МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ МІЖНАРОДНИХ ВІДНОСИН
Кафедра міжнародного права та порівняльного правознавства

ДОПУСТИТИ ДО ЗАХИСТУ

В.о. Завідувача кафедри
_____ Р.О. Максимович
«____»_____2023 р.

ДИПЛОМНА РОБОТА
ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ
«БАКАЛАВР»
спеціальності 293 «Міжнародне право»

Тема: **ПРАВОВІ ЗАСАДИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ЄВРОПЕЙСЬКОМУ СОЮЗІ**

Виконавець: Дунаєвська Діана Юріївна
Науковий керівник: д.ю.н., професор кафедри міжнародного права та порівняльного правознавства Мушак Наталія Богданівна
Нормоконтролер: викладач кафедри міжнародного права та порівняльного правознавства Головатенко Марина Юріївна

Київ, 2023

ЗМІСТ

ВСТУП

Актуальність обраної теми дослідження.

Широке поширення та застосування інформаційних технологій, методів автоматичної обробки даних, формування глобальних інформаційних систем, доступ до яких може здійснюватися практично будь-якою особою з будь-якої точки земної кулі - це реальні характеристики цифрової ери, що набирає обертів. З одного боку, всі переваги вільного доступу до інформації безпосередньо забезпечують громадянам вирішення одного з головних демократичних прав на свободу інформації, а ведення масштабних автоматизованих баз даних не тільки суттєво оптимізує різноманітні процеси підготовки та прийняття рішень, а й полегшує громадянам доступ до послуг цифрового керування від використання кредитних карток до формування біометричного портрета й прогнозування можливих захворювань. З іншого боку, широке використання персональних даних органами державної влади, комерційними та публічними організаціями суттєво посилює ризик несанкціонованого вторгнення сторонніх осіб у особисту сферу людини, створює загрозу порушення одного з її основоположних природних прав на недоторканність приватного життя

Сучасні технології, особливо в інформаційно-телекомунікаційній сфері, розвиваються настільки стрімко, що часто правове регулювання не встигає за цим розвитком, і це породжує безліч як реальних, так і потенційних загроз основним правам та свободам людини. Одна з актуальних проблем полягає в тому, що нові технології створюють безпрецедентні можливості для свідомого чи неусвідомленого порушення права недоторканності приватного життя.

З розвитком комп'ютерних технологій найбільш схильною до порушень категорією стала особиста інформація. Кількість загроз персональної інформації у XXI столітті неухильно зростає. В останні роки поширення

набуває така тенденція, як перетворення персональної інформації на товар. Однак володіють особистими даними не тільки самі індивіди, але й великий бізнес, який постійно використовує їх з метою отримання прибутку та захоплення ринку, державні органи та відомства тощо.

Особливо схильні до ризику держави, потоки інформації між якими можуть передаватися без будь-яких бар'єрів, зокрема, в рамках міжнародних та регіональних організацій. До таких державних об'єднань належить Європейський Союз, який є унікальним інтеграційним утворенням, яке не має аналогів у світі.

На даний момент у рамках Європейського Союзу здійснюється найбільш тісна та вільна економічна інтеграція у світі, продовжується формування економічного та валютного союзу та, зокрема, процес поступового переходу на наступну стадію інтеграційного об'єднання. У рамках цього союзу відбувається формування Єдиного цифрового ринку ЄС, створення якого є одним із пріоритетних напрямів діяльності європейських інституцій протягом останніх років. Тому питання легального використання персональних даних є важливим для суб'єктів економічної діяльності, що працюють у державах-членах ЄС, а також для всіх партнерів Союзу по всьому світу.

У Європейському Союзі та багатьох інших країнах спеціальне законодавство про захист персональних даних існує вже тривалий час. Однак, у цих країнах активний розвиток та вдосконалення інформаційних технологій, стирання кордонів передачі даних, початок використання нових видів персональних даних, таких як, наприклад, біометричні дані, зумовлюють появу нових викликів часу, що потребують вирішення. Подібно до інших соціальних перетворень, інтеграція не тільки створює нові можливості, а й породжує нові суспільні проблеми, зокрема високий рівень економічного розвитку країн ЄС стимулює проблеми безпеки персональної інформації.

Поява нових загроз недоторканності приватного життя, що виникають у процесі збирання, обробки, зберігання та іншого використання персональних даних у різних контекстах, очевидно доводить необхідність розробки ефективних заходів з охорони фундаментального права людини на захист персональних даних. Неправомірна діяльність може бути край небезпечною для збереження недоторканності приватного життя у разі відсутності належних інструментів правового регулювання захисту персональної інформації.

При всій значущості та актуальності проблематика забезпечення правової охорони та захисту персональних даних є одним із малодосліджених напрямів, як у європейському праві, так і у внутрішньодержавному праві. Окремі роботи зачіпають лише вибіркові аспекти правового регулювання захисту персональних даних - питання передачі між державами, захисту персональних даних працівника, технічні аспекти захисту персональних даних, використання персональних даних у мережі Інтернет тощо.

Теоретичні та практичні аспекти питання захисту персональних даних відображені у працях цілої низки як зарубіжних, так і вітчизняних вчених. До зарубіжних вчених, які розробляли й підтримували дане питання, праці та ідеї яких були використані при написанні даного дослідження, насамперед потрібно віднести таких юристів-міжнародників: Л Байгрейв, Л. Брендейс, А. Блас, П. Блум, Л. Бергкамп, Ч Бейкер, Е. Лін, С. Кірк, Н Кортес, А Рауль, Б. Уорлі, М Оуен, С Уоррен, П. Хустинкс, Я.Кабел, К.Прінс, Е Ерл, К.Харві, Д.Філіпс, Д.Харрінггон, М.Томсон, Д.Рейденберг, Л. Брейдейс, С. Уоррен, І. Вельдер.

Серед українських науковців варто назвати: М. Микієвич, О. Шевчук, І. Яворська,, В.Іванський, Б.Кормич, С.Кашкін, А. Чернобай, О.Капустін, Л. Чернявський, В. Цимбалюк, В. Брижко, О. Баранов, Ю. Базанов, І Жиляєв, О. Сидєльніков, М. Важорова. Однак, у переважній більшості даних праць в основному досліджується вплив на процеси захисту особистої інформації на рівні міжнародних конвенцій та договорів, частиною яких є також Україна.

Незважаючи на існування низки загальнотеоретичних і спеціальних робіт у галузі охорони та захисту персональних даних в Європейському Союзі, зазначена тема в даний час достатньо не розроблена, ціла низка питань є дискусійною, а деякі залишені поза увагою, у той час як від їх висвітлення багато в чому залежить розвиток правового регулювання захисту персональних даних - однієї з фундаментальних потреб людини у суспільстві. Слід враховувати, що тенденції розвитку правового регулювання захисту персональних даних в ЄС є досить динамічними, що зумовлює проведення подальших досліджень.

Метою роботи є комплексний аналіз правових засад захисту персональних даних у Європейському Союзі та виявлення особливостей механізму їх правового регулювання.

Поставлена мета зумовила необхідність вирішення наступних **завдань**:

-розглянути поняття, ознаки та особливості персональних даних у Європейському Союзі;

-визначити джерела та принципи правового регулювання персональних даних у Європейському Союзі;

-оцінити значення захисту персональних даних для підвищення ефективності внутрішнього ринку;

-розглянути основи захисту персональних даних у законодавстві Європейського Союзу;

-проаналізувати право на захист персональних даних у практиці Суду Європейського Союзу;

-дослідити особливості імплементації правових актів Європейського Союзу у сфері захисту персональних даних державами-членами ЄС;

-визначити та проаналізувати актуальні правові проблеми у сфері захисту персональних даних;

-дослідити напрямки розвитку правового регулювання захисту персональних даних у Європейському Союзі.

Об'єктом дослідження є суспільні відносини, що виникають щодо захисту персональних даних у Європейському Союзі.

Предмет дослідження складають проекти та чинні нормативні правові акти Європейського Союзу, інших міжнародних та регіональних організацій, держав-членів ЄС, практика їх застосування, наукова література з питань захисту персональних даних.

Методична і теоретична основа даного дослідження базуються на працях вітчизняних і закордонних учених по досліджуваній проблемі, а також застосуванні загальнонаукових та спеціально-наукових методів дослідження цілісної картини розвитку та можливих тенденцій подальшого функціонування інституту захисту персональних даних в Європейському Союзі.

Методологічну основу роботи склали філософські, загальнонаукові та спеціальні методи, які у своєму органічному поєднанні допомогли досягти виконання поставлених завдань. У роботі знайшли застосування сучасні методи наукового дослідження: діалектичний, функціональний, системно-структурний, порівняльно-правовий, моделювальний, логіко-семантичний та догматичний методи. Не були винятком і такі **методи**: аналізу і синтезу, дедукції та індукції, які використовувалися під час визначення особливостей механізмів правового регулювання захисту персональної інформації та дозволили виявити значення захисту персональних даних для підвищення ефективності внутрішнього ринку Європейського Союзу.

Окремі наукові результати дослідження були апробовані та опубліковані у межах наступних науково-практичних конференцій, круглих столів та семінарів:

– Правові засади захисту персональних даних у Європейському Союзі.(III міжнародна науково-практична конференція «Сучасні міжнародні відносини: актуальні проблеми теорії та практики – 2023»);

– Механізм правового регулювання захисту персональних даних в Європейському Союзі.(XVI Міжнародній науково-технічна конференція «ABIA-2023»).

Структура та обсяг дипломної роботи.

Структура роботи обумовлена її метою, завданнями та предметом дослідження. Дипломна робота складається із вступу, трьох розділів, якими охоплюються вісім підрозділів, висновків та списку використаних джерел (63 найменувань). Загальний обсяг дипломної роботи –75 сторінок, у тому числі список використаних джерел – 7 сторінок.

РОЗДІЛ 1
ПРАВОВІ ЗАСАДИ РЕГУЛЮВАННЯ ПЕРСОНАЛЬНИХ ДАНИХ У ЄВРОПЕЙСЬКОМУ СОЮЗІ

1.1. Поняття, ознаки та особливості персональних даних у Європейському Союзі

На сьогоднішній день сучасне суспільство та держава не можуть існувати та нормально розвиватися без використання інформаційних технологій, за допомогою яких акумулюється та обробляється різна інформація. Якщо раніше правових норм, що охороняють таємницю приватного життя, було достатньо для забезпечення прав людини, то сьогодні у зв'язку з використанням електронних баз даних про громадян державними та недержавними структурами проблеми збору, використання та розповсюдження інформації про людину набувають нового правового значення.

Поняття «персональні дані» тісно пов'язано з категорією «приватне життя» і тому може розглядатися як одна із форм реалізації права особи на повагу до її приватного, сімейного життя. Кордони між цими двома поняттями не завжди чітко помітні через відсутність конкретики у визначеннях. При цьому слід зазначити, що останнім часом спостерігається тенденція до закріплення на конституційному рівні права на захист персональних даних як самостійне, окреме від права на захист приватного життя. Враховуючи це, доцільно спочатку розглянути основні положення, які стосуються категорії «приватне життя».

Хоча загальноприйнятого трактування поняття «приватне життя» не існує, більшість теоретиків сходяться на тому, що терміном «приватне життя» позначаються: сфери життя людини, які вона не бажає робити надбанням інших (фізичних та юридичних осіб, органів та посадових осіб державної влади); «особистий розсуд» - свобода від зовнішнього керуючого впливу та контролю держави, громадських організацій, громадян у рамках

цих сфер та можливість контролювати їх[1, с. 220]. Інформаційна складова приватного життя включає:

будь-які фактичні дані про події, пов'язані з тілом людини: факти про хворобу особи, що становлять медичну таємницю; відомості про терапевтичне чи хірургічне лікування; фактичні дані про смерть та про долю людських останків;

фактичні відомості, що стосуються сімейного життя: персональні дані, крім загальнодоступних даних цивільного стану; про факти народження; про факти укладених шлюбів; про факти смертей; про секрет материнства та секрет усиновлення;

відомості про факти сексуального життя та почуття особи; про факти існування любовних відносин поза сім'єю або факт їхнього розриву;

відомості про внутрішні переконання індивіда: політичні та філософські погляди[2, с. 153-179].

Виведене на орбіту прав людини приватне життя набуває статусу права на приватне життя, яке дозволяє людині почуватися людиною[3]. Хоча категорія «приватне життя» не має нормативного юридичного змісту, правове регулювання встановлює межі її недоторканності і, отже, межі допустимого втручання .

Завдяки практиці правозастосування статті 8 Європейської Конвенції про захист прав та основних свобод людини (1950 р.) це поняття набуло чіткого нормативного трактування у заяві Європейського суду з прав людини (1992 р.): «Приватне (особисте) життя – це ємна категорія, якою неможливо дати вичерпне визначення. Кожна людина може розвивати це поняття і наповнювати його певним змістом. Було б недозволено обмежити поняття особистого життя «внутрішнім колом»... і виключити цілком зовнішній світ, який не входить до цього кола. Таким чином, поняття особистого життя з необхідністю включає право на розвиток взаємин з іншими особами та зовнішнім світом»[4, с. 62-66].

В свою чергу провідною складовою приватного життя, згідно з прецедентним правом Європейського Суду з прав людини, є персональні дані. Неправомірні дії по збору, збереженню, обробці, використанню або передачі персональних даних полягають у посяганні на право суб'єкта цих даних на не вміщення в його сфері приватного життя.

Терміном «машинні дані» або просто «дані» позначають інформацію, отриману при цифровій обробці або підготовлену в спеціальній формі для такої обробки. Причини спеціального виділення категорії «персональні дані», «персоніфіковані дані» із загального поняття «дані» пов’язані з тим, що такі дані є потенційно вразливими атрибутами сфери особистого життя людини. У правових документах ряду країн для позначення таких даних використовується термін «інформація, на підставі якої можна ідентифікувати особу» (інформація, яка дозволяє ідентифікувати особу)[5].

У цивільному судочинстві країн загального права використовується наступний принцип: публікація якогось факту особистого життя (персональних даних) визнається посяганням на сферу особистого життя, якщо було доведено, що «публікація цього факту була надзвичайно поганою з точки зору будь-якої розсудливої людини, наділеної звичайною чутливістю»[6, с. 53]. Сенс цього судового критерію в тому, «що закон не призначений для захисту надчутливих людей, оскільки кожна людина повинна до певної обґрунтованої межі відкривати своє життя для пильної уваги суспільства»[6, с. 53].

На підставі цього інформацію про індивідів поділяють на дві категорії: нейтральні персоніфіковані дані, до розкриття та поширення яких суб'єкт даних відносяться індиферентно; дані, циркуляцію яких суб’єкт даних прагне обмежити. Остання категорія отримала назву «персональні дані» та була кваліфікована як інформація, несанкціонований доступ або неналежне використання якої призводить до посягань на права суб'єкта даних. У визначеннях поняття «персональні дані» використовується, як правило, критерій ідентифікації даних суб'єкта на основі цих даних.

Проблема термінологічного визначення та розуміння поняття «персональні дані» є однією із найскладніших при роботі в цій сфері. Саме у визначенні містяться межі та критерії віднесення тієї чи іншої інформації до цієї категорії. Аналізуючи ті визначення, які містяться в національних та міжнародних правових актах, слід зазначити, що в основному вони збігаються.

Поняття «персональні дані» у широкому розумінні включає факти, повідомлення чи думки, пов'язані з певним індивідом і щодо яких розумно було б очікувати, що він вважає їх інтимними чи конфіденційними, і, отже, не бажає оприлюднювати їх або, принаймні, хоче обмежити їх звернення. З цього погляду «захист персональних даних» може вважатися свого роду аналогом терміна «інформаційна приватність» і в цьому сенсі передбачає право індивідів вирішувати, коли, яка та в якому обсязі інформація про них може повідомлятись іншим.

Поняття «відомості, що становлять таємницю індивіда» та «персональні дані» не є ідентичними. Персональні дані, такі як, наприклад, прізвище, ім'я, по-батькові, освіта, професія, особистої таємниці не містять, але дозволяють ідентифікувати ту чи іншу людину. Звідси визначення персональних даних у вузькому значенні – будь-які дані чи сукупність даних, що дозволяють ідентифікувати індивіда. Забезпечення захисту прав суб'єктів персональних даних передбачає не лише запобігання зловживанням при обробці інформації, а й захист права на інформаційне самовизначення.

Відповідно до загальний регламенту про захист даних у Європейському Союзі (General Data Protection Regulation, далі GDPR) персональні дані означають будь-яку інформацію, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати (суб'єкта даних)[7]. Особа, персональні дані якої обробляються, визначається як «суб’єкт персональних даних». Фактично людина має певні правомочності власника щодо своєї персональної інформації, але власником персональних даних де-юре наразі називатися не може.

Ключовим у вищенаведеному визначенні також є поняття «ідентифікована особа». Ідентифікованою особа вважається, якщо її можна безпомилково виділити серед інших. Зазвичай для того, щоб вважати особу ідентифікованою, необхідні її ім'я, прізвище, по батькові та реквізити документа, що посвідчує особу/цифровий номер, що присвоюється особі (наприклад, ідентифікаційний номер фізичної особи). Однак, за певних умов наявність меншої кількості інформації чи певного об'єму іншої інформації є достатніми для того, щоб ідентифікувати особу.

Поняття персональних даних включає будь-яку інформацію і не обмежується інформацією, яка відноситься до вузької інтерпретації приватного або сімейного життя людини. Персональні дані включають інформацію про людину та її будь-яку діяльність, включаючи професійну або громадську, контактну, фінансову, медичну, місце проживання або роботи, освіта, сімейна положення, інтереси та захоплення, відео, аудіозаписи або фотографії тощо.

Очевидно, що розуміння «персональності» тих чи інших даних пов'язано з ключовою їх властивістю – ідентифікацією (встановленням) фізичної особи. Виходячи з цього та ґрунтуючись на європейському розумінні, поняття «персональні дані» необхідно трактувати таким чином[8]:

дані набувають характеру персональних в тому разі, коли вони становлять інформацію про вже відому (встановлену, визначену, ідентифіковану) особу чи, принаймні, особу, яку можна встановити; особою, яку можна встановити, є така, що може бути визначена як на підставі вже наявних даних, так і за допомогою деякої додаткової інформації, отримання якої не вимагає істотних зусиль;

встановлення особи розглядається як процес, що може бути здійснений будь-яким суб'єктом, якому стали відомі або будуть відомі персональні дані в ході їх запланованого оброблення (інакше кажучи, якщо процес оброблення інформації передбачає ідентифікацію особи, то будь-який суб'єкт, що бере в

ньому участь зобов’язаний виконувати правові вимоги щодо захисту персональних даних);

процес встановлення особи повинен складатися з елементів, що описують людину в такий спосіб, який дає змогу безпомилково виділити її серед усіх інших людей (найяскравішим елементом такого опису є ім’я фізичної особи, або схожий ефект може забезпечити знання про те, що особа займає високу публічну посаду, наприклад Міністра);

не вважаються персональними даними ті дані, які не мають жодних ідентифікаторів (анонімні, знеособлені дані), що унеможливлює встановлення особи.

Через необмежене розмаїття особистої інформації встановити за допомогою нормативно-правових засобів певний визначений перелік персональних даних, що підлягають захисту, як не можливо, так і не доцільно. Проте використання окремих категорій персональних даних може створювати відчутний негативний вплив на людину, що вимагає їх чіткого визначення законом та встановлення особливих вимог щодо їх обробки. Ці категорії персональних даних загалом прийнято називати особливими, «чутливими», або такими, обробка яких загрожує правам і свободам суб’єктів персональних даних. Відповідно до Конвенції 108 (стаття 6), і Директиві про захист персональних даних (стаття 8) такі дані становить інформація про: расове або етнічне походження; політичні, релігійні або світоглядні переконання; здоров’я; статеве життя[9, с. 31-48].

Враховуючи те, що термінологія GDPR характеризується низьким рівнем формальної визначеності, що дозволяє зарахувати практично будь-яку інформацію до персональних даних доцільно виділити характерні ознаки відповідного поняття. Природу і сутність персональних даних визначають такі ознаки.

Першою ознакою персональних даних є те, що це відомості про особистісні властивості людини, тобто. очевидна їхня природна пов'язаність з людиною. Проте зв'язок із людиною та особистістю підкреслює лише родову

обумовленість інформації, її найбільш загальний характер. Персональність людини та особистості визначається вже індивідуальними ознаками конкретної особи, якими володіє кожен.

Таким чином, головною ознакою, що визначає зміст поняття «персональні дані», є те, що це будь-яка інформація, що відноситься до певної фізичної особи, тобто відомості, на підставі яких можна не тільки виділити людину з багатьох інших, але і точно її встановити (ідентифікувати). Такі індивідуальні ознаки конкретної людини відображаються у відомостях про неї незалежно від їхньої форми (алфавітної, графічної, цифрової, біометричної та ін.). Інакше висловлюючись, перша ознака підкреслює функціональне значення персональних даних.

Другою ознакою персональних даних є те, що це особливо важливі відомості про факти, події та обставини життя людини чи особистості. Не всі відомості про людину мають ціннісні характеристики, а лише ті, які визначають її зовнішні якості та діяльнісні (поведінкові) ознаки, а також внутрішні (сутнісні) властивості, у тому числі фізіологічні особливості, багато з яких подаються в біометричній формі (дактилоскопічна та геномна) інформація).

Життєво важливий характер персональних даних підкреслює їхню особливу цінність для конкретної людини, тому вони вимагають високого ступеня захисту. Людина приходить у світ із набором індивідуальних ознак, основою яких є історична природа, традиції, принципи, моральні імперативи. Від батьків індивід отримує генетичну інформацію як молекул ДНК, що зумовлює його індивідуальні фізіологічні і біологічні якості. Але володіючи набором персональних даних, фізична особа поводиться як людина, як конкретна особистість з певним рівнем освіти, культури, професійними навичками та креативною поведінкою. Такий особистісний потенціал є основою включення людини у соціум. «Персональні дані — це нитки, які пов'язують людину з суспільством та всіма його інституціями, насамперед із тими, які для себе обирає кожна окрема людина»[10, с. 6-8].

Отже, друга ознака наголошує на ціннісному значенні персональних даних. Персональні відомості людини є нічим іншим, як її візитною карткою у навколишньому середовищі, тобто. в умовах, в якій йому доводиться перебувати протягом відведеного йому періоду життя (і навіть після нього, якщо він залишить більший чи менший слід свого перебування на землі для наступних поколінь). Говорячи сучасною мовою, персональні дані людини – це персональний портал у навколишній дійсності.

Третьою ознакою персональних даних є конфіденційність відомостей про людину. Персональні дані - це інформація обмеженого доступу, але не таємниця, хоча за рівнем вимог режим захисту персональних даних не менш суворий, ніж режим комерційної або державної таємниці. На відміну від таємниці, конфіденційність персональних даних не має абсолютного характеру, оскільки за згодою суб'єкта відомості, їх складові можуть поширюватися і передаватися третім особам.

Розглянуті ознаки та особливості дозволяють більш точно відносити той чи інший набір даних до персональних.

1.2. Джерела та принципи правового регулювання персональних даних у Європейському Союзі

В даний час країни Євросоюзу особливу увагу приділяють системі захисту персональних даних, що виступає як невід'ємний елемент фундаментальних прав і свобод особистості. Цьому інституту присвячені відповідні правові акти, які закріплюють основні засади та механізми захисту персональних даних. Режим забезпечення захисту персональних даних є стратегічною метою Європейського Союзу. Це пояснюється тим, що Європейський Союз, як один із головних гравців на міжнародній арені, є першочерговим об'єктом для негативних кібервпливів, що вимагає вживання своєчасних, адекватних та ефективних заходів протидії, у тому числі

вживання дієвого та комплексного законодавства та інших правових механізмів захисту персональних даних .

Спочатку законодавчу основу в країнах Європейського Союзу у сфері захисту персональних даних утворювали міжнародні інструменти – Рамкові принципи ОЕСР у сфері захисту недоторканності приватного життя та транскордонної передачі персональних даних 1980 р. та Конвенція Ради Європи про захист фізичних осіб при автоматизованій обробці персональних даних, відкрита для підписання 1981 р[11, с. 512]. Дані правові акти закріплювали права на захист персональних даних, особливості реалізації механізмів захисту персональних даних. З розвитком інформаційних та комунікаційних технологій в ЄС було взято курс на формування власних більш докладних внутрішніх правил у цій галузі, які динамічно змінюються та удосконалюються.

У процесі формування та розвитку правове регулювання захисту персональних даних у Європейському Союзі пройшло чотири етапи. Кожен із цих етапів має характерні особливості і, зокрема, пов'язаний із впровадженням у правову систему Союзу певних нормативних актів, що заповнюють прогалини у правовому регулюванні та відповідають на існуючі виклики та ризики для персональної інформації. Прийняття цих актів обумовлено різними причинами політичного, економічного, технологічного, соціального характеру.

Перший етап має часові рамки з 1995 по 2001 рр., другий етап – з 2002 по 2009 рр., третій – з 2010 по 2018 рр., четвертий етап триває з травня 2018 року до теперішнього часу. Початком формування правового регулювання захисту персональних даних у ЄС слід вважати ухвалення у 1995 р. Директиви 95/46/ЄС – першого загальнообов'язкового правового акта, що заклав основи захисту персональних даних фізичних осіб у Європейському Союзі.

Другий етап характеризується прийняттям документів у специфічних сферах, які не підпадали під дію Директиви 95/46/ЄС, зокрема, що

встановлюють правила обробки персональних даних та захисту конфіденційності у секторі електронних засобів зв'язку (Директива 2002/58/ЄС); правила обробки персональних даних інститутами, органами та агентствами Союзу та установи на рівні ЄС незалежного Європейського Уповноваженого із захисту даних (Регламент (ЄС) ? 45/2001); а також створення Європейського агентства з мережевої та інформаційної безпеки (Регламент (ЄС) ?406/2004).

Третій етап характеризується закріпленням права на захист персональних даних як фундаментального та невід'ємного права людини на рівні первинного права ЄС – в установчих Договорах, зокрема, у статті 16 Договору про функціонування Європейського Союзу, у статті 39 Договору про Європейський Союз та у статті 8 Хартії Основні права Європейського Союзу. Норми захисту даних, закріплені у цих документах, стали базою для розробки та впровадження в правову систему ЄС Загального Регламенту захисту даних.

Сучасний етап формування механізму правового регулювання захисту персональних даних ЄС починається з другого десятиліття 21 століття. Він пов'язаний із набранням чинності 2018 р. на території ЄС Загального Регламенту із захисту даних (Регламент (ЄС) 2016/679), який замінює та скасовує Директиву 95/46/ЄС, та Директиви (ЄС) 2016/680 , яка встановлює

правила про захист фізичних осіб щодо обробки персональних даних компетентними органами з метою запобігання, розслідування, виявлення або переслідування за скоєння злочинів або виконання кримінальних покарань, яку кожна держава-член ЄС імплементує в законодавство та зобов'язана застосовувати на своїй території з 6 травня 2011 року[12].

Аналіз документів свідчить, що базовими принципами, на яких на сьогодні базується правовий захист персональних даних у Європейському Союзі, є:

принцип персоноцентризму (система захисту персональних даних утворена, насамперед, для служіння людині),

принцип екстериторіальності (володільці персональних даних (контролери) незалежно від національності чи місця проживання фізичних осіб повинні поважати їх основні права і свободи);

принцип субсидіарності (будь-яка обробка персональних даних у ЄС повинна відбуватись відповідно до законодавства однієї з держав-членів; повноваження володільця персональних даних (контролера), створеного в державі-члені ЄС, повинні визначатися національними законодавствами; держави-члени за власним бажанням визначають ризики для прав і свобод суб'єктів даних у своєму законодавстві).

Також у різних документах закладено механізми зв'язку права на захист персональних даних з правом на невтручання в особисте життя. Рівень захисту прав і свобод фізичних осіб при обробці цих даних повинен бути однаковим у всіх державах-членах для усунення перешкод на шляху передачі персональних даних[13, с. 197].

Окрема увага приділяється принципам обробки персональних даних. Захист даних фізичних осіб повинен застосовуватись як до автоматизованої обробки даних, так і до ручної обробки, а масштаби такого захисту не повинні залежати від використовуваних методів. Відступ від заборони обробляти конфіденційні категорії даних може бути виправдано суспільним інтересом в таких сферах як охорона суспільного здоров'я і соціальний захист, наукові дослідження та урядова статистика тощо [14, с. 30-44].

Основні принципи Вівіан Редінг обробки персональних даних у Європейському Союзі наведено в таблиці 1.1.

Таблиця 1.1.

Основні принципи обробки персональних даних у ЄС

Принцип	Сутність
законність, справедливість і прозорість	персональні дані повинні оброблятися законно, справедливо і в доступній формі по відношенню до суб'єкта даних
цільове обмеження	збиратися для певної, конкретної і законної мети і не піддаватися додатковій обробці, яка несумісна з цією метою; подальша обробка для цілей архівації, з метою наукових, дослідницьких, історичних і статистичних цілей не може бути несумісною з початковою метою

зведення до мінімуму даних	бути адекватними і обмежуватися тими даними, які відповідають і необхідні для досягнення цілі, для яких вони обробляються
точність	бути точними і, при необхідності, постійно підтримуватися в актуальному стані; неточні персональні дані, з урахуванням цілі, для якої вони обробляються, слід видаляти або виправляти без затримки
обмеження зберігання	зберігається у формі, що дозволяє ідентифікувати суб'єкта даних не довше, ніж це необхідно для цілі, для якої вони обробляються; персональні дані можуть зберігатися протягом тривалішого періоду виключно для цілей архівації, інтересів наукових, дослідницьких, історичних і статистичних цілей
цілісність і конфідеційність	обробляються так, щоб забезпечити належний захист персональних даних, включаючи захист від несанкціонованої або незаконної обробки, випадкової втрати, знищення або пошкодження, з використанням відповідних технічних або організаційних заходів

Під обробкою персональних даних Директива ЄС розуміє будь-які операції з персональними даними або їх сукупність, включаючи збір, запис, систематизацію, зберігання, зміну, передачу та розкриття. Основним принципом, на основі якого повинні діяти контролери персональних даних, визнана об'єктивна та неупереджена обробка персональних даних, завдяки якій суб'єкт даних має отримати інформацію про те, хто саме є контролером даних, мету їх обробки та використання, а також надати згоду на використання персональних даних.

28 січня 2014 року в День захисту персональних даних, що відзначався в Європі, віце-президент Європейської комісії, Уповноважений (Єврокомісар) з питань юстиції Вівіан Редінг виступила з промовою, в якій сформулювала вісім принципів захисту персональних даних, відповідно до яких має здійснюватися обробка персональних даних, як у державному, так і в приватному секторах[15, с. 234-240].

Принцип 1: Європа має створити надійну правову базу для захисту персональних даних, яка б могла стати для всього світу зразком і стандартом. А якщо ні, то інші країни нас випередять і нав'яжуть свої стандарти Європі.

Принцип 2: Правова база захисту персональних даних не повинна проводити різницю між приватним та державним секторами. Громадяни просто не зрозуміють таку різницю в умовах, коли державний сектор збирає, зіставляє, а іноді навіть хоче продавати персональні дані.

Принцип 3: Під час підготовки законодавства про захист персональних даних необхідно проводити його громадське обговорення, оскільки воно стосується громадянських свобод в онлайн-середовищі. Захист персональних даних має бути темою кампанії з інформування громадськості, спрямованої на спільне обговорення питання громадянами, правозахисними групами, комерційними організаціями та державними органами.

Принцип 4: Нічим не обмежене перехоплення електронних комунікацій є неприйнятним. Збір даних на користь спостереження і контролю має бути націленим і обмеженим рамками, пропорційними цілям такого спостереження.

Принцип 5: Закони мають бути чіткими і мають підтримуватися їх актуальність. Не можна, щоб країни-члени Євросоюзу, встановлюючи рамки сучасних програм контролю та спостереження, покладалися на застарілі закони, розроблені в іншу технологічну епоху. Такі закони мало чи взагалі нічого не говорять громадянам про те, що насправді відбувається.

Принцип 6: Винятки з посиланням на інтереси національної безпеки слід використовувати економно. Вони мають бути саме винятками, а не правилом. Необхідність захисту національної безпеки може виправдати особливі норми. Однак не все, що стосується зовнішніх зв'язків, є питаннями національної безпеки. Інший підхід підриває легітимність законів, які мають життєво важливе значення для нашої безпеки.

Принцип 7: Судовий нагляд необхідний для того, щоб уникнути занадто сильного розгойдування маятника в різні боки. Нагляд з боку
виконавчої влади – справа хороша. Парламентський контроль необхідний. Судовий нагляд є ключовим чинником.

Принцип 8: Законодавство про захист персональних даних слід застосовувати незалежно від громадянства зацікавлених осіб. Застосування різних стандартів залежно від того, чи є особа громадянином цієї країни, немає сенсу через відкриту природу інтернету[15, с. 234-240].

Іншими принципами є такі: законність і зрозумілість цілей збору та обробки персональних даних; точна відповідність обсягу запитаних персональних даних цілям їх використання; зберігання персональних даних не більше терміну, обумовленого цілями їх обробки; можливість доступу суб’єкта інформації до своїх персональних даних для їх зміни, уточнення або видалення; створення необхідних технічних та організаційних заходів для забезпечення захисту даних від незаконної або несанкціонованої обробки, випадкової втрати або руйнівного використання.

Таким чином, на сучасному етапі право на захист даних особистого характеру декларується на рівні первинного права ЄС, а правове регулювання суспільних відносин, пов'язаних з опрацюванням персональних даних, здійснюється найновішими документами: Регламентом (ЄС) 2016/679, Директивою (ЄС) 2016/680 , Регламентом (ЄС) 2018/1725, Директивою (ЄС) 2016/11481 та актами, прийнятими на підставі них інститутами та органами ЄС; правовими актами Союзу, які залишаються чинними, зокрема, Директивою 2002/58/ЄС; міжнародними угодами, укладеними інститутами та органами ЄС з третіми країнами та міжнародними організаціями з питань міжнародної передачі персональних даних.

З розвитком інформаційних технологій, що зумовлює активний збір та обробку персональних даних, як у сфері приватного життя, так і в суспільних відносинах фізичних осіб організаціями та владними структурами, помітно змінюється зміст правової категорії «персональні дані». Ця категорія стрімко вивається за межі приватного життя, й у європейському праві на початку XXI століття починається формування самостійного інституту захисту персональних даних, заснованого на праві на захист персональних даних як одного з основних прав людини. До цього право на захист персональних даних розглядалося у рамках інституту права на недоторканність приватного життя.

1.3. Значення захисту персональних даних для підвищення ефективності внутрішнього ринку

У світлі багатьох впроваджуваємих заходів Європейським Союзом внутрішній ринок ЄС перебуває у постійній динаміці та розвитку. Зокрема, внутрішній ринок відіграє провідну роль у реагуванні на цілу серію викликів, з якими останнім часом стикається ЄС. Серед них – прискорення впровадження нових технологій. Справді, без мобільного інтернету, онлайн-платформ та інших цифрових винаходів важко уявити сучасне життя. Масштаби та наслідки сучасного етапу інформатизації суспільства носять революційний характер.

В 2020 році як ніколи люди відчули незамінність цифрових технологій, насамперед Інтернету. Усім очевидно, що пандемія коронавірусу радикально змінила значення цифровізації. Цифрові технології тепер стали ще більш невід'ємною частиною різних сфер нашого життя: роботи, навчання, спілкування, придбання товарів та послуг від сфери охорони здоров'я до культури. Вона також продемонструвала вкотре вразливість цифрового простору, а отже, і сфери прав людини, і необхідність ще детальнішого її правового регулювання.

Двома із десяти пріоритетних напрямів діяльності Європейської комісії, проголошених її головою Ж.-К. Юнкером виступали більш поглиблений і рівноправний (справедливий) єдиний внутрішній ринок та забезпечення простору правосуддя та основних прав людини, заснованих на взаємній довірі[16].

Внутрішній ринок, будучи центром європейської інтеграції, є одним з основних досягнень ЄС і одним з головних активів в умовах глобалізації. Він за підсумками існування ЄС характеризується: спрощеним доступом споживачів до численних товарів та послуг із пільговими цінами; перевагами підприємств від ринку збуту та підтримки конкуренції; високими вимогами до безпеки та захисту навколишнього середовища. Реалізація економічних

свобод внутрішнього ринку сприяє появі нових можливостей для громадян, працівників, підприємців, підприємств та споживачів.

Однак на даний момент потенціал внутрішнього ринку не використовується в повній мірі через незнання права ЄС або його незастосування або неналежне застосування державами-членами; зберігається також багато економічних, правових та інших перешкод. До того ж правове регулювання внутрішнього ринку має приводиться у відповідність до реалій сьогодення, до яких належать різні інноваційні ідеї та нові організаційні форми підприємств. Підвищення ефективності внутрішнього ринку можливе за допомогою усунення правових і неправових перешкод, що все ще залишилися, наприклад, на шляху реалізації свободи руху товарів і послуг.

Останнє було неодноразово проголошено як пріоритетний напрям у щорічних оглядах зростання. Також, спираючись на переваги внутрішнього ринку, досягнуті протягом останніх років, Комісія вжила цілий комплекс заходів, щоб створити споживачам та підприємствам нові перспективи. Зокрема, у 2015 році вона розробила Стратегію єдиного цифрового ринку, в якій прийнято заходи стимулювання економічного зростання та збільшення кількості робочих місць, а також поглиблення співпраці в рамках внутрішнього ринку та підвищення рівня його справедливості[17].

Спільне використання персональних даних часто виступає нарівні з товарами та послугами як складова економіки спільного споживання, яка, у свою чергу, є одним із інструментів досягнення цілей, визначених Комісією у Стратегії для єдиного ринку 2015 року. Захист персональних даних постачальників та споживачів має велике значення для забезпечення та підтримки довіри різних суб'єктів, що діють на ринку. Таким чином, виходячи з аналізу Стратегії, одним із інструментів підвищення ефективності єдиного внутрішнього ринку є захист персональних даних, який, у свою
чергу, є невід'ємною частиною простору правосуддя та основних прав людини.

Захист персональних даних як цифрової сфери приватного життя - основна потребність людини в сучасному інформаційному суспільстві. З одного боку, цифрова трансформація надає нові можливості для розвитку економічних свобод внутрішнього ринку, а з іншого — при цьому має сприяти тому, щоб люди мали доступ до своїх персональних даних, могли їх використовувати та керувати ними абсолютно безпечно на території всього ЄС незалежно від свого місцезнаходження та місцезнаходження персональних даних. І це справді взаємопов'язані аспекти процесу цифровізації. Не варто забувати, що і саме створення та розвиток внутрішнього ринку призвело до істотного збільшення обсягів персональних даних, що транскордонно переміщуються в рамках ЄС. Персональні дані завдяки сучасним технологіям переміщуються вільно, приватні компанії та органи державної влади використовують персональні дані в небувалих раніше масштабах, фізичні особи все більше і більше надають доступ до своїх даних[18, с. 442].

Якщо люди будуть впевнені в тому, що при передачі своїх персональних даних у будь-якій державі-члені ЄС гарантовано дотримуватимуться норми права ЄС про захист персональних даних, то довіра до інновацій, заснованих на даних, лише зростатиме. І в цьому проявляється позитивний аспект співвідношення принципу поваги до прав людини та реалізації економічних свобод внутрішнього ринку ЄС. Але не слід забувати і про негативне: захист прав людини може бути підставою для обмеження економічних свобод внутрішнього ринку як передбаченим у Договорі про функціонування Європейського Союзу (далі – ДФЄС), так і у формі імперативних вимог спільного інтересу, які відбилися у практиці Суду ЄС. Важливо відзначити, що право на захист персональних даних не є абсолютним правом, і має бути збалансовано щодо інших основних прав у відповідності до принципу пропорційності.

В 2020 році Комісія на виконання Європейської стратегії для даних представила проект Регламенту з Європейського управління даними («Акт

про управління даними»)[19]. Цікаво, що правовою основою для ухвалення такого регламенту, на думку Комісії, є стаття 114 ДФЄС. Це вкотре підтверджує, що заходи ЄС у сфері, зокрема, захисту персональних даних відносяться до заходів щодо створення та функціонування внутрішнього ринку ЄС. Цифрова політика належить до спільної компетенції ЄС та держав-членів. Відповідно до пункту 3 статті 4 ДФЄС ЄС має право проводити заходи у сфері технологічного розвитку, у тому числі щодо розробки та реалізації програм, за умови, що здійснення такої компетенції не перешкоджатиме державам-членам здійснювати свою власну компетенцію.

Економічний чинник став однією з головних причин ухвалення Загального Регламенту захисту даних. Той факт, що Регламент встановлює єдині правила для всіх держав-членів, призведе, за оцінками Європейської комісії, до економії близько 2,3 млрд. євро на рік для європейської економіки[20].

Враховуючи важливість малого та середнього бізнесу для економіки, у Регламенті передбачені особливі правила для таких категорій суб'єктів господарювання. Так, зобов'язання, пов'язані з обробкою персональних даних, залежить від обсягу підприємства. Наприклад, мале підприємство може у випадках, зазначених у ст. 37, не призначати співробітника захисту даних. Зобов'язання (ведення обліку операцій обробки, документування категорій одержувачів даних тощо), згадані у п. 1 та 2 ст. 30, не застосовуються до підприємства чи організації, у якій працевлаштовано менше 250 осіб тощо.

Для ефективного функціонування підприємств за умов розвитку великих даних (Big Data) потрібно використання спеціальних механізмів, які забезпечують захист персональних даних «за умовчанням». Це означає, що контролер повинен впроваджувати відповідні технічні та організаційні заходи як під час визначення засобів обробки, так і під час самої обробки для ефективної реалізації принципів захисту даних, і тому в Регламенті велика

увага приділяється не тільки правовим, а й технічним аспектам захисту даних.

Таким чином, прийняття Регламенту та Директиви — великий крок уперед на шляху дотримання права фізичної особи на захист персональних даних, що має позитивно вплинути на функціонування внутрішнього ринку ЄС.

Варто згадати також і щорічний звіт щодо функціонування внутрішнього ринку, опублікований у травні 2021 року[21]. У цьому звіті Комісія наголошує, що ефективне та етичне використання даних матиме ключове значення для майбутньої конкурентоспроможності Європи, а Європейська стратегія для даних спрямована на створення єдиного європейського простору даних, у якому персональні та інші дані знаходяться у безпеці, а підприємства також мають простий доступ до високоякісних промислових даних. З точки зору Комісії Європейська стратегія управління даними покращить доступ до даних і підвищить довіру до обміну персональними та іншими даними, а також знизить транзакційні витрати, пов'язані з обміном даними.

Технологічний прогрес та глобалізація створили багато різних проблем при реалізації фізичними особами свого права на захист персональних даних, з якими, звісно, зіткнулися і в державах-членах ЄС, і в самому ЄС у цілому. Захист персональних даних є невід'ємною частиною правового регулювання в рамках інформаційного суспільства. Наслідком цього є необхідність постійного вдосконалення механізму правового регулювання ЄС у цій сфері.

Проведене дослідження демонструє, що інститути ЄС досить у короткі терміни здатні вживати цілий комплекс, з першого погляду логічних, послідовних, взаємопов'язаних, швидше за все, своєчасних, надзвичайно необхідних, затребуваних та виправданих заходів для вдосконалення правового регулювання внутрішнього ринку, створюючи єдиний цифровий, як відповідь на низку викликів, з якими стикається весь світ та Європа, зокрема. Хоча, звичайно ж, лише в процесі застосування на практиці

прийнятих правових актів можна буде більш впевнено оцінювати досягнення поставлених цілей ЄС.

Необхідно, щоб внутрішній ринок постійно адаптувався до умов цифрової революції та глобалізації, що швидко змінюються. Нова ера цифрових інновацій крім маси позитивних аспектів створює виклик, для захисту прав споживачів та безпеки. Пандемія Covid-19 продемонструвала важливість спільного розгляду промислової політики ЄС та єдиного внутрішнього ринку, щоб якісніше враховувати економічні та соціальні наслідки збоїв у вільному переміщенні товарів, послуг та людей для діяльності компаній, а також щоб краще розуміти складні взаємозв'язки між ними у різних регіонах та секторах[22, с. 216].

Інститути ЄС неодноразово і навіть багаторазово звертали увагу на взаємозв'язок, а точніше важливість забезпечення захисту персональних даних для ефективного функціонування єдиного цифрового ринку і, отже, внутрішнього ринку в цілому. Як ілюстрування позитивного аспекту співвідношення захисту прав людини і основних свобод, з одного боку й економічних свобод внутрішнього ринку, з іншого, очевидно, посилення забезпечення захисту персональних даних сприяє підвищенню ефективності реалізації останніх. Для того, щоб єдиний цифровий ринок функціонував належним чином, необхідно, щоб свобода переміщення персональних даних до ЄС не була ні обмежена, ні заборонена через причини, пов'язані із захистом фізичних осіб у зв'язку з обробкою їх персональних даних.

РОЗДІЛ 2
МЕХАНІЗМ ПРАВОВОГО РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ЄВРОПЕЙСЬКОМУ СОЮЗІ

2.1. Основи захисту персональних даних у законодавстві Європейського Союзу

В даний час країни Євросоюзу особливу увагу приділяють системі захисту персональних даних, що виступає як невід'ємний елемент фундаментальних прав і свобод особистості. Цьому інституту присвячені відповідні правові акти, які закріплюють основні засади та механізми захисту персональних даних.

Спочатку законодавчу основу в країнах Європейського Союзу у сфері захисту персональних даних утворювали міжнародні інструменти – Базові принципи ОЕСР у сфері захисту недоторканності приватного життя та транскордонної передачі персональних даних 1980 р.[23] та Конвенція Ради Європи про захист фізичних осіб при автоматизованій обробці персональних даних 1981 р[24]. У цьому документі вперше викладено ключові принципи обробки персональних даних, права особи у зв’язку з обробкою її персональних даних, базові норми щодо транскордонної передачі даних, а також передбачено створення консультативного комітету, до чиїх обов’язків входило проведення аналізу того, як застосовується Конвенція, та в разі необхідності підготування пропозицій щодо внесення змін до Конвенції.

Дані правові акти закріплювали права на захист персональних даних, особливості реалізації механізмів захисту персональних даних. З розвитком інформаційних та комунікаційних технологій в ЄС було взято курс на формування власних, більш докладних внутрішніх правил у цій галузі, які динамічно змінюються та удосконалюються. Як зазначає М. Бем «саме Європейський Союз сьогодні став локомотивом розвитку правового регулювання у сфері захисту персональних даних»[25].

Варто зазначити, що регулювання захисту персональних даних здійснюється між іншим у рамках трьох базових документів: Договору ЄС, Договору про функціонування ЄС та Хартії ЄС з прав людини.

В статті 39 Договору про ЄС зазначається: Відповідно до статті 16 Договору про функціонування Європейського Союзу та у відступ від параграфа 2 статті Рада приймає рішення, що встановлює правила щодо захисту фізичних осіб щодо обробки персональних даних державами-членами при провадженні діяльності, що входить до сфери застосування цієї глави, та про вільне переміщення таких даних. Дотримання цих правил знаходиться під контролем незалежних органів.

Сам Договір про функціонування ЄС у статті 16 містить такі положення[26]:Кожен має право на захист персональних даних, що належать до нього; Європейський Парламент та Рада, ухвалюючи відповідно до звичайної законодавчої процедури, встановлюють правила про захист фізичних осіб щодо обробки персональних даних інститутами, органами та установами Союзу, а також державами-членами при провадженні діяльності, що входить до сфери застосування права Союзу, та про вільне переміщення таких даних. Дотримання цих правил під контролем незалежних органів. Правила, прийняті на підставі цієї статті, не завдають шкоди спеціальним правилам, передбаченим у статті 39 Договору про Європейський Союз.

Ключове місце права на приватність серед спільних європейських цінностей було підтверджене і в Хартії основних прав ЄС від 7 грудня 2000 р[27]. У Хартію внесено як ст. 7, що гарантувала право на приватність, так і ст. 8, що встановлювала гарантії «Захисту відомостей особистого характеру». Ця стаття передбачає, що такі відомості «повинні використовуватися відповідно до встановлених правил для певних цілей і на підставі згоди зацікавленої особи або на інших правомірних підставах, передбачених законом». Крім того, ст. 8 гарантувала право на доступ до своїх персональних даних та право на їх виправлення, а також передбачала, що відповідний захист має підлягати контролю з боку незалежного органу[27].

У 1990 р. Рада Європейського Союзу ухвалила рішення щодо розробки проектів двох директив:

«базової» директиви про захист приватних осіб щодо обробки персональних даних, що визначає загальну регламентацію захисту даних;

«галузевої» директиви про захист приватності та персональних даних при передачі даних з використанням цифрових телекомунікаційних мереж зв'язку загального користування, зокрема, які працюють на базі протоколу зв'язку ISDN, та каналами цифрових мереж мобільного зв'язку громадського користування.

У процесі узгодження проектів виявилися серйозні розбіжності між країнами-членами ЄС щодо ступеня суворості правила отримання «згоди суб'єкта даних» та передачі персональних даних по телекомунікаційних лініях до третіх країн.

Остаточний текст «базової» директиви було опубліковано 1995 р., а 1996 р. було опубліковано секторальну директиву – про захист персональних даних. Директива 1996 р. втратила чинність після прийняття Директиви Європейського Парламенту та Ради Європейського Союзу 2002/58/ЄС від 12 липня 2002 р. щодо обробки персональних даних та захисту конфіденційності в секторі електронних засобів зв'язку (Директива про конфіденційність та електронні засоби зв'язку)[28]. Цього ж року було прийнято Директиву Європейського Парламенту та Ради Європейського Союзу 2002/22/ЄС від 7 березня 2002 р. про універсальні послуги та права користувачів щодо мереж електронних комунікацій та послуг (Директива про універсальні послуги)[29].

До недавнього часу Директива 95/46/ЄС Європейського Парламенту та Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року (далі – Директива) була не просто одним із найавторитетніших документів у сфері захисту персональних даних була, а й зразком для багатьох національних законів про захист персональних даних за межами ЄС.

Директива ЄС про недоторканність особистого життя та про електронні комунікації 2002/58/ЄС встановила ж конкретні вимоги щодо Інтернету, торкнувшись таких чутливих тем, як збереження даних, електронні повідомлення, що направляються «без попиту», використання фрагментів даних типу cookies, а також включення особистих даних до каталогів загального користування.

Загальні принципи, закладені в європейську директиву, аналогічні принципам 108 Конвенції Ради Європи та Керівним принципам ОЕСР. Вимоги директиви поширюються на всі типи обробки даних, за винятком операцій, що стосуються громадської безпеки, оборони та державної безпеки.

Директива передбачала високий рівень захисту даних, встановлюючи суворі обмеження щодо збору, використання та розкриття особистих даних. Дотримання вимог у кожній країні ЄС мав забезпечувати незалежний національний орган із наглядовими повноваженнями. Відповідно до вимог директиви, створювалася консультативна робоча група щодо однаковості застосовуваних національних заходів, а також заходів щодо захисту даних у третіх країнах, оскільки транскордонна передача даних до країн за межами ЄС дозволена лише за умови забезпечення країною-отримувачем адекватного рівня захисту.

Новаторською нормою, порівняно з Конвенцією 108 та Керівними принципами ОЕСР, була стаття 15, яка стосувалася «автоматичних рішень фізичної особи» та покликана вирішити проблему практики формування профілів користувачів[30, с. 58-65].

Варто зазначити важливий момент, що директиви, на відміну від Конвенції, мають обов'язкову юридичну силу для всіх країн-членів ЄС, які зобов'язані їх виконувати як рамковий законодавчий акт, що підлягає включенню до національного законодавства. Ця вимога забезпечила однакове ставлення до обробки особистих даних по всій території ЄС. Крім того, за рахунок наявності вимог до транскордонних потоків даних директива є документом, що надає значний вплив на інші країни світу.

Директива 1995 включала жорсткі вимоги по відношенню до комерційних підприємств. Внаслідок цього директива сприймалася не лише як вимога законодавчого закріплення недоторканності приватного життя, а й як загроза вільній торгівлі на тлі посилення глобалізації економіки. Зокрема, Міжнародна торгова палата наголосила на таких негативних наслідках введення в дію директиви:

високі витрати на забезпечення дотримання вимог директиви;

перешкоди впровадженню на ринок нових товарів та послуг;

підрив стимулів до інвестування.

Відношення міжнародної бізнес-спільноти до збалансованого захисту сфери приватного життя та персональних даних індивіда, з одного боку, та свободи транскордонних потоків даних, з іншого боку, можна узагальнити у 5 базових принципах, сформульованих у документах Міжнародної торгової палати:

важливість захисту приватності громадянина , включаючи захист проти неналежного використання інформації, пов'язаної з ним;

важливість ефективного обміну інформацією у розвитку сучасної міжнародної торгівлі та комерції;

право будь-якого бізнесу на вільні комунікації як усередині, так і поза його корпоративною структурою;

необхідність визнання всесвітньої залежності сучасних бізнес-комунікацій від транскордонних потоків даних;

необхідність гармонізувати засоби та заходи правового захисту приватності на міжнародній основі, при чому провести цю гармонізацію таким чином, щоб уникнути створення бар'єрів для міжнародних інформаційних потоків[31].

Ці принципи лягли в основу обов'язкових корпоративних правил, рекомендованих Міжнародною торговою палатою[32].

У першому звіті про реалізацію положень директиви 1995 р. Європейська комісія визнала, що надмірні обмеження, особливо спричинені відмінностями у тлумаченні вимоги адекватного рівня захисту, виявилися «дискредитуючими, як саму директиву так і правові норми Співтовариства загалом»[33, с. 123-126]. Тим не менш, ЄК було доручено оцінити та визначити рівень адекватності, що вона і зробила стосовно до Норвегії, Ліхтенштейну, Ісландії, Швейцарії, Канади, Аргентини, і за окремою угодою – США.

Всупереч наявності докладних і досить суворих вимог щодо захисту даних, а, можливо, і завдяки їм, так чи інакше, ця директива на глобальному рівні істотно вплинула на законодавство інших країн, при цьому не тільки в Європі. Вона послужила модельним законом для багатьох країн світу.

Попри те, що Директива була одним з найпрогресивніших документів у сфері захисту персональних даних у світі, технологічний прогрес та зростання обсягів автоматизованої обробки персональних даних зумовили виникнення нових викликів та проблем у цій сфері, які потребували додаткової правової регламентації. Зокрема, активний розвиток таких гігантів як «Фейсбук» чи «Альфабет» («Гугл») невідривно пов’язаний із відстежуванням активності користувачів та обробкою їхньої персональної інформації, що приводило до зростання їхньої власної прибутковості з одночасним збільшенням ризиків для суб’єктів персональних даних.

Через це з’явилася потреба в розробленні нового регулювання на рівні Європейського Союзу, яке б доповнювало і розширювало зміст Директиви, встановлювало додаткові гарантії для суб’єктів і вимоги до володільців і розпорядників персональних даних. Його розроблення стало можливим після укладення Лісабонського договору 2007 р., який вніс зміни в установчі договори ЄС. Як вже зазначалося Стаття 16 Договору про функціонування ЄС в редакції Лісабонського договору підтверджує, що «кожен має право на захист своїх персональних даних» і передбачала право Європейської Ради та

Парламенту встановлювати спільні правила обробки персональних даних для всіх держав – членів ЄС.

З урахуванням появи нових технологічних розробок – від сайтів соціальних мереж та «хмарних» методів обробки даних до послуг, прив'язаних до певного розташування користувача, та смарт-карток – Єврокомісія розпочала процес консультацій з питання перегляду положень Директиви про захист даних 1995 р. Від учасників процесу , що представляють усі групи зацікавлених сторін, надійшло кілька пропозицій.

У 2012 р. Європейська комісія виступила з комплексною пропозицією щодо реформування законодавства в галузі захисту даних, у тому числі з проектом регламенту із загальними вимогами до захисту особистих даних фізичних осіб у процесі їх обробки та проектом директиви, присвяченої питанню обробки особистих даних у контексті розслідування кримінальних. справ та кримінального переслідування.

Слід зазначити, що основу пропозиції становить проект регламенту, а не директиви. Йдеться не просто про зміну найменування документа – регламенти «сильніші» за директиви, оскільки мають силу закону в країнах-членах ЄС і підлягають прямому застосуванню, тоді як положення директив підлягають перенесенню до національного законодавства (країни-члени ЄС зобов'язані приймати законодавчі акти, що забезпечують реалізацію поставлених у директиві цілей, однак мають право обирати способи реалізації на власний розсуд).

Можливо, саме вибір типу нормативно-правового акта у 1995 р. для регулювання системи захисту даних призвів до недостатньої її гармонізації через різні способи імплементації у різних країнах ЄС. Запропоновані Єврокомісією проекти регламенту та директиви до їхнього офіційного прийняття та набрання чинності обговорювалися Європейським парламентом та Європейською радою.

Отже, дискусія щодо необхідності спільного загальноєвропейського регулювання обробки та захисту персональних даних з ініціативи

Європейської комісії призвела до прийняття документа, який встановив таке регулювання. Ним став Загальний регламент про захист персональних даних (англ. General Data Protection Regulation, GDPR, надалі – Регламент). Ухвалення на рівні ЄС відбулося 14 квітня 2016 р., а набрання чинності – 25 травня 2018 р. Цей документ складається з 11 розділів та 99 статей та супроводжується 173 коментарями[34]. Серед головних особливостей юридичної дії Регламенту можна виділити такі:

його дія поширюється на всіх громадян держав – членів ЄС, а також резидентів ЄС, незалежно від їхнього громадянства;

територіальна дія Регламенту поширюється на територію як держав – членів ЄС, так і держав, що входять до Європейської економічної зони (Норвегія, Ісландія та Ліхтенштейн);

Регламент – акт прямої дії, він загальнообов'язковий та застосовується державами – членами ЄС без додаткового ухвалення внутрішніх нормативних актів.

Говорячи про головні змістовні новели цього правового акта, якщо порівняти з Директивою ЄС, Регламент визначає правила гри для всіх учасників процесу захисту та обробки персональних даних – як суб'єктів, так і для володільців і розпорядників та контрольних органів у цій сфері. Зокрема, документ містить повний каталог прав суб'єктів персональних даних, які були раніше закріплені в Директиві та Хартії та розширює їхній зміст [35].

Щодо організацій, які проводять обробку персональних даних як володільці та розпорядники, то до них встановлено вимогу гарантувати, що в разі автоматизованої обробки персональних даних інформаційні системи та програмне забезпечення за замовчуванням забезпечують їхній захист (ст. 25), у разі необхідності призначати в організації уповноваженого із захисту персональних даних (ст. 37–39) та відповідного представника в ЄС, якщо організація зареєстрована та має центр ухвалення рішень за межами ЄС (ст. 27), положення щодо співпраці з контрольними органами держав – членів ЄС

у разі витоку персональних даних (ст. 31, 33–34), санкції, зокрема штрафи, за порушення правил Регламенту (розділ 8) та ін.[35].

Важливі також положення, які регламентують діяльність незалежних контрольних органів щодо захисту персональних даних, які повинні діяти в держав-членах ЄС, правила їх створення та компетенції (ст.ст. 51–59). Слід окремо відзначити правила транскордонної передачі персональних даних, що містяться в розділі 5, що де-факто розширює суб'єктну сферу дії Регламенту, спонукаючи організації з третіх держав, які ведуть діяльність з обробки особистої інформації громадян та резидентів ЄС, дотримуватися його положень[35].

Ухвалення Регламенту та насамперед його зміст, істотно змінили ландшафт захисту персональних даних у Європі та у світі. Як відзначав засновник «Фейсбуку» Марк Цукерберг у ході слухань у Сенаті США у квітні 2018 р., ухвалення Регламенту було правильним кроком і США теж варто обдумати ухвалення схожого правового акта[36, с. 283].

Дуже часто Регламент зазнає критики у зв'язку з начебто надмірною суворістю його положень, що ускладнює обробку персональних даних у комерційній, творчій, науковій та інших сферах. Водночас європейські експерти слушно наголошують, що цей акт «створює єдині узгоджені правила захисту персональних даних для всього Європейського Союзу, встановлюючи простір юридичної визначеності, з якого мають користь як суб'єкти економічної діяльності, так і фізичні особи – суб'єкти персональних даних»[37, с. 34].

Таким чином Регламент враховує усі останні тенденції в системі захисту персональних даних в Європі і світі та постає станом на сьогодні дороговказом щодо шляхів реформування національного законодавства у сфері захисту персональних даних. Сама динаміки змін правового регулювання захисту персональних даних у Європейському Союзі, дозволяє говорити про те, що європейський підхід до регулювання питань про право на захист персональних даних ґрунтується на розумінні цього права як одного

з фундаментальних прав людини, що живе у сучасному інформаційному суспільстві. Багато дослідників вказують на те, що в рамках права ЄС на даний момент сформувалася комплексна галузь інформаційного права, за допомогою норм та принципів якої здійснюється регулювання різноманітних суспільних відносин щодо використання різної інформації, у тому числі особистого характеру.

2.2. Право на захист персональних даних у практиці Суду Європейського Союзу

Суд ЄС неодноразово наголошував на необхідності захисту основних прав людини, а також дотримання їх балансу в епоху цифрових технологій. Діяльність Суду Європейського Союзу щодо захисту персональних даних реалізується у формі висновків, які Суд ЄС надає з приводу преюдиційних звернень національних судів на запити осіб з приводу законності опрацювання персональних даних, строків доступу осіб з приводу законності опрацювання персональних даних, строків доступу осіб до інформаціп, що належить до персональних даних, забезпечення належноп безпеки зберігання персональних даних, заборони зібрання надмірноп кількості інформаціп про особу, а також щодо правильності запровадження у національне законодавство забезпечення вимог щодо «повноп незалежності» наглядов их органів, відповідальних за забезпечення запиту персональних даних. Усі вони спрямовані на недопущення «порушення захисту персональних даних» – порушення безпеки, що спричиняє випадкове чи незаконне знищення, втрату, зміну, несанкціоноване розкриття або доступ до персональних даних, які передано, збережено або іншим чином опрацьовано.

Слід зазначити, що позиції Суду ЄС у розмежуванні понять «повага приватного життя» та «захист персональних даних» зазнавали змін: спочатку Суд ЄС не виділяв право на захист даних як окреме право, але потім фактично визнав ці дві категорії самостійними, але «тісно

взаємопов’язаними»[38]. У рішенні у справі Schecke Суд ЄС пов'язав поняття права «на повагу до приватного життя з обробкою персональних даних»[39], яке, за твердженням Г. Занфір, є симбіотичним продуктом ст. 7 та 8 Хартії ЄС про основні права без чітко визначеного змісту[40, с. 114].

Особливу увагу слід приділити двом рішенням Суду ЄС, винесеним у квітні та травні 2014 р., які визначили подальший розвиток права на захист даних у правовій системі ЄС. Ці два рішення Г. Занфір розглядає як «privacy spring», зазначаючи, що ст. 7 (право на повагу до приватного життя) та ст. 8 (право на захист особистих даних) Хартії основних прав ЄС були ефективно застосовані в обох випадках[40, с. 114].

У першому рішенні у справі Digital Rights Ireland Суд ЄС визнав недійсною Директиву 2006/24/ЕС[41], яка передбачала зберігання персональних даних, включаючи дані про трафік та місцезнаходження або інших метаданих з метою розслідування, виявлення та судового переслідування серйозних злочинів. Суд ЄС дійшов висновку, що положення директиви виходять за межі мети «боротьби з міжнародним тероризмом з метою підтримки міжнародного миру та безпеки». Суд також ухвалив, що стандарт, встановлений Директивою, є розпливчастим і, отже, не може бути витлумачений як «суворо необхідний»[42]. Директива 2006/24/ЕС надавала довільний доступ до всієї інформації, забезпечуючи мінімальні гарантії захисту. Особлива значимість захисту даних була підкреслена Судом ЄС у рішенні по цій справі, в якому зазначено, що захист персональних даних відіграє важливу роль «у світлі основоположного права на повагу до приватного життя»[43].

Не менш важливим є кейс у справі Google Spain SL проти Agencia Espacola de Proteccion de Datos. У березні 2010 року громадянин Іспанії Костеха Гонзалес подав скаргу до Національного агентства захисту даних на газету La Vanguardia, компанію Google Spain та Google Inc. Гонзалес зажадав, щоб газета прибрала або змінила запис про провадження у справі про накладення у 1998 р. арешту на його майно, щоб ця інформація більше не

була доступна в Інтернет-пошуковиках. Гонзалес стверджував, що розгляд його справи повністю завершився кілька років тому, і тому ця інформація більше не повинна відображатися в Інтернеті. Агентство відхилило скаргу проти газети на підставі того, що публікація була юридично обґрунтована постановою уряду. Проте, воно підтримало скаргу проти Google, визнавши, що пошукові системи в мережі Інтернет також повинні дотримуватися законів про захист даних і зобов'язані вживати необхідних заходів щодо захисту особистої інформації.

На стадії оскарження Національний Вищий Суд Іспанії призупинив судове провадження та подав низку питань до Європейського суду щодо застосування Директиви ЄС 95/46 до пошукових систем у мережі Інтернет. Суд ухвалив, що пошукова система розглядається як «контролер» щодо «обробки» особистих даних при пошуку, індексуванні, зберіганні та розповсюдженні такої інформації. Крім того, він ухвалив, що для того, щоб гарантувати права конфіденційності та захисту особистих даних, оператори пошукових систем можуть бути зобов'язані видалити особисту інформацію, опубліковану веб-сайтами третіх осіб. Однак право суб'єкта цих даних на такий запит має бути збалансоване з інтересом широкого загалу до його особистої інформації.

Таким чином у другому рішенні «Google v. Spain» [44] Суд ЄС внаслідок тлумачення положень Директиви 95/46/ЄС та ст. 8 Хартії ЄС про основні права дійшов висновку, що законодавство ЄС про захист даних застосовується «ratione personae» до американської компанії Google Inc. внаслідок «нерозривного зв'язку» зі своєю дочірньою компанією Google Spain[44]. Крім того, Суд ввів у дію «право на забуття» («right to erasure»), згідно з яким фізичні особи можуть просити про видалення посилань, пов'язаних з їх ім'ям та відображаються на сторінці результатів пошукової системи Google.

У GDPR більш детально регламентовано «право бути забутим» (ст. 17), яке спочатку з'явилося у культовому рішенні Суду ЄС у справі «Google v.

Spain». Після цього рішення «right to be forgotten» стало частиною GDPR і, як зазначає Л. Едвардс, однією з його суперечливих положений[45]. Вже зараз очевидно, що положення ст. 17 досить розпливчасті і потребують подальшого розвитку на практиці Суду ЄС, а саме «право бути забутим» є частиною глобальної дискусії щодо збалансування різних прав та інтересів в Інтернеті.

Розглянуті два рішення Суду ЄС істотно вплинули на подальший розвиток законодавства та практики у сфері захисту даних. Через деякий час низка конституційних судів держав-членів ЄС «ефектом доміно» визнали неконституційними закони, прийняті на основі Директиви 2006/24/ЕС (Румунія[46], Словенія[47], Австрія[48]). Це підкреслює також і роль Суду ЄС, який виступає координатором серед держав — членів ЄС у тлумаченні норм про захист прав людини в цифрову епоху.

Незважаючи на те, що з моменту винесення «весняних» рішень Суду ЄС у справах Google та Digital Rights Ireland минуло вже майже десять років, відлуння цих рішень все ще чутно. Наприклад, компанія Google створила консультативну раду з права бути забутою, щоб «допомогти» своїм користувачам «орієнтуватися в питанні» про те, «як право однієї людини бути забутою має бути збалансовано з правом громадськості на інформацію»[49]. Google також створила спеціальну сторінку підтримки для користувачів, які хочуть бути забутими, і періодично публікує статистику за кількістю отриманих запитів.

Між іншим рішення у справі Digital Rights Ireland є гарним прикладом того, як національні суди та Суд ЄС можуть субсидіарно співпрацювати у сфері захисту даних. У зв'язку з цим національні суди та конституційні суди держав — членів ЄС покликані відіграти важливу роль у такому уважному застосуванні критеріїв, які розробляє Суд ЄС та ЄСПЛ.

Цікава також справа C-362/14 Max Schrems, яка стосувалася ухваленого Комісією рішення на підставі п. 6 ст. 25 Директиви 95/46, що дозволяє передавати персональні дані до третьої країни (у цьому випадку — до США). Це було можливо, оскільки Комісія вважала, що у США має місце адекватний

рівень захисту з огляду на національне право чи міжнародні договори. Передача персональних даних ірландською філією компанії «Фейсбук» серверам у США та прийнятність їхнього захисту були оскаржені в національному суді Ірландії. Це було, зокрема, пов'язане з оприлюдненням інформації про стеження, яке проводили розвідувальні служби США у 2013 році. У результаті Суд ЄС визнав відповідне рішення Комісії недійсним.

У 2016 році Суд ЄС продовжив (в рамках преюдиційних запитів) спрямовувати діяльність суддів національних судів щодо застосування та тлумачення Хартії. Так, при розгляді об'єднаних справ C-203/15 Tele2 Sverige AB та C-698/15 Tom Watson Суд вивчав законодавчі акти двох держав-членів ЄС, згідно з якими дані всіх передплатників та зареєстрованих користувачів про трафік та місцезнаходження, що стосуються будь-яких засобів електронного зв'язку, повинні зберігатися на загальних та недискримінаційних засадах. Суд дійшов висновку, що ці закони обмежують основні права на приватне життя та захист персональних даних. Ці обмеження не були визнані об'єктивно виправданими через їх численність, а також малий обсяг передбачених гарантій, навіть коли їх метою виступала боротьба з серйозними злочинами. Однак все ж таки подібна мета може бути підставою для зберігання таких даних за умови, що воно буде обмежене рамками необхідного. Тобто зберігатися можуть лише певні категорії даних щодо зазначених видів засобів зв'язку, дані конкретних осіб, а також протягом фіксованого терміну.

Таким чином, Суд неодноразово нагадував інститутам ЄС та державам-членам про їх обов'язок дотримуватись положень Хартії ЄС про основні права, що закріплюють право на захист персональних даних.

Також необхідно торкнутися рішення Суду ЄС, пов'язаного із застосуванням актів права ЄС, що гарантують захист персональних даних, до компанії, місце заснування та місце діяльності якої є різними. У справі C-230/14 Weltimmo однойменна компанія, зареєстрована в Словаччині, керувала веб-сайтом, орієнтованим на здійснення угод з нерухомим майном

на ринку Угорщини, та була особою, яка відповідає за обробку персональних даних рекламодавців. Вона ігнорувала запити останніх щодо знищення даних і була за це оштрафована угорською владою. Weltimmo вважала, що не може бути оштрафована на підставі права Угорщини, оскільки була заснована у Словаччині. Суд ЄС дійшов висновку, що поняття «установа» необхідно тлумачити у світлі цілей Директиви 95/46 щодо захисту даних. Не має значення, в якій державі-члені ЄС компанія була заснована, але важливо, в якій державі вона здійснює реальну та ефективну діяльність через постійну організаційну структуру. Суд ЄС ухвалив, що компанія Weltimmo здійснювала таку діяльність на території Угорщини і відповідно до неї правомірно стягнуто штраф на підставі права Угорщини.

Не без уваги варто залишити і справу C-511/18 - La Quadrature du Net and Others[50]. Велика палата Суду ЄС в 2020 році у двох взаємопов'язаних рішеннях встановила, що законодавство ЄС обмежує дію національного законодавства, яке зобов'язує постачальників послуг електронного зв'язку здійснювати загальну та невиборчу передачу даних про трафік та місцезнаходження користувачів службам безпеки та розвідки з метою забезпечення національного законодавства щодо безпеки.

Під час розгляду об'єднаних заяв Великобританії, Франції та Бельгії Суд ЄС спробував визначити законність національного законодавства, яке зобов'язує постачальників послуг електронного зв'язку передавати дані про трафік та місцезнаходження користувачів державним органам або зберігати такі дані в загальному чи невиборчому порядку з метою запобігання злочинам та забезпечення національної безпеки.

Суд встановив, що таке зобов'язання не лише перешкоджає захисту права на недоторканність приватного життя та конфіденційність персональних даних, але й суперечить принципу свободи вираження поглядів відповідно до статті 11 Статуту ЄС. При цьому Суд зазначив, що у випадках, коли збереження даних виправдане наявністю серйозної загрози національній або громадській безпеці, характер такого заходу має бути «суворо»

пропорційним до її мети. Крім того, Суд уточнив обсяг повноважень, наданих державам-членам Директивою про конфіденційність та електронні засоби зв'язку щодо збереження даних для вищезазначених цілей.

Отже принципи та гарантії, що викладаються у розглядах ЄСПЛ та Судом ЄС, не лише підкреслюють провідну роль європейської системи у розгляді справ, пов'язаних із захистом даних, а й у визначенні векторів майбутньої концептуалізації права на захист даних. Майбутнє права на захист даних багато в чому залежить від ЄСПЛ та Суду ЄС, яким належить домінуюча роль у тлумаченні цього права, збагаченні його новими елементами та подальшому впливі на розвиток прецедентної практики та законодавства у державах – членах Ради Європи та ЄС. Зміцнення захисту персональних даних безпосередньо впливає ефективність реалізації економічних свобод внутрішнього ринку.

2.3. Особливості імплементації правових актів Європейського Союзу у сфері захисту персональних даних державами-членами ЄС

В європейських країнах встановлені власні національні вимоги щодо обробки персональних даних, однак незважаючи на всі національні особливості, у різних правових системах використовувалися лише два принципово відмінні підходи.

Генеральний – полягав у прагненні створити єдиний і всеосяжний закон про захист сфери приватного життя і був пов'язаний зі спробами теоретичного обґрунтування якогось «загального та абсолютного права на невтручання в приватне життя». Деякі країни включили право на захист персональних даних до Конституції (Швеція, Бельгія, Греція, Нідерланди).

Секторний (або галузевий) – полягав у створенні спеціалізованих законів або для кожного типу зазіхань на сферу приватного життя, або для кожної галузі або сектору людської діяльності, яка є потенційним джерелом загроз для права людини на невтручання у її приватне життя. Секторний підхід передбачає, що нові «галузеві» закони приймаються в міру

накопичення прецедентної бази, що вказує на нове джерело загроз для сфери приватного життя. Це призводило до безсистемності, дублювання та суперечливості законоположень.

Вже наприкінці 1990-х років. експерти зазначали, що у чистому вигляді і той, і інший підходи виявилися непродуктивними. У переважній більшості країн сучасні національні системи правового регулювання обробки та використання персональних даних застосовують так званий змішаний принцип, який би мав певні аспекти «генерального» і «галузевого» підходів.

Національне законодавство у сфері захисту даних, як правило, складається з: базового або системотворчого закону; комплексу галузевих законів, які забезпечують захист персональних даних у різних контекстах. Регулюючими компонентами сучасних систем захисту персональних даних є також національний уповноважений орган (або система органів) захисту даних та корпоративні засоби захисту (саморегулювання у формі кодексів поведінки/практики). Національний орган (або органи) із захисту даних, як правило, наділяються реєстраційно-дозвільними, контрольно-наглядовими, арбітражними, експертними та методологічними функціями.

Хоча процедурні норми викладаються по-різному, відповідно до правової системи кожної країни, існує широка згода щодо цілей, які мають бути забезпечені цими нормами. Національні законодавства включають, як мінімум, такі принципи, зафіксовані в міжнародних документах:

відкритість – суспільство має бути поінформовано про наявність баз персональних даних, які знаходяться у розпорядженні урядових органів, організацій та установ;

можливість доступу суб'єкта даних до даних про себе та можливість коригувати неточні чи застарілі дані;

збір персональних даних та обсяг цих даних має бути обмежений відповідно до цілей збору;

обмеження використання – персональні дані повинні використовуватися тільки з метою, для яких вони збиралися;

обмеження розкриття – персональні дані можуть бути розкриті лише з законною метою та за згодою суб'єкта даних1;

безпека – дані повинні бути захищені від втрати, несанкціонованого доступу, знищення, використання або модифікації[51].

Національні закони включають, в цілому, схожий «реєстратор» суб'єктів інформаційних правових відносин, що виникають у процесі збору, зберігання, обробки, використання та передачі персональних даних.

Не викликає сумнівів, що з прийняттям GDPR правове регулювання захисту персональних даних у Європейському Союзі набуло нової фази розвитку. Виходячи з положень 8, 10, 12-14 Преамбули Регламенту GDPR держави-члени поставлені перед завданням забезпечення узгодженого та високого рівня захисту фізичних осіб незалежно від їх національної приналежності або місця проживання щодо обробки їх персональних даних поряд із забезпеченням вільного руху потоків персональних даних в рамках Євросоюзу.

Можливий шлях досягнення поставленої мети – інкорпорація основ регламенту в національне законодавство держав-членів. На думку розробників, це спричиняє забезпечення узгодженості введених вимог і обмежень, а також забезпечення правової визначеності та прозорості для суб'єктів господарювання, для надання фізичним особам однакового рівня юридично закріплених прав та обов'язків, уніфікованого підходу до визначення функціональних обов'язків контролерів та обробників; забезпечення належного моніторингу обробки персональних даних; запровадження рівнозначних санкцій за допущені порушення; забезпечення ефективної співпраці між наглядовими органами різних держав-членів.

У той же час Регламент надає можливість державам-членам приймати власні правила з великого кола питань, у тому числі для обробки особливих категорій персональних даних (sensitive data), а також встановлювати обставини, за яких обробка особливих категорій персональних даних,

незважаючи на надзвичайність ситуації та відсутність згоди суб'єкта буде визнана правомірною.

Передбачається, що правотворча діяльність держав-членів здійснюватиметься паралельно з правотворчою діяльністю Європейського Парламенту та Європейської Ради. Регламент застосовується у всіх країнах ЄС з тією самою юридичною силою, начебто вони були місцевими законами. При цьому держави-учасниці Євросоюзу мають ухвалити свої власні закони для реалізації GDPR, але вони можуть відрізнятися. Скажімо, за GDPR вік згоди на обробку персональних даних встановлено у 16 років, але кожна держава може встановити свій. Це зроблено з метою, щоб процеси всередині держави відповідали єдиним вимогам, встановленим в ЄС. У результаті кожна європейська країна, виходячи зі своїх національних особливостей і проблем, наголосила на певних умовах і сама визначає суворість покарання за порушення. Особливості національних законодавств країн-членів ЄС щодо регулювання захисту персональних даних представлено в додатку А[52].

5 травня 2017 року Федеральна рада Німеччини схвалила Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 i zur Umsetzung der Richtlinie (EU) 2016/680 o BundesdatenschutzgesetzBDSG (Федеральний закон про захист даних)[52]. Це перший національний стандарт, адаптований до положень GDPR. Водночас в Іспанії новий проект закону про захист даних, представлений у звіті Ради міністрів 7 липня 2017 року, містив 78 статей щодо адаптації та розвитку GDPR. На момент написання цієї роботи країни-члени ЄС імплементували GDPR у національне законодавство. Розглянемо особливості імплементації цього документу деякими державами-членами ЄС.

У Німеччині діє Федеральний закон про захист даних (Bundesdatenschutzgesetz - BDSG), який встановлює такі особливості та доповнення до GDPR:

Більш детальні вимоги до призначення співробітника, відповідального за обробку персональних даних (DPO), порівняно з GDPR: в організації має

бути призначений відповідальний співробітник, якщо понад 20 осіб здійснює автоматизовану обробку персональних даних або якщо обробка пов'язана з передачею та анонімізацією даних, дослідженні ринків, DPO мають бути надані наглядовому органу;

Прямо заборонено передавати пул персональних даних, отриманих без дозволу суб'єктів - у комерційних цілях або заподіяння шкоди суб'єктам;

Дозволено відеоспостереження у загальнодоступних місцях: державні органи мають право здійснювати з метою охорони життя та здоров'я громадян (для запобігання загрозам державній та громадській безпеці, кримінальних злочинів), якщо відеоспостереження необхідне для захисту законних інтересів та ці інтереси вищі, ніж право суб'єктів на охорону персональних осіб даних;

Дозволено обробку даних для скорингу перед укладенням договору, за умови: дотримання законодавства щодо застосування заходів захисту даних; розрахунок значення ймовірності відбувається на основі науково визнаної математико-статистичної процедури; адресні дані не використовувалися виключно для розрахунку значення ймовірності; у разі використання адресних даних суб'єкта було поінформовано про передбачуване використання цих даних до розрахунку значення ймовірності; процес скорингу задокументований та має інструкцію.

Вік надання згоди на обробку даних – 16 років;

Додаткова відповідальність: штрафи за порушення BDSG можливі до 50 000 євро; Позбавлення волі до 2-х років.

У Франції на додаток до GDPR діє оновлений поправками Закон ? 78-17 від 6 січня 1978 р. про обробку даних, файлів і свободи (Loi n° 78-17 du 6 janvier 1978 relative a l'informatique, aux fichiers et aux libertйs)[54]. Його основні особливості та доповнення до GDPR:

Персональні дані померлих осіб можуть бути оброблені, якщо суб'єкт даних не висловив свою відмову за життя;

Вік надання згоди на обробку даних – 15 років;

Будь-який суб'єкт має право зареєструватися в спеціальному регістрі — Bloctel і тим самим висловити відмову від рекламних дзвінків та листів. Така відмова діє 3 роки і може продовжуватися на той самий термін. При цьому якщо суб'єкт уклав договір з контролером — йому можна дзвонити, але після пропонувати якісь товари та послуги вже не можна, якщо його дані містяться в Bloctel;

Можна купувати маркетингові списки з даними у третіх осіб, якщо є відповідний дозвіл на передачу персональних даних від суб'єктів, які у списках і забезпечується належний захист даних;

У відносинах працівник-роботодавець не обов'язково отримання письмових згод на обробку персональних даних, оскільки це передбачається спочатку, тому: дозволено відстеження геолокації транспортних засобів, керованих співробітниками, якщо це здійснюється під час роботи, співробітники поінформовані про це; дозволено запис телефонних розмов співробітників, якщо це відповідає заздалегідь визначеній меті, наприклад, для навчання або оцінки якості обслуговування; дозволено вивчення робочої електронної пошти, якщо листи не мають позначки «особисте».

Додаткова відповідальність: позбавлення волі до 5 років; штраф для фізичних осіб до 300 000 євро; штраф для юридичних осіб до 1500000 євро.

У національному законодавстві Кіпру про персональні дані зараз головну роль відіграє Закон ? 125(I) від 16.10.2018 року. Ось його основні особливості та доповнення[52]:

Генетичні та біометричні дані не можуть бути оброблені з метою отримання медичного страхування та страхування життя, навіть якщо суб'єкт даних дав згоду;

Зобов'язання отримати консультацію та схвалення наглядового органу під час передачі спеціальних категорій персональних даних у третіх осіб, які перебувають в інших державах;

Використання відеоспостереження на робочому місці та біометричних даних працівників можливе виключно, якщо роботодавець може довести

необхідність проведення цих заходів або у тому випадку, коли для досягнення цілей контролю немає інших способів;

Використання cookie дозволено лише за згодою користувача, якому має бути надана чітка та вичерпна інформація про цілі обробки, за винятком випадків використання cookie, необхідних для надання послуг суб'єкту і без яких функціонування неможливе;

Додаткова відповідальність: позбавлення волі до 3 років та/або штраф у розмірі не більше 30 000 євро; позбавлення волі не більше 1 року та/або штраф не більше 10 000 євро; позбавлення волі до 5 років та/або штраф у розмірі не більше 50 000 євро.

В Іспанії діє Закон ? 3/2018 від 5 грудня 2018 року про захист персональних даних та гарантії цифрових прав — Ley Orgбnica 3/2018 de Proteccіyn de Datos Personales y garantna de los derechos digitales, в якому[52]:

надається можливість контролеру самостійно розібратися зі скаргою.У разі подання скарги на контролера або процесора до наглядового органу: наглядовий орган повідомляє контролера та відповідальну особу за обробку персональних даних вправі самостійно вирішити питання протягом двох місяців з моменту отримання такої скарги;

великої критиці піддалося положення закону у тому, що політичні партії вправі використовувати персональні дані, отримані з веб-сторінок та інших громадських джерел, реалізації політичної діяльності під час виборів. Після оскарження в конституційному суді цього положення було внесено правки і тепер політичні партії мають право обробляти політичні думки лише в тому випадку, якщо вони були вільно виражені людьми при здійсненні свого права на свободу вираження думок та своєї ідеологічної свободи;

є цілий розділ про гарантії цифрових прав, де йдеться про захист приватного життя у сфері праці, наприклад, про право на недоторканність приватного життя та право використання цифрових пристроїв на робочому місці, право на недоторканність приватного життя від використання пристроїв відеоспостереження та звукозапису на робочому місці та

використання систем геолокації при виконанні трудових зобов'язань. Крім того, в ній встановлено: право на свободу вираження поглядів та інформації, особливо щодо висловлювання думки в Інтернеті; наявність алгоритмів у соціальних мережах (та публічних ресурсах), що дозволяють виправити та видалити опубліковану інформацію; право на забуття у пошукових системах та соціальних мережах.

згоду на використання файлів cookie може вважатися отриманою на законних підставах, якщо на сайті хоча б мінімум інформації про використання надається за допомогою банера. Згодою буде однозначна дія суб'єкта, що вказують на згоду - наприклад, використання смуги прокручування або перехід за посиланнями на відвідуваному сайті;

вік згоди на обробку персональних даних починається після досягнення 14 років;

до кримінальної відповідальності (у формі позбавлення волі від 1 до 4 років та/або щоденного штрафу на строк від 12 до 14 місяців) може бути притягнута будь-яка особа, яка вчиняє дії з метою розкриття персональних даних без згоди суб'єкта: зламування електронної пошти або поштової скриньки, месенджера, іншого сховища; перехоплення телекомунікацій; використання технічних пристроїв для прослуховування, передачі, запису або відтворення звуку або зображень.

На території Королівства Швеція діють Закон про захист даних (2018: 218) та Регламент про захист даних (2018:219). Однак крім них також є і багато галузевих законів, які регулюють обробку персональних даних у різних сферах. Серед них, наприклад, можна виділити Закон про відеоспостереження (Kamerabevakningslag, 2018: 1200), Закон про кредитну інформацію (Kreditupplysningslagen, 1973: 1173), Закон про стягнення боргу (Inkassolagen, 1974: 182) (Yttrandefrihetsgrundlag, 1991: 1469), Закон про маркетинг (Marknadsfцringslag (2008: 486)), Закон про дані пацієнта (Patientdatalag, 2008: 355), Закон про електронні комунікації (Lag, 2003)[56].

Проте, незважаючи на те, що правове регулювання у Швеції роботи з персональними даними децентралізоване та має велику кількість нормативних актів, всі вони закріплюють на національному рівні прийняті норми GDPR та інших законів ЄС. Загалом шведське законодавство встановлює такі прикметні доповнення до GDPR:

Щодо персональних даних померлих осіб немає жодних юридичних відмінностей від живих. Інакше кажучи, якщо покійний встиг до смерті дати згоду на обробку своїх даних, вона зберігається в колишньому обсязі та правах;

Вік надання згоди на обробку даних 13 років;

Згода суб'єкта на використання файлів cookie може бути виражена через налаштування веб-браузера, але на сайті у будь-якому випадку має бути попередження про використання cookie.

Проведений аналіз особливостей національних та загальноєвропейських норм щодо захисту персональних даних свідчить, що вони знаходяться в центрі уваги з низки причин. По-перше, різке збільшення масштабів обробки персональних даних неминуче призвело до необхідності встановлення єдиних стандартів та норм збору та обробки даних. По-друге, право на захист даних було визнано на міжнародному рівні у прецедентних практиках Суду ЄС та ЄСПЛ.

На сьогоднішній день можна констатувати, що незважаючи на зусилля міжнародних організацій і держав, нині жодна держава або міжнародна організація не мають досконалої системи захисту персональних даних. Дійсно, кожен механізм, створюваний як на національному, так і на міжнародному рівнях, по-своєму порочний і обмежений і потребує постійного вдосконалення.

GDPR змінив підходи до захисту персональних даних: відтепер акцент зміщується із захисту даних корпоративного сектору на захист персональних даних, створення цифрового ринку, де роль ЄС у забезпеченні регулювання є

вирішальною. Персональні дані стали новим фактором виробництва та новою валютою змін.

РОЗДІЛ 3
ПЕРСПЕКТИВИ РОЗВИТКУ ПРАВОВОГО РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ЄВРОПЕЙСЬКОМУ СОЮЗІ

3.1. Аналіз актуальних правових проблем у сфері захисту персональних даних

На сьогоднішній день для ЄС характерний принципово новий підхід до захисту персональних даних, орієнтований на людину, та інноваційний, з точки зору управління персональними даними. Органи захисту налагоджують співпрацю на основі механізму «єдиного вікна» та використовують взаємодопомогу, зокрема, у транскордонному співробітництві щодо захисту даних. Існуючий механізм захисту відповідає концепціям сталого розвитку та цифрової трансформації, де людина є партнером держави та має право розпоряджатися власними даними як учасник цифрового ринку та власник ресурсу у формі персональних даних.

Варто зазначити, що новий механізм захисту персональних даних поки що неможливо оцінити на поточному початковому етапі впровадження в ЄС. Враховуючи необхідність впровадження механізму в усіх країнах ЄС, рівень адаптивності можна охарактеризувати як високий. Водночас фрагментарність реалізації законодавчих положень свідчить про необхідність підвищення рівня гнучкості.

Низка проблем виникає через особливості законодавства країн ЄС, які пов’язані з правами на захист персональних даних та правом на свободу вираження поглядів. Пріоритет прав відрізняється в межах ЄС, що призводить до розбіжностей щодо впровадження механізму захисту персональних даних. GDPR передбачає послідовність формування механізму захисту персональних даних. Це зумовлює фрагментарність реалізації правових норм. Як наслідок, бізнес (у тому числі транснаціональні компанії) стикається з проблемами впровадження інновацій, нових технологічних розробок, вирішення проблем у сфері кібербезпеки.

Таким чином, ситуація з розвитком механізмів захисту персональних даних є певною мірою нерівномірною, зокрема через те, що в окремих країнах, наприклад таких як Ірландії та Люксембургу працюють великі транснаціональні компанії. Органам захисту персональних даних ЄС потрібно залучати більші людські, фінансові та технічні ресурси, щоб механізми працювали ефективніше.

Інша проблема із захистом персональних даних стосується рівня гармонізації права на захист персональних даних та свободи вираження поглядів. Одні країни визначають пріоритет свободи вираження поглядів, інші – пріоритет захисту даних, зменшуючи від цього контроль в певних ситуаціях. Натомість в деяких країнах права збалансовані та оцінюються в конкретних ситуаціях. Правила захисту даних не повинні впливати на свободу вираження поглядів, особливо в публічних сферах діяльності.

Основною проблемою обробки персональних даних у період розвитку цифрових технологій є порушення прав та свобод людини, в тому числі порушення принципу інформаційного самовизначення особистості. Ця проблема є ключовою, складною та багатоаспектною. Розкриваючи її багатоаспектний характер, хотілося б відзначити, що сьогодні персональні дані постійно збираються та обробляються операторами в мережі Інтернет, цифрових додатках, мобільних пристроях тощо, проте фізичні особи часто ставляться неуважно до питання використання та витоку їх персональних даних. Відносини між суб'єктом персональних даних та оператором є відносинами економічної асиметрії, оскільки оператор має значні економічні переваги за рахунок володіння масивами великих даних.

Говорячи про таку «цифрову» категорію, як великі дані (big data), можна відзначити, що в підприємницькому обороті вони розглядаються не тільки з технічної, але і з комерційної точки зору, виступаючи активом. Великі дані є масивом різних даних, зібраних з доступних оператору джерел. Можна відзначити недостатнє правове регулювання великих даних, до

масивів яких потрапляють персональні дані, внаслідок чого можуть бути порушені права людини (наприклад, у разі витоку).

У цифровому середовищі операторами використовуються численні маніпулятивні практики збору даних, що впливають на споживачів, змушуючи їх погоджуватися на збір даних в обмін на доступ до послуг. Цю проблему можна позначити як проблему надання «вимушеної» згоди користувача на обробку персональних даних операторам, що займають домінуюче положення на ринку. Зловживання операторами привертає пильну увагу законодавців уже тривалий час.

Одним із останніх яскравих прикладів порушення прав людини операторами, які займають домінуюче становище на ринку, є справа про порушення компанією Facebook законодавства про персональні дані у 2019 р., в якому антимонопольний орган Німеччини визнав умови політики конфіденційності компанії зловживанням[57]. У зазначеній політиці конфіденційності було встановлено, що використання соціальної мережі Facebook, яка займає домінуюче становище на ринку, можливе лише в тому випадку, якщо користувачі дають свою згоду на об'єднання їхніх особистих даних з інших сервісів Facebook та сторонніх сайтів. В умовах домінуючого становища Facebook користувачі вимушено погоджувалися із такими умовами[57].

Оператори, що мають масиви цифрових даних, мають можливість впливати на реалізацію прав людини в цифровому просторі та на стан конкуренції на відповідному ринку. Аналізуючи зловживання операторів під час використання цифрових платформ і підкреслюючи необхідність запровадження для них обмежень, можна звернути увагу на іншу важливу проблему, саме проблему негативних наслідків через посилення контролю у сфері захисту персональних даних на стан конкуренції на ринку, а також на розвиток інновацій[58] .

Отже, станом на зараз існує багато нормативно-правових актів, які регламентують захист персональних даних. Разом з цим, проблема

неправомірних і несанкціонованих дій у сфері персональних даних залишається актуальною і повноцінно не вирішеною, як в юридичному, так і практичному аспекті, зокрема[59]:

більшість баз персональних даних у функціонуванні не є автономними, що суперечить вимогам міжнародних правових стандартів;

передача персональних даних за кордон не має реального організаційно-правового механізму;

для будь-якого бізнесу персональні дані – зручне і необхідне доповнення до всього того, що надається через Інтернет;

на багатьох ринках має місце незаконна торгівля цифрових носіїв з персональними даними;

продовжує функціонувати відповідна система збирання і продажу адресних списків персональних даних тощо.

Про ефективність застосування GDPR говорить статистика, оскільки за весь час функціонування за його порушення стягнуто чимало податків. Водночас ця статистика вказує на те, що в Європі все ще залишаються проблеми щодо захисту персональних даних. Тим не менш ефективний захист, запроваджений механізмом GDPR, у перспективі має призвести до значного покращення справ цій сфері.

Таким чином на даному етапі розвитку суспільства складно передбачити результати використання нових правових механізмів у галузі захисту прав і свобод людини, оскільки сфера обробки персональних даних нестабільна і має залежність від розвитку цифровізації, а також операторів, які вже зібрали масив даних і використовують його з метою отримання прибутку. Проблеми правового регулювання в сфері, що розглядається, не повинні бути приводом до кардинальної зміни концепції обробки персональних даних, а можуть бути вирішені для початку шляхом прийняття конкретних організаційних, правових або технічних рішень. Проте внесення різних змін до існуючого порядку має бути продиктовано забезпеченням фундаментальних цінностей суспільства, у контексті права людини на

недоторканність приватного життя та захисту персональних даних. Дискусії щодо розглянутих у роботі проблем правового регулювання в галузі забезпечення прав людини при обробці персональних даних будуть поступово набирати все більшої популярності, у зв'язку з цим можна вважати, що в майбутньому будуть підтримані ідеї щодо зміни існуючої концепції.

3.2. Напрямки розвитку правового регулювання захисту персональних даних у Європейському Союзі

Європейський підхід до правового регулювання обробки персональних даних, спрямований на забезпечення прав людини правовими, організаційними та технічними заходами, найбільш прогресивний у світі та набуває все більшого поширення в правових системах різних країн, що є основною тенденцією розвитку у зазначеній сфері. Немає іншого глобального підходу правового забезпечення захисту персональних даних.

Правові акти ЄС, що діють на сучасному етапі, утворюють цілісну систему правового регулювання захисту персональних даних у Європейському Союзі. Основним елементом цієї системи є Регламент (ЄС) 2016/679, а такі правові акти, як Директива (ЄС) 2016/680, Регламент (ЄС) 2018/1725, Директива 2002/58/ЄС та інші, доповнюють Загальний Регламент із захисту даних, розповсюджуючи дію правового регулювання захисту персональних даних на багато сфер суспільного життя в Союзі.

Правове регулювання суспільних відносин, пов'язаних з обробкою персональних даних людини в контексті захисту її прав і свобод, є комплексним і містить у собі як публічно-, так і приватно-правові засади. Це свідчить про необхідність забезпечення балансу інтересів особи, суспільства та держави, а також створення єдиного середовища довіри.

Реформа правового регулювання захисту персональних даних, проведена за допомогою прийняття та набрання чинності зазначених актів, є фундаментальним кроком для безпеки особистих даних фізичних осіб у Європейському Союзі. Загальний Регламент захисту даних створює міцну

основу, що допомагає розвивати інноваційні електронно-цифрові послуги та сервіси, і розглядається як наріжний камінь у справі реалізації європейської стратегії Єдиного цифрового ринку, націленої на сприяння вільному доступу суб'єктів господарювання до онлайн-ринків в умовах справедливої конкуренції та високого рівня захисту споживачів та їх персональних даних.

Варто зазначити, що останніми роками спостерігається підвищення рівня поінформованості населення про право на доступ, виправлення, видалення та інші дії з персональними даними, підвищення рівня прозорості використання. GDPR удосконалив процеси та процедури захисту, такі як право на скаргу, зокрема через представництво, а не судовий процес. Однак механізм захисту персональних даних все ще потребує вдосконалення в контексті полегшення доступу людей до персональних даних, прийняття колективних рішень та зменшення витрат на зустрічні перевірки та митні операції. Потенціал для розвитку механізму полягає в передачі персональних даних. Таким чином, людина опиниться в центрі цифрового ринку, зможе обирати постачальника послуг, поєднуючи різні послуги, обирати інноваційні послуги. Це опосередковано вплине на конкуренцію між постачальниками послуг.

Між іншим важливою такою уявляється, мобільність персональних даних (наприклад, за допомогою технології передачі даних на друкованих носіях у реальному часі у віртуальному середовищі), яка дозволить спростити механізм передачі даних. Мобільність персональних даних особливо актуальна у сфері медицини та наукових досліджень. GDPR і Регламент про вільний потік персональних даних надають компаніям можливості за допомогою конкуренції та інновацій забезпечити вільний потік даних у межах ЄС і створити рівні умови для компаній, заснованих за межами ЄС.

Загалом на сьогодні, захист персональних даних у цифровому середовищі є другою актуальною складовою діяльності ЄС у сфері побудови надійного та безпечного цифрового середовища. Нормативне регулювання захисту персональних даних на наднаціональному рівні в ЄС на поточному

етапі переважно зосереджено навколо положень Загального регламенту захисту персональних даних 2016 р., про повну імплементацію якого у національні правопорядки держав-членів Єврокомісія відзвітувала в червні 2020 р[60].

Проте, пандемія коронавірусу виявила серйозні недоліки регулювання, які містяться у цьому акті. Ключовою проблемою тут є той факт, що в даний час основними суб'єктами збирання, зберігання та аналізу великих даних (в тому числі персональних) виступають компанії, інкорпоровані в США (так звані GAFAM – Google, Apple, Facebook, Amazon та Microsoft) та у Китаї. Подібна ситуація спричиняє фактичну втрату контролю над поводженням з персональними даними громадян ЄС [61, с. 28]. Як наслідок, у більшості випадків використання персональних даних для відстеження соціальних контактів у період пандемії наднаціональне європейське регулювання не було застосовним. При цьому подібна ситуація була вже досить тривалий час. Пандемія китайського коронавірусу лише яскравіше висвітлила її наявність.

Таким чином, необхідність удосконалення наднаціональної системи захисту персональних даних у ЄС стала розглядатися як невід'ємний елемент стратегії формування єдиного цифрового простору. В даний час ведеться робота зі створення та прийняття стандартів та інструкцій у сфері посиленого захисту персональних даних у найбільш чутливих сферах суспільного життя (фінансовому секторі, охороні здоров'я тощо), проте до 2030 р. планується повністю модернізувати систему захисту персональних даних таким чином, щоб вона забезпечувала високий рівень захисту даних та конфіденційності незалежно від конкретних обставин зберігання та обробки таких даних[62].

Актуальні напрями вдосконалення наднаціонального правового регулювання єдиного цифрового простору ЄС на сьогодні представлені трьома основними напрямами:

удосконалення наднаціонального регулювання єдиного цифрового середовища щодо забезпечення кібербезпеки та захисту персональних даних;

розвиток наднаціональних правових засад єдиної цифрової (хмарної) інфраструктури;

створення наднаціональних правових засад єдиного цифрового ринку.

У рамках першого напряму наразі передбачається розробка та впровадження нових стандартів кібербезпеки та поводження з персональними даними на рівні ЄС. При цьому ці стандарти повинні поширюватися як на внутрішніх (резидентів ЄС), так і на зовнішніх учасників цифрового ринку. Загальною нормативною основою для впровадження нових стандартів кібербезпеки має стати внесення змін до Директиви про безпеку мереж та інформаційних систем 2016 року.

Другий напрямок представлений переважно положеннями Європейської стратегії даних 2020 р., що встановлює необхідність розробки та прийняття наднаціональних правил створення та функціонування хмарної інфраструктури, які забезпечили б створення конкурентних умов збору, аналізу, обробки та обміну даними для резидентів ЄС. При цьому основою такого регулювання є принцип відкритого доступу до державних та наднаціональних даних в окремих стратегічних секторах (зокрема, у сфері транспорту та охорони здоров'я). Крім того, у сферу правового регулювання цифрової інфраструктури було інкорпоровано вимоги кліматичної нейтральності та енергоефективності через покладання на Єврокомісію обов'язку розробити нові розширені індекси цифрової економіки та суспільства (DESI)[63].

Третій напрямок удосконалення правового регулювання цифрового простору на рівні ЄС сьогодні представлений двома «законодавчими» ініціативами Європейської комісії: Пропозицією про прийняття Регламенту про цифрові послуги та Пропозицією про прийняття Регламенту про цифрові ринки. Обидва зазначені «законопроекти» прямо спрямовані на створення загальних нормативних засад регулювання цифрових ринків та цифрових послуг на наднаціональному рівні. При цьому прямо вказується на створення єдиного цифрового ринку ЄС. Крім того, у цій сфері передбачається

впровадження нових вимог антимонопольного законодавства, спрямованих на недопущення безконтрольного поглинання стартапів у цифровій сфері зарубіжними великими ІТ-гігантами. Також планується трансформація системи оподаткування учасників цифрових ринків у бік створення сприятливішого податкового режиму для малого та середнього бізнесу. Ці заходи розцінюються в ЄС як один із найважливіших кроків на шляху до забезпечення цифрового суверенітету.

Ще один із пріоритетних напрямків розвитку правового регулювання захисту персональних даних у Європейському Союзі є захист оперативних даних правоохоронними органами ЄС. Комісія ЄС періодично переглядає чинні правові акти, які регулюють обробку персональних даних органами, установами або агентствами Союзу при здійсненні поліцейського співробітництва та судового співробітництва у кримінальних справах для того, щоб оцінити їхню відповідність Директиві (ЄС) 2016/680 та Глава IX Регламенту (ЄС) 2018/1725. Комісія ЄС вживатиме всіх необхідних заходів для застосування глави IX Регламенту (ЄС) 2018/1725 до Європол та Європейської прокуратури (після набуття чинності Регламентом про Європейську прокуратуру).

Найактивніший розвиток правового регулювання захисту даних очікується у сфері електронних комунікацій. Необхідним кроком є прийняття нового Регламенту (ePrivacy), який замінить діючу Директиву 2002/58/ЄС, а також Директиви, що встановлює Європейський код електронних комунікацій. Проекти обох документів, що доповнюють один одного, наразі відбуваються процедури обговорення в інститутах ЄС. Комісія ЄС проводитиме періодичний огляд Регламенту (ЄС) 2016/679, Директиви (ЄС) 2016/680, Регламенту (ЄС) 2018/1725 та інших правових актів для того, щоб за необхідності подавати відповідні пропозиції щодо внесення поправок до зазначених актів.

На підставі Регламенту (ЄС) 2016/679 Комісія ЄС скористається своїм правом приймати акти вторинного права щодо захисту персональних даних.

Так, наразі перебувають у розробці акти з питань прийняття стандартних договірних форм, технічних стандартів та механізмів сертифікації, з питань здійснення взаємодопомоги між уповноваженими органами тощо. З питань процедурного характеру потрібне прийняття актів, зокрема юридично обов'язкових, уповноваженими органами Союзу захисту даних. Такі акти у межах своєї компетенції уповноважені приймати Європейська Рада із захисту даних та Європейська Уповноважена із захисту даних. Зокрема, йдеться про керівні принципи та передову практику, про акти рекомендаційного та консультаційного характеру, прийняті як за своєю ініціативою, так і за запитами Комісії ЄС та інших інститутів Союзу.

Таким чином, на сьогоднішній день можна констатувати, що право захисту персональних даних у ЄС перебуває у процесі постійного розвитку та вдосконалення. Виходячи з проведеного аналізу можна припустити, що в перспективі право захисту персональних даних поширить свою дію на переважну більшість сфер суспільного життя в Європейському Союзі.

Правове регулювання з питань захисту персональних даних відбуватиметься надалі в рамках короткострокових та довгострокових стратегій Європейського Союзу, його інститутів та органів. Серед основних стратегій, спрямованих на перспективу, можна виділити Стратегію розвитку Єдиного цифрового ринку.

ВИСНОВКИ

Концепція «захисту даних» була розроблена в минулому столітті, щоб забезпечити правовий захист осіб від неналежного використання інформаційних технологій для обробки інформації, що стосується них. Вона не створювалася для запобігання обробці інформації чи обмеження використання інформаційних технологій як таких. Натомість вона була розроблена для забезпечення гарантій кожного разу, коли інформаційні технології будуть використовуватися для обробки інформації, що стосується окремих осіб. Це ґрунтувалося на ранньому переконанні, що широке використання інформаційних технологій для цієї мети може мати далекосяжні наслідки для прав та інтересів осіб.

У будь-якому випадку, ця концепція була винайдена в той момент, коли використання інформаційних технологій було ще в зародку. Зараз це зовсім інше, і потенційний вплив такого використання – завдяки Інтернету та мобільним пристроям – тепер повсюди навколо нас, щохвилини щодня, як в особистому, так і в професійному житті. Ймовірно, у майбутньому ця ситуація ще більше посилиться.

За темою дипломної кваліфікаційної роботи було досліджено правові засади захисту персональних даних у Європейському Союзі та особливості механізму їх правового регулювання. Теоретична значущість дослідження полягає у розкритті юридичного змісту того інституту персональних даних, що набуває в сучасний період дедалі більшої важливості, обґрунтовано його самостійність, визначено місце у правовій системі на прикладі ЄС та виявлено основні елементи механізму його реалізації. Практична значущість роботи полягає у тому, що результати дослідження можуть бути використані у правотворчій та правозастосовній діяльності в Україні, інших наукових дослідженнях, у навчальному процесі. За отриманими результатами дослідження можна сформувати відповідні висновки.

Персональні дані, як найбільш чутлива, делікатна і пріоритетно важлива для людини інформація, посідає особливе місце в інформаційних відносинах. Проблема їх захисту та поширення все життя супроводжує людину та пронизує будь-які сфери діяльності суспільства і держави. Від розуміння важливості й необхідності створення системи ефективного захисту персональних даних залежить спокій та благополуччя як окремої людини, так і держави.

Поняття персональних даних включає будь-яку інформацію і не обмежується інформацією, яка відноситься до вузької інтерпретації приватного або сімейного життя людини. Персональні дані включають інформацію про людину та її будь-яку діяльність, включаючи професійну або громадську, контактну, фінансову, медичну, місце проживання або роботи, освіта, сімейна положення, інтереси та захоплення, відео, аудіозаписи або фотографії тощо

В умовах неспинного розширення інформаційного простору право на захист персональних даних має бути зараховане до фундаментальних прав та свобод людини. Воно відрізняється від права на недоторканність приватного життя, хоча має певну подібність із ним. Відмінність полягає в тому, що право про недоторканність приватного життя передбачає захист, поряд з іншим, інформації, що стосується приватного життя, а право на захист персональних даних - справедливу і законну обробку цих даних незалежно від їх характеру та сфери використання.

Інститут захисту персональних даних є сукупністю правових норм, що регулюють суспільні відносини, що виникають при збиранні, використанні, зберіганні, обробці, видаленні, передачі та розкритті персональних даних. Процес формування інституту захисту персональних даних, який є характерним для сучасного етапу правового розвитку, протікає нерівномірно. Так, у ЄС цей процес перебуває на стадії завершення. Головним свідченням є сформований і діючий правовий механізм захисту персональних даних. Його основу становлять нормативні документи Європейського Союзу, які

встановлюють основні норми-принципи, якими визначаються правовий статус суб'єкта даних та компетенція державних органів захисту персональних даних.

Правові акти ЄС, що діють на сучасному етапі, утворюють цілісну систему правового регулювання захисту персональних даних у Європейському Союзі. Основним елементом цієї системи є Регламент (ЄС) 2016/679, а такі правові акти, як Директива (ЄС) 2016/680, Регламент (ЄС) 2018/1725, Директива 2002/58/ЄС та інші, доповнюють Загальний Регламент із захисту даних, розповсюджуючи дію правового регулювання захисту персональних даних на багато сфер суспільного життя в Союзі.

Основу інституту захисту персональних даних у європейському законодавстві становлять вісім універсальних правових принципів. Узагальнення основних принципів захисту персональних даних, які відображаються у положеннях всіх міжнародних стандартів, передбачає обов’язкове дотримання конкретних умов застосування персональних даних для будь-яких суб’єктів інформаційних відносин, при яких персональні дані повинні: бути доступними для суб’єкта даних; бути точними і оновлюватися; бути отримані законним способом; оброблятися з конкретною метою та за згодою на це суб’єкта даних і в кількості мінімально необхідній для визначеної мети; використовуватися тільки згідно визначеної мети; бути захищеними від несанкціонованого доступу та незаконної обробки.

Розглянувши глобальні механізми правового регулювання захисту персональних даних на сучасному етапі, можна констатувати, що європейська система є найпрогресивнішою на даний момент. Правові механізми ЄС найбільш розгорнуто регламентують свою сферу застосування, створюють жорсткі рамки для європейських, а також іноземних компаній та світових корпорацій, впроваджують незалежні контролюючі органи та, що найголовніше, обов'язкові до застосування у всіх державах-членах ЄС. Крім того, вони не лише закликають та заохочують, а й зобов'язують розвивати

міжнародне співробітництво у сфері захисту даних у сучасному глобалізованому світі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. – К.: К.І.С., 2015. – 220 с

2. Бернард А. Захист приватного життя приватним правом: хвала пліткам або як викриті вади породжують чесноти. Les For Interieur, с.153-179. [Електронний ресурс] / Режим доступу: http://www.upicardie.fr/labo/curapp/revues/root/35/alain_bernard.pdf

3. Байгрейв Л.А. Конфіденційність і захист даних у міжнародному аспекті. Стокгольмський інститут скандинавського права & Lee A Bygrave 2010.p.165-200 [Електронний ресурс] / Режим доступу: http://www.uio/studier/privacy-and-dataprotection-ininternational-perspective.pdf

4. Сопілко І. М. Генезис змісту категорії «персональні дані» / І. М. Сопілко // Юридичний вісник. Повітряне і космічне право. – 2013. – ? 4. – С. 62–66.

5. Геллман, Р. (2014) Справедлива інформаційна практика: Основна історія». [Електронний ресурс] / Режим доступу: http://www.bobgellman. com/rg-docs/rg-FIPShistory.pdf.

6. Судове визначення із справи “Діас проти Окленд Трибюн, Інкорпорейтед” (139 Cal App3d 118, 1983). Цит. за: Уоррен Фрідінан, Право на конфіденційність в епоху комп’ютерів. – Л. – Лондон, Нью-Йорк. 1986, стор. 53.

7. Загальний регламент захисту даних (General Data Protection Regulation; GDPR; Regulation (EU) 2016/679) [Електронний ресурс] / Режим доступу: https://gdpr-info.eu/

8. Вайхерт, Г. (2011) Захист персональних даних у рамках серії дискусій «Сьогодення майбутнього». [Електронний ресурс] / Режим

доступу:https://www.datenschutzzentrum.de/vortraege/20110224-weichert-datenschutz-moskauru.pdf.

9. Брижко В.М. Захист персональних даних : реалії та практика сучасності // Інформація і право. – ? 3(9) 2013. – С. 31- 48.

10. Пилипчук В.Г. Актуальні питання захисту прав, свобод і безпеки людини в сучасному інформаційному суспільстві : зб. матеріалів виступів на наук.-практ. конференції ["Проблеми захисту прав людини в інформаційному суспільстві"], (Київ, 1 липня 2016 р.) / НДІІП НАПрН України, НІСД, Секретаріат Уповноваженого Верховної Ради України з прав людини, НТУУ "КПІ" ; упорядн. Фурашев В.М., Петряев С.Ю. – К. : Вид-во "Політехніка", 2016. – С. 6-8.

11. Рогова О. Г. Захист персональних даних у законодавстві Європейського Союзу та України // Теорія та практика державного управління : зб. наук. пр. – Х. : Вид-во ХарРІ НАДУ "Магістр", 2011. – Вип. 3 (34). – 512 с.

12. Волосецький В. О. Іноземний досвід правового регулювання захисту персональних даних В. О. Волосецький // Міжнародний науковий журнал "Інтернаука" // 2016. – ? 12.

13. Шевчук О. Правове регулювання охорони персональних даних в Європейському Союзі : дис. … канд. юрид. н. : спец. 12.00.11 – міжнародне право. Київ, 2018. 197 с.

14. Мельник К. С. Удосконалення нормативно-правового регулювання захисту персональних даних в Україні / К.С. Мельник // Правова інформатика. – ? 1 (41). – 2014. – С. 30-44.

15. Яворська І., Микієвич М. Захист персональних даних у праві Європейського Союзу. Вісник Львівського університету. Серія міжнародні відносини. 2019. Випуск 46. С. 234–240

16. Jean-Claude Juncker. A New Start for Europe: My Agenda for Jobs, Growth, Fairness and Democratic Change Political Guidelines for the next European Commission Opening Statement in the European Parliament Plenary

Session. Strasbourg, 15 July 2014 // [Електронний ресурс] / Режим доступу: https://www.theparliamentmagazine.eu/whitepaper/jean-claude-juncker

17. Commission staff working document «A Digital Single Market Strategy for Europe — Analysis and Evidence». Accompanying the document «A Digital Single Market Strategy for Europe». COM(2015) 192 final. Brussels, 06.05.2015 SWD(2015) 100 final

18. Bennett C. and Raab C. The Governance of Privacy: Policy Instruments in Global Perspective. 2003. P. 257 // The European Journal of International Law. Vol. 21, no. 2, 2010. P. 442.

19. Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act). Brussels, 25.11.2020. COM/2020/767 final

20. Оцінка Європейської комісії економічного впливу від прийнятого Регламенту. [Електронний ресурс] / Режим доступу: https://european-union.europa.eu/contact-eu_uk

21. Commission staff working document. Annual Single Market Report 2021. Accompanying the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions «Updating the 2020 New Industrial Strategy: Building a stronger Single Market for Europe's recovery». Brussels, 05.05.2021. SWD/2021/351 final

22. Посібник з європейського права у сфері захисту персональних даних. – К.: К.І.С., 2021. – 216 с.

23. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. . [Електронний ресурс] / Режим доступу: https://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en

24. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981. – Офіційний вісник України. 2011. 14 січ. (? 58). Ст. 701.

25. Маркіян Бем, Іван Городиський. Захист персональних даних: Правове регулювання та практичні аспекти науково-практичний посібник. 2021. [Електронний ресурс] / Режим доступу: https://rm.coe.int/handbook-pers-data-protect-2021-web/1680a37a69

26. Консолідовані версії Договору про Європейський Союз та Договору про функціонування Європейського Союзу з протоколами та деклараціями. . [Електронний ресурс] / Режим доступу: https://zakon.rada.gov.ua/laws/show/994_b06#Text

27. Хартія основних прав Європейського Союзу від 07 грудня 2000 р. [Електронний ресурс] / Режим доступу: https://zakon. rada.gov.ua/laws/show/994_524#Text.

28. Директива N 2002/58/ЄС Європейського Парламенту та Ради ЄС щодо обробки персональних даних та захисту конфіденційності в секторі електронних засобів зв'язку (Директива про конфіденційність та електронні засоби зв'язку). [Електронний ресурс] / Режим доступу: https://ips.ligazakon.net/document/MU02283

29. Директива ? 2002/22/ЄС Європейського Парламенту та Ради від 7 березня 2002 року про універсальні послуги та права користувачів стосовно електронних комунікаційних мереж та послуг із змінами, внесеними Директивою ? 2009/136/ЄС Європейського Парламенту та Ради від 25 листопада 2009 року.

30. Романюк І. І. Персональні дані особи як об’єкт цивільного обороту / І. І. Романюк // Право і суспільство. – 2014. – ? 6.1(2). – С. 58–65. 20.

31. Protection of Personal Data: An International Business View, Document ICC, No. 373/128, 4 October 1991.

32. ICC Task Force on Privacy and Protection of Personal Data (2004) ICC report on binding corporate rules for international transfers of personal data [Електронний ресурс] / Режим доступу: http://www.iccwbo.org/Data/Documents/DigitalEconomy/ICC-report-on-Binding-Corporate-Rules/; ICC (2003)

33. Кравчук М. М. Міжнародний досвід правового регулювання захисту персональних даних в мережі Інтернет. Наукові записки Інституту законодавства Верховної Ради України. 2013. ? 3. С. 123–126.

34. General Data Protection Regulation. [Електронний ресурс] / Режим доступу: https://gdpr-info.eu/

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

36. Lynskey O. The "Europeanisation" of Data Protection Law // Cambridge Yearbook of European Legal Studies. 2017. Vol. 19. P. 283.

37. Посібник з європейського права у сфері захисту персональних даних. К.: К.І.С., 2020. С. 34.

38. CJEU, Judgment of the Court in Joined Cases C-468/10 and C-469/10 ASNEF and FECEMED of 24 November 2011.

39. CJEU, Judgment of the Court in Joined Cases C-92/09 Volker und Markus Schecke and C-93/09 Hartmut Eifert of 9 November 2010.

40. Zanfir G. How CJEU's "Privacy Spring" Construed the Human Rights Shield in the Digital Age // European judicial systems as a challenge for democracy. Cambridge; Antwerpen; Portland, 2015. P. 114.

41. Council Directive 2006/24/EC 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 [2006] OJ L105/54, Art. 1(1).

42. Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources (CJEU, 8 April 2014).

43. CJEU, Decision of the Court in joined cases C-293/12 and C-594/12 Digital Rights Ireland of 8 April 2014. Para. 48.

44.CJEU, Decision of the Court in Case C-131/12 Google v. Spain of 13 May 2014.

45. Edwards L. Data Protection: Enter the General Data Protection Regulation // Law, Policy and the Internet. Oxford, 2018. [Електронний ресурс] / Режим доступу: https://ssrn.com/abstract=3182454.

46. Constitutional Court of Romania, Decision No. 440/2014 from 8 July 2014.

47. Constitutional Court of the Republic of Slovenia, Judgement U-I-65/13-19 from 3 July 2014.

48. Austrian Constitutional Court, Decision G47/2012 and others, from 27 June 2014.

49. Консультативна рада Google щодо права бути забутим. https://archive.google.com/advisorycouncil/

50. C-511/18 - La Quadrature du Net and Others. https://curia.europa.eu/juris/liste.jsf?language=en&num=C-511/18

51. Герт, П. (2013) Три сценарії міжнародного управління конфіденційністю даних: на шляху до міжнародної організації із захисту конфіденційності даних. [Електронний ресурс] / Режим доступу: http://moritzlaw.osu.edu/students/groups/is/files/2013/08/7-Hert

52. Teatini, S. & Matinmikko-Blue, M.: Privacy in the 5G World: The GDPR in a Datafied Society. In: Tafazolli, R., Chatzimisios, P., Wang, C.-L. (eds.), Wiley 5G Ref: The Essential 5G Reference Online. Wiley, Hoboken (2020). [Електронний ресурс] / Режим доступу: https://doi.org/10.1002/9781119471509.w5GRef173

53. Венгер В., Заярний О. Правовий аналіз основних моделей інституалізації державного контролю у сфері персональних даних та доступу до публічної інформації. Council of Europe. 2020. URL: https://rm.coe.int/legal-analysis-data-ua/16809ee077

54. Daigle B., Khan M. EU GDPR: An Analysis of Enforcement Trends by EU Data Protection Authorities. Journal of International Commerce and

Economics. June, 2020. [Електронний ресурс] / Режим доступу: https://www.usitc.gov/publications/332/journals/jice_gdpr_enforcement.pdf

55. Martнnez-Martнnez, D. F.: Unification of Personal Data Protection in the European Union: Challenges and Implications. El Profesional de la Informaciyn 27(1), 185- 194 (2018).

56. Kuner C. Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection. University of Cambridge Faculty of Law Research Paper No. 20/2021. April 16, 2021. [Електронний ресурс] / Режим доступу: http://dx.doi.org/10.2139/ssrn.3827850

57. Шарма, С. (ред.): Посібник із конфіденційності даних і GDPR. Wiley, Hoboken (2020).

58. Доповідь "Consumer Data Rights and Competition - Background note". [Електронний ресурс] / Режим доступу: https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf

59. Брижко В.М. Сучасні основи захисту персональних даних в європейських правових актах. // «Інформація і право» ? 3(18) / 2016

60. Commission report: EU data protection rules empower citizens and are fit for the digital age // [Electronic source] // European Commission. 24 June 2020. [Електронний ресурс] / Режим доступу: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018PC0630

61. Єлінек, Т. (2021). Картографування стратегії цифрового суверенітету Європи: трикутник ЄС-Китай-США. Пекін: Інститут Тайхе. 28 стор.

62. Council, the European economic and social committee and the Committee of the regions: 2030 Digital Compass: the European way for the Digital Decade (COM/2021/118 final). Brussels, 9.3.2021.

63. Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions: 2030 Digital Compass: the European way for the Digital Decade (COM/2021/118 final). Brussels, 9.3.2021.