Інформаційна довідка
щодо правил конфіденційності
електронних комунікацій*

Анотація. В Інформаційній довідці викладено результати аналізу законодавства Європейського Союзу щодо обробки персональних даних і захисту конфіденційності в секторі електронних комунікацій. Акцентовано увагу на основних проблемах щодо визначення засад удосконалення законодавчого регулювання обробки персональних даних у мережі електронних комунікацій.

Ключові слова: *електронні комунікаційні мережі, захист інформації, персональні дані, конфіденційність*.

Вступ.

Сучасний цифровий простір неймовірно складний. Конвергенція персональних даних, правил конфіденційності, маркетингових практик створюють чималі ризики у правозастосуванні та захисті прав користувачів електронних комунікаційних мереж. Положення законодавства про конфіденційність користувачів пов'язують із доступом до онлайн-контенту, інтерактивних медіа та широкого спектру можливостей, які пропонуються мережевими комунікаціями, залишаючи поза увагою те, як приватні компанії, державні організації та установи зберігають і використовують персональні дані.

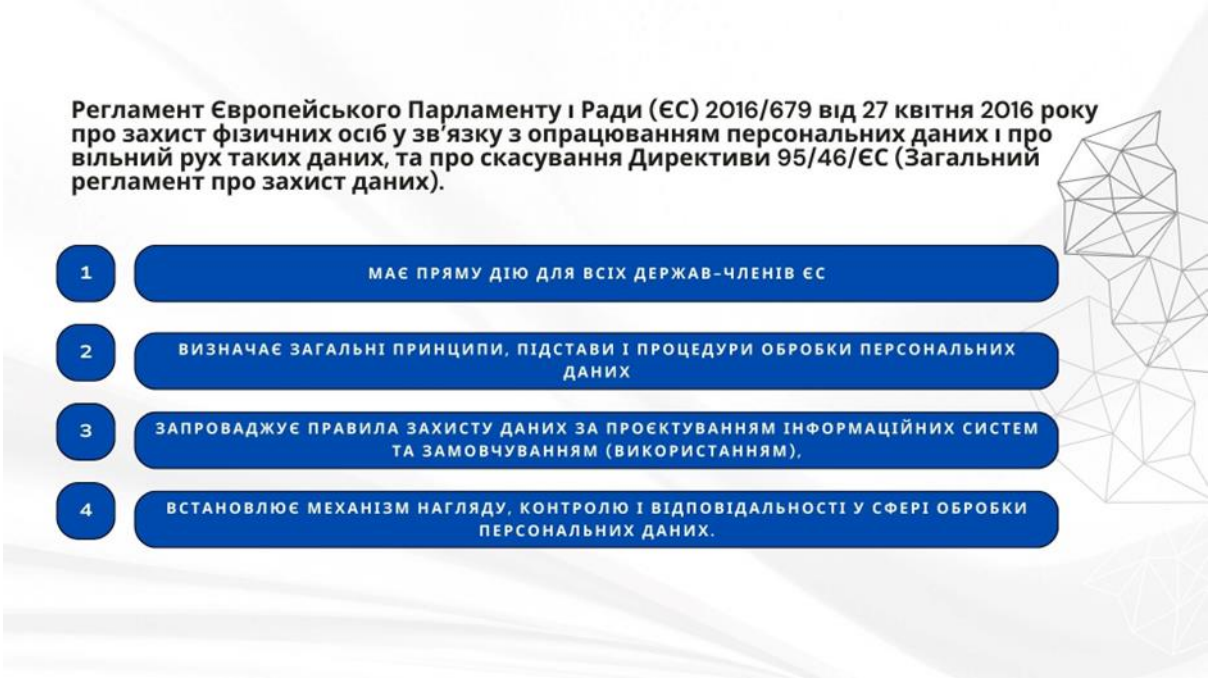
Електронні комунікації стали важливою галуззю будь-якої національної економіки й окремим напрямом транскордонного співробітництва, в межах якого здійснюється обробка значних обсягів персональних даних. Існування ризиків, які супроводжують надання електронних комунікаційних послуг, обумовило необхідність постійного оновлення законодавства про захист інформації. Значний внесок у сучасний розвиток законодавчого врегулювання цифрових інновацій та стандартів конфіденційності належить Європейському Союзу (далі – ЄС).

Основна частина.

Наразі електронні комунікаційні мережі, окрім традиційних сфер, використовуються для багатьох цілей, включаючи бізнес (комерцію), роботу, соціальну взаємодію, доступ до медіа, взаємодію з урядом тощо. Інтереси конфіденційності користувачів, які беруть участь у цій різноманітній діяльності, виходять за межі інтересів, захищених законодавством про конфіденційність електронних даних. Враховуючи зазначене, у ЄС, попри існування окремого законодавчого регулювання відносин з обробки персональних даних, забезпечення конфіденційності персональних даних у секторі/мережі електронних комунікацій розглядається крізь призму права особи на невтручання у приватне і сімейне життя. Це означає, що, окрім актів Європейського Парламенту, на відносини з обробки й захисту персональних даних в електронних комунікаційних мережах поширюються положення Конвенцій Ради Європи про захист прав людини і основоположних

свобод і про захист фізичних осіб у зв’язку з автоматизованою обробкою персональних даних (Модернізована Конвенція 108+).

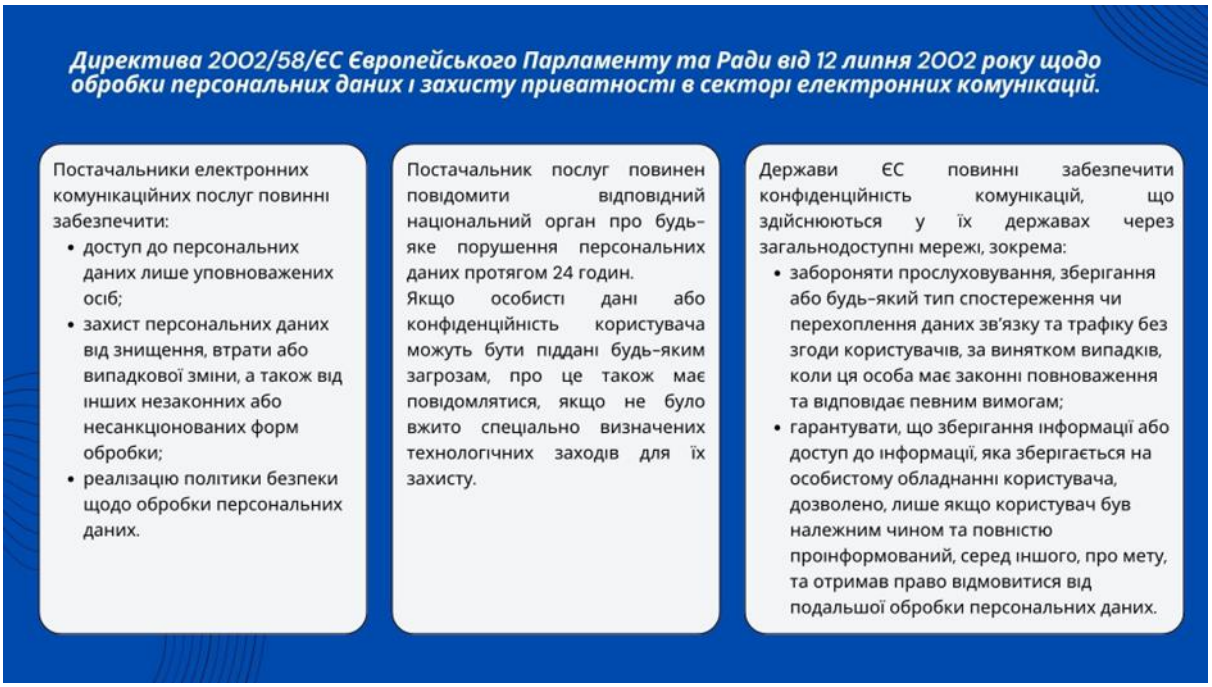
Основним законодавчим актом, яким визначено універсальні правила обробки персональних даних в ЄС (а в окремих випадках і в інших державах), є Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних)[1]. Як акт Європейського Парламенту, який має пряму дію для всіх держав-членів ЄС, Загальний Регламент про захист даних визначає базові принципи, підстави і процедури обробки персональних даних, запроваджує правила захисту даних за проєктуванням інформаційних систем та замовчуванням (використанням), встановлює механізм нагляду, контролю і відповідальності у сфері обробки персональних даних.



Галузь електронних комунікацій в ЄС належить до тих сфер регулювання, де чинними є спеціальні правила захисту персональних даних. Такі правила визначаються Директивою 2002/58/ЄС Європейського Парламенту та Ради від 12 липня 2002 року щодо обробки персональних даних і захисту приватності в секторі електронних комунікацій (далі – Директива про конфіденційність та електронні комунікації)[2]. Системний аналіз положень вказаного акта дозволяє виділити основні концептуальні засади забезпечення конфіденційності у секторі електронних комунікацій:

[1] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року 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). URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text

[2] 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). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32002L0058

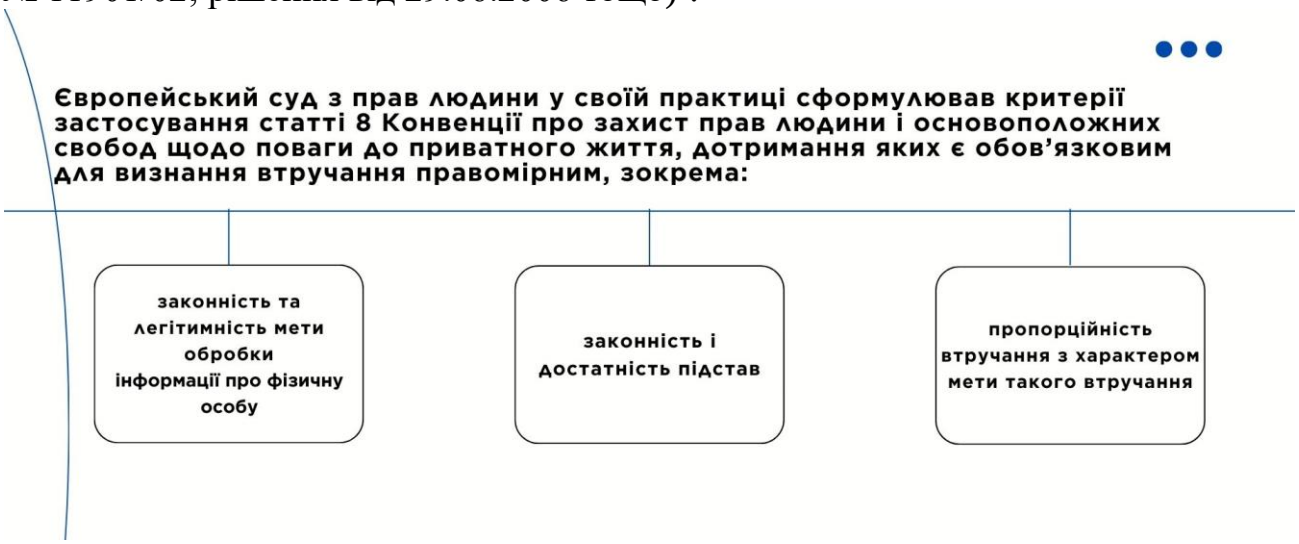


Коли дані трафіку більше не потрібні для зв'язку чи виставлення рахунків, їх потрібно стерти або зробити анонімними. Проте постачальники послуг можуть обробляти ці дані для маркетингових цілей до тих пір, поки зацікавлені користувачі дають свою згоду. Ця згода може бути відкликана в будь-який час.

Згода користувача також потрібна в інших випадках, зокрема: до надсилання повідомлення (спам, небажані повідомлення). Це стосується служб коротких повідомлень (SMS) та інших систем обміну електронними повідомленнями; до моменту, коли інформація (файли cookie) буде збережена на їхніх комп'ютерах чи пристроях, або до того, як буде отримано доступ до цієї інформації – користувач має отримати чітку та повну інформацію, серед іншого, про мету зберігання чи доступу; до того, як номери телефонів, адреси електронної пошти чи поштові адреси з'являться в загальнодоступних каталогах.

Відповідно до статті 15 Директиви про конфіденційність даних та електронні комунікації, обсяг прав і обов'язків може бути обмежений лише національними законодавчими актами, коли такі обмеження є необхідними та пропорційними для захисту конкретних суспільних інтересів, наприклад: щоб дозволити кримінальне розслідування; для захисту національної безпеки, оборони; для забезпечення громадської безпеки. Зазначені вимоги ґрунтуються на нормах міжнародного права про мету і підстави обробки персональних даних, які мають загальний характер (стаття 12 Загальної Декларації прав людини (1948 р.), стаття 17 Міжнародного пакту про громадянські і політичні права (1966 р.); стаття 8 Конвенції про захист прав людини і основоположних свобод (1950 р.) тощо.)

Європейський суд з прав людини у своїй практиці сформулював критерії застосування статті 8 Конвенції про захист прав людини і основоположних свобод[3] щодо поваги до приватного життя, дотримання яких є обов'язковим для визнання втручання правомірним. Це, зокрема, законність та легітимність мети обробки інформації про фізичну особу, законність і достатність підстав, а також пропорційність втручання з характером мети такого втручання (Справи: «S. and Marper v. The United Kingdom» (заяви № 30562/04 30566/04, рішення від 04.12.2008); «Ciubotaru v. Moldova» (заява № 27138/04, рішення від 27/04/2010); «Авілкіна та інші проти Російської Федерації» («Avilkina andeOthers v. Russia»; заява № 1585/09; рішення від 06.06.2013), «Пантелеєнко проти України» («Panteleyenko v. Ukraine»; заява № 11901/02; рішення від 29.06.2006 тощо)[4].



У справі «Big Brother Watch та інші проти Сполученого Королівства», яка розглядалася Європейським судом з прав людини щодо електронного спостереження з боку розвідувальних служб за великою кількістю компаній, неурядових організацій та фізичних осіб, увага була приділена можливості

[3] Конвенція про захист прав людини і основоположних свобод. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text

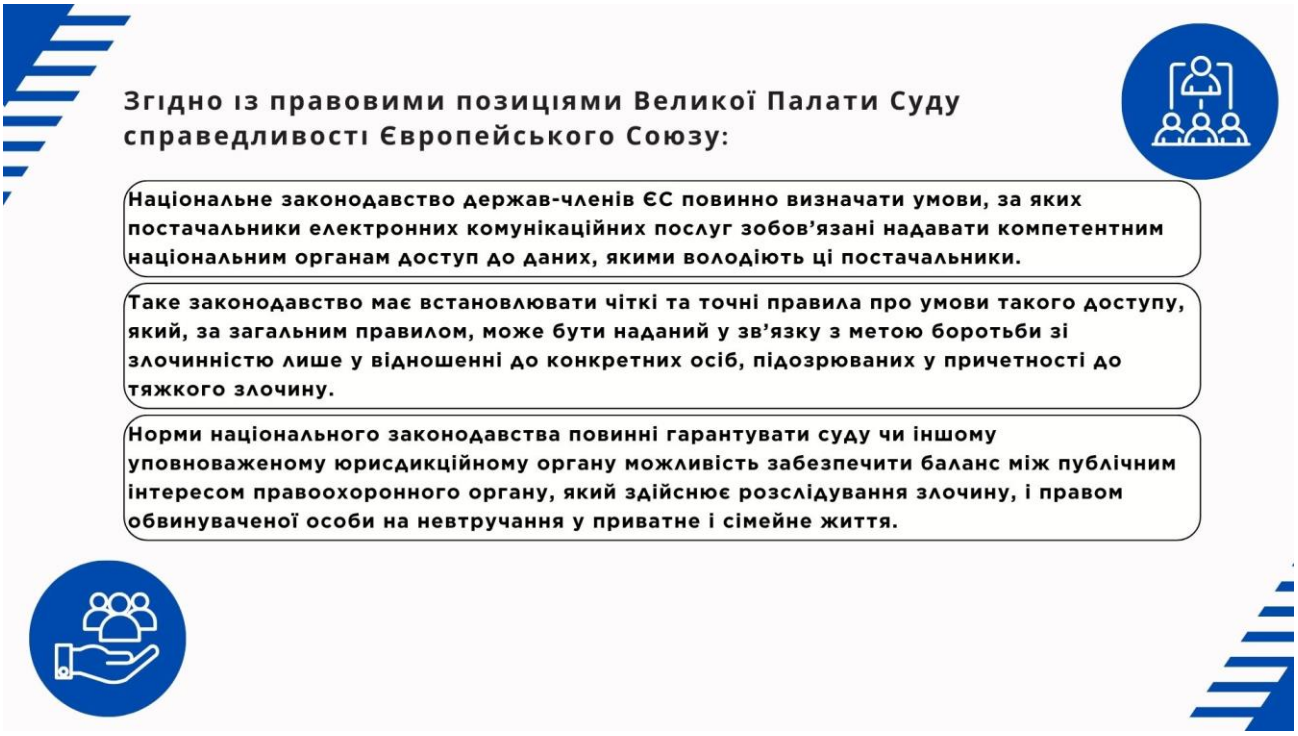
[4] Заслуговує на увагу рішення Європейського суду з прав людини у справі «Бенедік проти Словенії» (2018 р.), у якому вкотре наголошено: закон, який є підставою втручання у приватність, має бути чітким і пропонувати достатні гарантії від зловживань посадовими особами під час процедури доступу та передачі персональних даних. Суть справи полягала у тому, що правоохоронні органи, розслідуючи справу про розповсюдження дитячої порнографії, без судового ордеру отримали від провайдера інформацію, яка ідентифікувала власника динамічної IP-адреси. Одним із ключових питань для Суду у цій справі стало питання: чи міг заявник, користуючись всесвітньою мережею, обґрунтовано розраховувати на анонімність та чи достатньою мірою національне законодавство захищало його приватність від втручання. Суд наголосив, що заявник не міг обґрунтовано очікувати збереження його динамічної IP-адреси в таємниці, але він міг обґрунтовано очікувати конфіденційності стосовно його особистості, зокрема тому, що присвоєну динамічну IP-адресу, навіть якщо її могли бачити інші користувачі мережі, неможливо було простежити до певного комп'ютера без перевірки даних провайдерів на підставі запиту поліції. Встановивши порушення, суд зазначив, що у відповідний час не існувало жодних правил, які б визначали умови для збереження отриманих у ході розслідування даних, а також жодних гарантій від зловживань посадових осіб під час процедури доступу та передачі таких даних, а отже – законодавство було, принаймні, не когерентним щодо рівня захисту інтересів заявника в конфіденційності.

зловживань з боку держави. Суд аналізував матеріали справи за такими критеріями: характер правопорушення, який може обумовити видачу ордера на перехоплення даних; визначення категорії осіб, чиї переговори можуть бути перехоплені; встановлення обмежень щодо тривалості періоду перехоплення даних; визначення процедури для дослідження, використання та зберігання отриманих даних; запобіжні заходи під час передачі даних третім особам; визначення обставин, за яких перехоплені дані можуть і повинні бути знищені. У своєму рішенні Суд зазначив, що саме по собі масове перехоплення інформації державними розвідувальними службами не вважається порушенням права на приватність, оскільки воно є важливим засобом для досягнення законних цілей, враховуючи поточний рівень небезпеки як з боку терористичних організацій, так і в контексті скоєння тяжких злочинів. Разом із тим критерії пошуку та фільтри відбору, які використовуються для обробки такої інформації, повинні піддаватися незалежній перевірці та нагляду, а гарантії, що регулюють вибір перехоплених даних для аналізу, мають бути посилені. Окремо суд наголосив на небезпеці для конфіденційної діяльності журналістів. Відсутність запобіжників щодо перехоплення даних у журналістів та можливість аналізувати будь-яку перехоплену стосовно них інформацію, на думку Суду, має негативні наслідки для свободи преси.

Таким чином, незалежно від сфери обробки персональних даних, забезпечення законності підстав такої обробки, а також дотримання пропорційності, легітимності і заздалегідь визначеності мети вчинення будь-яких дій із персональними даними є обов’язковими умовами. Для сектору (мережі, галузі) електронних комунікацій дотримання наведених вимог посилюється вимогами, передбаченими статтею 95 Загального регламенту про захист даних, а саме: на учасників відносин у галузі електронних комунікацій загальні обов’язки у сфері обробки персональних даних поширюються відповідно до Директиви ЄС про конфіденційність даних та електронні комунікації. Будь-які дії з персональними даними або базами персональних даних, які перебувають у володінні постачальників електронних комунікаційних послуг, якщо вони виходять за межі визначеної мети і підстав обробки, вважаються протиправними.

Необхідно зауважити, що в державах-членах ЄС відсутній єдиний законодавчий підхід щодо розуміння винятків із заборони на передачу постачальниками електронних комунікаційних послуг персональних даних правоохоронним органам. Важливим інструментом досягнення спільної позиції у цьому питанні є практика Суду Європейського Союзу та Європейського суду з прав людини.

Базовими з досліджуваного питання є правові позиції Великої Палати Суду справедливості Європейського Союзу (далі – Суд), викладені у попередньому рішенні від 30 квітня 2024 у справі C 178/22:



Для забезпечення на практиці дотримання принципів необхідного та пропорційного втручання важливо, щоб доступ компетентних національних органів до збережених даних був залежним (за винятком випадків належним чином обґрунтованої терміновості) від попередньої перевірки, здійсненої судом або незалежним органом адміністративної юрисдикції.

Суд вказав на неприпустимість розширення змісту поняття «тяжкий злочин» з метою запровадження нормами національного законодавства додаткових підстав для порушення принципу конфіденційності даних, які обробляються у секторі електронних комунікацій.

Із наведеного рішення слідує фактична заборона на будь-які систематичні широкі обміни персональними даними між суб'єктами надання електронних комунікаційних послуг і правоохоронними органами, включаючи потреби наповнення правоохоронних інформаційних ресурсів.

Зважаючи на існуючі розбіжності у підходах до правового регулювання обробки персональних даних у секторі електронних комунікацій, Європейська комісія висунула пропозицію оновити ці правила (активні спроби робилися у 2015 та 2017 роках). Однак законодавці поки що не змогли спільно узгодити остаточний текст проєкту Регламенту про захист персональних даних у секторі електронних комунікацій. Тривають дискусії щодо концептуального підходу до засад регулювання.

Поширеними є три підходи: перший – орієнтований на послуги, другий – орієнтований на дані і третій – орієнтований на значення. У підході, орієнтованому на послуги, сфера застосування правил конфіденційності визначається на основі виду послуг (основний ризик – існування різних правил конфіденційності). Підхід,

орієнтований на дані, передбачає захист інтересів конфіденційності користувачів через встановлення правил обробки типів персональних даних, зокрема правил щодо даних про місцезнаходження та трафік (основний ризик – пріоритетом у створенні системи конфіденційності електронних комунікацій має бути захист людей, а не даних). Підхід, орієнтований на цінності, визначає сферу застосування правил на основі інтересів конфіденційності користувача під час використання електронних комунікаційних мереж (основний ризик – як правило, ці інтереси виходять за межі інтересів конфіденційності в традиційних телекомунікаційних мережах).

Серед представників Європейського Парламенту і галузевих асоціацій у сфері електронних комунікацій поширеною є думка, відповідно до якої Європейська комісія повинна знову зосередитися на тому, що є найважливішим у чинній Директиві про електронну конфіденційність: принципі конфіденційності, закріпленому в Хартії основних прав ЄС, Договорі про функціонування ЄС та національних конституціях. Якщо для розробки конституційного принципу конфіденційності комунікацій необхідні додаткові правила, їх слід включити в горизонтальний інструмент – Загальний регламент про захист даних або майбутній Регламент про цифрові мережі.

За словами комісара Тьєррі Бретона, відповідального за внутрішній ринок, Європейська комісія працюватиме над сміливою, перспективною та кардинальною пропозицією про включення принципу конфіденційності комунікацій до майбутнього Регламенту про цифрові мережі, що зробить непотрібними правила для окремих секторів, оскільки всі суб’єкти, що надають цифрові комунікації, підпорядковуватимуться цьому фундаментальному принципу.

Висновки.

З урахуванням проведеного дослідження можна сформулювати такі основні висновки:

1. Галузь електронних комунікацій в ЄС залишається однією з небагатьох сфер правового регулювання, де діють загальні та спеціальні акти Європейського Парламенту.

2. Хоча норми Загального регламенту про захист персональних даних покладають на учасників відносин у галузі електронних комунікацій загальні обов’язки щодо обробки персональних даних, це не обмежує дію Директиви ЄС про конфіденційність даних у секторі електронних комунікацій з відповідних питань.

3. У законодавстві держав-членів ЄС діє загальне правило, відповідно до якого постачальники електронних комунікаційних послуг зобов’язані надавати на запит уповноважених правоохоронних органів персональні дані клієнтів лише у справах про розслідування тяжких злочинів і на підставі вмотивованого процесуального акта, у якому визначаються види запитуваних персональних даних, мета їх обробки, умови забезпечення конфіденційності, вид провадження, де буде здійснюватися їх подальша обробка.

4. Враховуючи існуючий в ЄС підхід до врегулювання процедур обробки персональних даних, автоматичний обмін інформацією про фізичних осіб між суб'єктами ринку електронних комунікацій і правоохоронними органами вбачається неможливим.

5. Зважаючи на триваючі в ЄС дискусії щодо подальшого застосування Директиви ЄС про конфіденційність персональних даних у секторі електронних комунікацій, доцільним вбачається вивчення досвіду щодо можливості прийняття Кодексу цифрової трансформації України як основного законодавчого акта у секторах електронних комунікацій, цифрових послуг й електронного урядування, у положеннях якого своє закріплення можуть знайти спеціальні норми про обробку персональних даних у зазначених сферах правового регулювання.

Дослідницька служба
Верховної Ради України