт, в якому запровадити незалежний нагляд за такими діями, наприклад через уповноважений орган або судову інстанцію із забезпеченням прозорості звітуванням перед парламентом і громадськістю.

Держави-члени ЄС можуть приймати законодавчі заходи, які обмежують права на конфіденційність, якщо такі заходи є необхідними, пропорційними та відповідають демократичному суспільству для забезпечення національної безпеки. Тобто під час дії воєнного стану Україна має законне право тимчасово обмежувати певні права, зокрема конфіденційність електронних комунікацій, у межах, необхідних для забезпечення оборони та національної безпеки. Водночас навіть за таких обставин слід дотримуватися принципів необхідності, пропорційності та демократичної обґрунтованості, згідно з практикою ЄС. Це означає, що будь-яке втручання у приватне спілкування має:

– здійснюватися лише за наявності чітко визначених правових підстав, з дотриманням процедури;

– супроводжуватися обмеженням обсягу даних, що збираються (мінімізація);

– мати встановлений строк зберігання інформації, із подальшим обов'язковим знищенням;

– передбачати документовану правову оцінку необхідності такого втручання.

Prokopchenko S. Regulation in the EU of access to information in electronic communications networks

The article provides a comprehensive analysis of the evolution of the regulatory framework governing access to electronic communications data by law enforcement agencies in the European Union Member States. The research focuses on key EU regulatory frameworks, including: Council Resolution of 17 January 1995 on the lawful interception of telecommunications № 96/C329/01; Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union № 994_238, Directive (EU) № 96/C329/01 (ENFOPOL), Directive (EU) 2006/24 про зберігання даних, Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast).

The aim of the study is to identify the transformation of the European Union's approaches to ensuring a balance between national security interests and respect for fundamental human rights, in particular the right to privacy and protection of personal data. The legal basis, scope, and limits of lawful interception of electronic messages, the introduction of the obligation of providers to store data traffic, as well as key challenges in the implementation of these norms at the national level are analyzed.

Particular attention is paid to the analysis of the decision of the Court of Justice of the European Union in the Digital Rights Ireland case (2014), which led to the recognition of Directive 2006/24/EC as incompatible with the EU Charter of Fundamental Rights. Against this background, a conceptual reboot of data retention approaches is considered in the context of the new regulatory environment outlined by the provisions of Directive 2018/1972. The article formulates proposals on the possibilities of adapting

European approaches to Ukrainian legislation in the context of harmonization with EU law and in the context of modern security challenges, including countering international terrorism and military aggression.

Conclusion. The EU has evolved from security centralism to a democratic compromise focused on the rule of law and fundamental freedoms. The data access system has become more transparent, accountable, risk-oriented, and not mass-oriented, which is a benchmark for Ukraine on the path to implementing European standards in the field of electronic communications and human rights.

Key words: ENFOPOL, lawful interception, electronic communications networks, law enforcement requests, data retention, privacy, European Union, national security, Court of Justice of the EU.

Література:

1. Степанов В.А., Грищенко С.М. (2019). Особливості побудови системи законного перехоплення інформації з телекомунікаційних мереж. *Збірник наукових праць НА СБУ*, 69, 199–204.
2. Кокіза С.В., Степанов В.А. (2021). Вимоги правоохоронних органів ЄС щодо законного перехоплення інформації в електронних комунікаційних мережах. *Інформація і право*, 3(38) 115–120. https://doi.org/10.37750/2616-6798.2021.3(38).243815.
3. Council Resolution of 17 January 1995 on the lawful interception of telecommunications: 96/C329/01. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj%3AJOC_1996_329_R_0001_01&utm
4. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A31995L0046.
5. 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). https://eur-lex.europa.eu/eli/reg/2016/679/oj
6. Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Unionhttps. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000F0712%2802%29.
7. Council Resolution on law enforcement operational needs with respect to public telecommunication networks and services. 9194/01 ENFOPOL 55 ECO 143 https://www.statewatch.org/media/documents/news/2001/sep/9194.pdf
8. ETSI TS 101 671 «Lawful Interception (LI); Handover Interface for the Lawful Interception of Telecommunications Traffic».
9. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0058.
10. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. https://eur-lex.europa.eu/eli/dir/2006/24/oj.
11. Recalibrating Data Retention in the EU The Jurisprudence of the CJEU – Is this the End or the Beginning? Adam Juszczak and Elisa Sason. https://eucrim.eu/articles/recalibrating-data-retention-in-the-eu/#statement
12. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast). https://eur-lex.europa.eu/eli/dir/2018/1972/oj/eng.

Стаття надійшла до редакції 05.06.2025
Рекомендована до друку 13.08.2025
Опублікована _____.2025