УДК 347.2/3

***Гуйван П.Д.***
Національний юридичний університет імені Ярослава Мудрого

# ОКРЕМІ АСПЕКТИ ЗАКОНОДАВСТВА ПРО ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В ЄВРОПЕЙСЬКОМУ СОЮЗІ

*У статті вивчається і проводиться науковий аналіз чинного законодавства Євросоюзу, призначеного для врегулювання порядку збору, обробки, поширення та захисту персональних даних. Зокрема, досліджується зміст, основні засоби та правові підходи при винесенні Рекомендацій Комітету Міністрів Ради Європи. Виявляються особливості реалізації принципу щодо поваги до права на приватність у цій площині. Надаються рекомендації стосовно адаптації вказаних підходів до вітчизняної правової системи.*

***Ключові слова:*** *охорона приватного життя, захист персональних даних.*

**Вступ.** Законодавче закріплення механізмів збирання, використання, поширення та захисту особистої інформації про людину є дуже важливим, позаяк у такий спосіб забезпечується захист персональних даних як елемент піклування суспільства про охорону приватного життя. Особливо значного обсягу нормативне врегулювання даних відносин набуло в Європі, зокрема у країнах Європейського Союзу (далі – ЄС). Від моменту створення даної міжнародної організації було передбачено необхідність вироблення спеціальних актів Спільноти про захист інтересів особи щодо опрацьовування особових даних і вільного руху таких даних та їхнє належне застосовування до інституцій та органів, створених Договором про заснування Європейської Спільноти чи на його підставі (ч. 1 ст. 286 Договору) [1]. Дослідження змісту різних актів ЄС вельми актуальне і для України, бо, враховуючи прагнення нашої держави до вступу до європейської спільноти, вона має враховувати усталені підходи цієї організації. Адже Україна лише нещодавно почала розробку та прийняття відповідних регуляторних актів (достатньо сказати, що Закон України «Про захист персональних даних» набрав чинності з 2011 року), тож спеціальне законодавство у цій царині знаходиться у зародковому стані. Практично відсутня і необхідна судова практика, відтак рішення судів у нечисленних справах мають або волюнтаристичний, або відверто дискримінаційний характер.

Власне, окремі акти міжнародного характеру щодо регулювання порядку збирання, обробки та охорони персональних даних мають обов'язковий характер для усіх країн-учасників, у тому числі для України. Мова йде, наприклад, про Європейську Конвенцію про захист прав людини та основоположних свобод, стаття 8 якої вимагає від учасників державних гарантій стосовно права на повагу до свого приватного і сімейного життя [2]. Більш детально правила поведінки учасників коментованих відносин регламентовано у Конвенції про захист фізичних осіб при автоматизованій обробці персональних даних [3]. Цей документ встановив поняття персональних даних: та інформація, яка стосується конкретного суб'єкта, котрий ідентифікований або може бути ідентифікованим. У Конвенції також сформульовані основні засади обробки персональних даних, права людини у зв'язку з їх обробкою, принципи передачі даних.

Але загальні підходи, як показало життя, не є достатньо дієвими та потребують більш детального регламентування з урахуванням того, що збір, обробка та поширення персональних даних відбувається практично у всіх сферах нашого життя. В Європейському Союзі на рівні актів різної юридичної сили було деталізовано та конкретизовано загальне законодавство, включаючи прийняття різних за функціональним та галузевим призначенням, чого наразі не зроблено у нашій державі. Так, нормативними актами, обов'язковими для усіх держав-членів, є Директиви Європейського парламенту і Ради, які встановлюють справедливі правила поведінки при обробці особистої інформації. Слід навести Директиву Європей-

ського Парламенту і Ради № 95/46/ЄС про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних від 24 жовтня 1995 року, Директиву 97/66/ЄС про обробку персональних даних і захист прав осіб у телекомунікаційному секторі Європейського парламенту та Ради від 15 грудня 1997 року, Директиву № 2002/58/ЄС Європейського Парламенту і Ради ЄС стосовно обробки персональних даних та захисту права на недоторканість особистого життя у сфері електронних засобів зв'язку від 12 липня 2002 року та велику кількість подібних регуляторних актів, які охоплюють опосередкування охорони персональних даних практично у всіх сферах діяльності.

Відповідно до основних принципів у коментованій сфері 18 грудня 2000 року було прийнято Регламент Європейського Парламенту і Ради № 45/2001 стосовно захисту осіб з точки зору обробки персональних даних установами та органами Спільноти і вільного руху таких даних [4]. Окрім загальних правил, даний документ указує, що фундаментальні права та свободи фізичних осіб, поміж іншого, їхнє право на приватність поважаються установами та органами Спільноти. З метою практичної реалізації цієї задачі було запроваджено новий незалежний контрольний орган – Європейського інспектора із захисту персональних даних. Очолює дану інституцію Уповноважений ЄС. Даний суб'єкт заслуховує та розслідує скарги, а також інформує осіб, які звернулися зі скаргою (приватних осіб про яких або від яких збираються або обробляються дані) про своє рішення упродовж розумного строку (ст. 46 Регламенту). З цією метою Уповноважений вправі вимагати від контролера даних необхідну інформацію, а останній зобов'язаний її надати. Уповноважений взаємодіє як з національними органами влади щодо розгляду суперечливих питань, обміну інформацією, надсилання їм вимог про виконання свої обов'язків із захисту даних, так і з наглядовими органами, такими, скажімо, як Європол та Evrojust [5, с. 34]. Згідно зі ст. 24 Регламенту кожен орган ЄС призначає спеціально уповноважену особу – Офіцера із захисту персональних даних, відповідальну за забезпечення суб'єктів даних інформацією про їхні права та дотримання законодавства про обіг особистих даних на інституційному рівні. Він також зобов'язаний сприяти Уповноваженому у розслідуванні скарг, реєструвати операції з обробки даних та повідомляти останнього, якщо вони мають ризикований характер.

**Аналіз останніх досліджень і публікацій.** Питанням оцінки зарубіжного законодавства наразі присвячено не так і багато наукових праць. Слід згадати розробки таких учених, як В. Брижко, В. Іванський, Б.Кормич, С. Кашкін, А. Чернобай, О. Капустін, Л. Чернявський, В. Цимбалюк. Однак, у даних працях в основному досліджується вплив на процеси захисту особистої інформації на рівні міжнародних конвенцій та договорів, учасником яких є такі держави, як Україна чи Росія. На жаль, законодавство ЄС у цьому плані залишається практично не дослідженим. Між тим, саме воно є найбільш розвиненим, і його вплив на український поступ у сфері захисту персональних даних є безсумнівним та допоможе у його розвитку у правильному напрямі. Вищевказані актуальні теоретичні та практичні проблеми захисту персональної інформації становлять значний публічний інтерес щодо вивчення законодавчого досвіду зарубіжних держав у регламентуванні коментованих відносин. Тож, метою даної праці є здійснення наукового аналізу усіх чеснот і вад європейських нормативних актів та інших документів, присвячених обороту персональних даних, та напрацювання правових механізмів регламентування вказаних відносин у різних галузевих напрямках відповідної взаємодії.

**Постановка завдання.** Як бачимо, законодавство у сфері регулювання обороту та захисту персональних даних в Європейській Спільноті є достатньо конкретним, дієвим та ефективним. При цьому маємо зазначити, що з огляду на стрімкий розвиток суспільних відносин, передусім у технічній та інформаційній площині, воно постійно оновлюється, доповнюється та модернізується, намагаючись відповідати потребі дня. То є яскравим прикладом як для національного нормотворця, так і для доктрини. Тож має бути чітко на теоретичному та практичному рівнях дано однозначне визначення понять персональні дані та здійснена класифікація їх видів, бо саме особиста інформація є основним об'єктом зазіхань на недоторканність сфери приватного життя [6, с. 156].

**Виклад основного матеріалу дослідження.** Слід погодитися з тезою про те, що належний і повноцінний захист персональних даних у різних органах державної влади, установах, організаціях тощо просто неможливий без прийняття низки підзаконних нормативно-організаційних актів, покликаних конкретизувати вказану діяльність в окремих напрямках [7, с. 121]. На рівні Європейського Союзу дана конкретизація

здійснюється шляхом реалізації Комітетом Міністрів ЄС делегованих повноважень стосовно прийняття відповідних Рекомендацій. Вказані акти мають субсидіарний характер і певною мірою деталізують положення Директив Європарламенту і Ради.

До прикладу, захисту персональних даних в Інтернеті присвячено Рекомендацію Комітету Міністрів державам-членам Ради Європи «Основні напрямки захисту прав фізичних осіб у зв'язку з обробкою персональних даних в інформаційних супермагістралях» від 9 грудня 1997 року [8] та Рекомендацію N R(99)5 «Про захист недоторканності приватної власності в Інтернеті» [9]. Рекомендації наголошують, що користувачі та провайдери послуг Інтернету мусять враховувати особливість захисту персональних даних у цій мережі з огляду на можливість несанкціонованого їх використання та нанесення шкоди людині, суспільству або державі. При цьому, споживачі застерігаються, що Інтернет – небезпечна мережа. Будь-яка транзакція, будь-яке відвідування сайту в Інтернеті залишає сліди. Подібні «електронні сліди» можуть бути використані без відома користувача для створення профілю про нього і його інтереси. Однак, наявні зараз і розробляються різні засоби, що дозволяють підвищити рівень захисту даних. То можуть бути легально доступні засоби шифрування для конфіденційної електронної пошти та коди доступу до персонального комп'ютеру. Якщо сторонній доступ є небажаним, слід використовувати новітні технічні досягнення, що дозволяють проінформувати про це споживача послуг. Можна також запитати постачальника про методи забезпечення недоторканності приватного життя, що надаються різними програмами і сайтами, і віддати перевагу тим з них, які реєструють мінімум даних про користувача або можуть бути доступні анонімно (п. 1-4). Також необхідно повідомляти постачальникові послуг інтернету тільки ті дані, які необхідні для виконання певних дій, про які суб'єкт заздалегідь поінформований. Особлива обережність необхідна при використанні кредитних карток і номерів рахунків, які в Інтернеті можуть легко стати об'єктом зловживань. Слід з обережністю ставитись до сайтів, де просять інформацію особистого характеру більшу, ніж це потрібно для доступу чи здійснення транзакції, чи не написано, для чого така інформація необхідна взагалі.

Для постачальників послуг інтернету рекомендації передбачають необхідність використання процедур і доступних технологій, переважно сертифікованих, для забезпечення недоторканності приватного життя людини (навіть якщо вони не користувачі мережі Інтернет), особливо шляхом забезпечення цілісності і конфіденційності даних поряд із забезпеченням фізичної і логічної безпеки мережі і послуг, наданих у мережі. Провайдер має попередньо інформувати користувачів при їхній підписці на послуги чи початком обслуговування про ризики недоторканності приватного життя при використанні Інтернету, а також про технічні засоби, що можуть використовуватися на законній підставі для зниження ризику порушення безпеки персональних даних і їхньої передачі. Він повинен вживати заходи із метою недопущення будь-якого зовнішнього втручання у зміст переданих даних, якщо тільки це не передбачено законом і не здійснюється державними органами. Збирання, оброблення і зберігання персональних даних користувачів дозволяється тільки тоді, коли це необхідно для зрозумілих, точно визначених і законних цілей. Передача персональних даних можлива лише за наявних, законодавчо визначених підстав, або згоди суб'єкта персональних даних. Інформація, що надається користувачеві, має бути точною та актуальною. Зберігання персональних даних повинно відбуватися не довше, ніж це необхідно для цілей їх оброблення.

Приблизно такі ж підходи зафіксовані і у Рекомендації № R(95)4 щодо захисту даних особистого характеру у сфері телекомунікаційних послуг [10]. У цьому акті акцентується на необхідності надання телекомунікаційних послуг, зокрема телефонних, на засадах поваги до приватного життя користувачів, з дотриманням таємниці листування та свободи комунікаційних обмінів даними. Можливості анонімного доступу до мережі і до телекомунікаційних послуг повинні бути надані у доступне розпорядження. Будь-яке втручання у зміст комунікації або операторами мережі, або постачальниками послуг повинно бути заборонене, за винятком, якщо це є дозволеним з технічних причин запису або передавання послання, з інших законних причин, або з виконання контракту послуг, укладеного з абонентом. Дані щодо змісту зібраних послань під час такого втручання не повинні бути переданими третій стороні. Не може бути втручання органів державної влади у зміст комунікації, включаючи використання пристроїв прослуховування або інших засобів нагляду чи

перехоплення комунікацій, якщо тільки таке втручання не є передбаченим законом та не є необхідним заходом у демократичному суспільстві, спрямованим на захист державної та громадської безпеки, валютно-кредитних інтересів держави або на боротьбу із кримінальними правопорушеннями та на захист відповідної особи або прав і свобод інших людей. У випадках втручання органів державної влади у зміст комунікації, внутрішнє законодавство повинно регламентувати: a) здійснення прав доступу та внесення змін відповідною особою; b) умови, за яких компетентні державні органи матимуть право відмовити у наданні інформації відповідній особі або відкласти її надання; c) порядок зберігання або знищення цих даних. Коли оператор мережі або постачальник послуг є уповноваженим державним органом на здійснення втручання, зібрані дані мають бути направленими тільки до організації, визначеної у дозволі на таке втручання (п. 2, 4.2-4.3).

Збір та обробка даних особистого характеру у телекомунікаційній сфері має здійснюватися і розвиватися у рамках політики захисту даних, зважаючи на положення, визначені у Конвенції про захист осіб стосовно автоматизованої обробки даних особистого характеру і зокрема на принцип доцільності. Дані особистого характеру мають збиратися і оброблятися операторами мережі і постачальниками послуг тільки з метою підключення до мережі та надання у розпорядження певної телекомунікаційної послуги, або з метою визначення суми для сплати, як і для забезпечення запровадження оптимальних технологій і розвитку мережі і послуг. Оператори мережі та постачальники послуг повинні інформувати у належний спосіб абонентів телекомунікаційних послуг про категорії зібраних і оброблених даних особистого характеру, які їх стосуються, про юридичне обгрунтування такого збору, про цілі, з якими вони зібрані і оброблені, про той характер їх використання, що здійснений, та про строки тривалості їх зберігання (п. 3). Дані особистого характеру, зібрані і оброблені операторами мережі або постачальниками послуг, не повинні передаватися, за виключенням випадків, коли абонент, якого це стосується, надав письмову чітко викладену згоду, висловивши свою поінформованість, та, коли характер переданої інформації не дозволить ідентифікувати абонентів. Абонент може забрати свій дозвіл у будь-який момент, але без надання цій дії ретроактивної сили (п. 4.1, 4,4).

Кожен абонент повинен мати право після своєї вимоги та у розумні проміжки часу і без відкладання та надмірних витрат отримати всі дані, що його стосуються і які є зібраними та обробленими операторами мережі або постачальниками послуг, та їх виправити або видалити, коли вони є невірними, недоцільними чи надмірними, або, якщо вони зберігалися занадто довгий час. У задоволенні сформульованих вимог може бути відмовлено, вони можуть бути обмеженими або відкладеними на пізніше, якщо це дозволяє законодавство та є у демократичному суспільстві необхідним заходом, спрямованим на захист державної та громадської безпеки, відповідної особи або прав і свобод інших людей (п. 5). Оператори мережі та постачальники послуг повинні вжити всіх належних технічних і організаційних заходів для того, щоб забезпечити фізичну і програмну безпеку мережі, послуг і даних, які вони збирають і обробляють, та унеможливити будь-яке несанкціоноване втручання або перехоплення комунікаційних повідомлень. Абоненти телекомунікаційних послуг повинні бути проінформованими про ризики зламу безпеки мереж та про спосіб, в який вони можуть обмежити ризики безпеки для своїх повідомлень (п. 6).

Абоненти повинні мати право, безкоштовно і не вдаючись до мотивації, відмовити у розміщенні своїх даних особистого характеру у довідниках. Коли внутрішнє законодавство вимагає, щоб певні дані були включені у довідник, абонент повинен мати можливість виключити ці дані на підставі пояснювальних документів. За умови тих випадків, коли абонент бажає включити додаткові дані, що його стосуються, то дані особистого характеру, що містяться у довіднику, повинні бути обмеженими достатнім обсягом даних, необхідних для ідентифікації окремого абонента та для того, аби завадити плутанині між або серед різних абонентів, що фігурують у довіднику. Під час консультування електронного довідника повинні бути запроваджені технічні засоби для того, щоб упередити зловживання і, зокрема, неавторизовані вивантажування даних. Будь-яка довідка має бути обмеженою наданням даних, що фігурують у довіднику. Мають бути вжиті належні заходи для того, щоб боротися зі зловживаннями. Служба інформаційної довідки не повинна надавати інформацію стосовно абонентів, котрі не фігурують у довіднику, окрім тих випадків, коли абонент, якого це стосується, надав письмову чітко викладену згоду, висловивши свою поінформованість. Власники

мережі і постачальники послуг повинні надавати детальні рахунки з номерами викликаних абонентів у розпорядження певного абонента лише за його вимогою. З розумінням необхідно ставитися до приватного життя співкористувачів і кореспондентів (п. 7).

Важливим актом, який регулює особливості взаємин між учасниками у сфері поширення особистої інформації, є Рекомендація № R(91)10 щодо передачі третім особам інформації особистого характеру, яка знаходиться у розпорядженні органів влади [11]. Він також ґрунтується на принципі поваги до приватного життя та захисту даних. При цьому наголошується, що повідомлення, зокрема засобами електронного зв'язку, даних особистого характеру чи файлів з даними особистого характеру третім сторонам має супроводжуватися гарантіями, що приватне життя суб'єкта даних не буде порушуватися у незаконному порядку. Зокрема, дані особистого характеру та файли з даними особистого характеру не повинні повідомлятися третім сторонам, окрім випадків, коли: a) це передбачено спеціальним законом; або b) громадськість має доступ до них відповідно до правових положень, що регулюють доступ до інформації публічного сектора; або c) повідомлення здійснюється відповідно до національного законодавства про захист інформації; або d) суб'єкт даних вільно та поінформовано надав свою згоду. Якщо нормами національного права не передбачено забезпечення належних гарантій суб'єкта даних, дані особистого характеру або файли з даними особистого характеру не можуть повідомлятися третім сторонам для цілей, що не відповідають тим, для яких ці дані були зібрані (п. 2). При цьому особлива увага надається застереженням, які повинні враховуватися при поширенні даних чутливого характеру. Вони не повинні зберігатись у файлі чи частині файлу, доступних третім сторонам. Будь-які винятки з цього принципу мають бути чітко передбачені законом із забезпеченням відповідних гарантій суб'єктові даних (п. 3).

Спеціальним документом у даній сфері регулювання є також Рекомендація № R(97)5 Комітету міністрів ЄС державам-членам щодо захисту медичних даних [12], спрямована на координування поведінки учасників відповідних відносин. Медичні дані про особу як особиста інформація про стан її здоров'я та інші відомості, що чітко та тісно пов'язані з даними про стан здоров'я і генетичними даними, мають збиратися і оброблятися на засадах поваги до приватного життя лише медичними працівниками, особами й органами, які працюють від імені медичних працівників, та лише для певних законних цілей. Медичні дані повинні отримуватись від суб'єкта даних, при цьому інформація, яка надається, повинна бути доречною і придатною для суб'єкта. У разі, коли суб'єкт зобов'язаний дати згоду, така згода повинна бути добровільною та чітко вираженою. Медичні дані можуть розголошуватись лише особі, яка підпорядковується нормам конфіденційності, покладеної на медичного працівника, чи схожим нормам конфіденційності. Медичні дані можуть розголошуватись у випадках, передбачених законом, для визначених цілей, зокрема захисту суб'єкта даних чи його родичів по генетичній лінії, а також при згоді суб'єкта чи органу для певних цілей або якщо відсутнє заперечення суб'єкта (п. 1-5, 9-10).

Окремі Рекомендації КМ ЄС присвячені питанням врегулювання відносин щодо збору та обробки персональних даних при здійсненні правоохоронної діяльності. До прикладу, можемо назвати Рекомендацію № R(87)15 Комітету Міністрів державам-членам, що регулює використання персональних даних у секторі поліції [13] (схвалена 17 вересня 1987 на 410-й зустрічі заступників Міністрів). Вказаний документ прийнятий згідно зі Статтею 156 Статуту Ради Європи, зважаючи на зростаюче використання персональних даних для автоматизованої обробки у секторі поліції та заради майбутньої користі від застосування комп'ютерів та інших технічних засобів у цій сфері, беручи до уваги стурбованість можливою загрозою приватності особи, що виникає внаслідок неправильного застосування методів автоматизованої обробки. У зазначених цілях вираз «у цілях поліції» означає всі завдання, які можуть розв'язувати органи поліції для запобігання чи припинення кримінальних правопорушень та досягнення громадського порядку. Основні принципи даної Рекомендації ґрунтуються на загальних підходах і спрямовані на максимальну законність та відкритість процесу обробки даних виключно із легітимною метою.

З проведеного дослідження можемо зробити певні висновки. Рекомендації, що прийняті Кабінетом Міністрів Ради Європи на виконання нормативних актів, охоплюють різні напрямки захисту персональних даних. Крім детально вивчених у цій праці, можемо ще привести Реко-

мендації № R(83)10, яка стосується, зокрема, охорони персональної інформації у сфері наукових досліджень та статистики, № R(85)20 (про прямий маркетинг), № R(89)2 про захист персональних даних, які використовуються для потреб працевлаштування, № R (86)1, яка регулює вказані відносини у сфері соціальної безпеки; № R(91) щодо передачі даних суспільними установами, № R(90)19 про фінансові платежі та пов'язані з цим операції.

Як бачимо, згідно з законодавством ЄС і, зокрема, відповідно до приписів вказаних вище Рекомендацій КМ ЄС діяльність європейських органів та установ стосовно обробки персональних даних та їх поширення знаходиться під жорстким контролем. Той вибір, який зробили країни ЄС, впровадив серйозні вимоги щодо правил поводження з персональними даними, і він вимагає від інших країн переглядати власні підходи у пошуках компромісу [14, с. 9]. Утім, мусимо констатувати, що українське законодавство, а отже, і реалії ще дуже далекі від даних вимірів. Тож, якщо наша держава реально, а не на словах, прагне вступити до Європейської Спільноти, їй треба ой як постаратися, аби гармонізувати міжнародну і національну правові системи.

**Список літератури:**

1. Договір про заснування Європейської Спільноти ЄЕС; Договір, Перелік, Міжнародний документ від 25.03.1957 року. URL: http://zakon2.rada.gov.ua/laws/show/994_017/page.

2. Конвенція про захист прав людини і основоположних свобод. Рада Європи; Конвенція, Міжнародний документ від 04.11.1950 року. Ратифікована Україною 17 липня 1997 року. URL: http://zakon3.rada.gov.ua/laws/show/995_004.

3. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних Рада Європи; Конвенція, Міжнародний документ від 28 січня 1981 року. Ратифікована Україною 6 липня 2010 року. URL: http://zakon2.rada.gov.ua/laws/show/994_326.

4. Регламент Європейського Перламенту і Ради № 45/2001 від 18 грудня 2000 року стосовно захисту осіб з точки зору обробки персональних даних установами та органами Спільноти і вільного руху таких даних. URL: https://www.dst.dk/ext/454209204/0/.../UKR_Regulation-(EC)-No-45_2001--docx.

5. Валеев Р.М. Контроль в современном международном праве. Казань: Центр инновационных технологий, 2001. 211 с.

6. Иванский В.П. Правовое регулирование персональных данных в законодательстве зарубежных государств. Вестник Российского университета дружбы народов. Серия: Юридические науки. 2012. № 1. С. 156-168.

7. Брижко В.М. Організаційно-правові питання захисту персональних даних: дис.. … канд.. юрид. наук. 12.00.07. Київ, 2004. 203 с.

8. Рекомендація Ради Європи Основні напрямки захисту прав фізичних осіб у зв'язку з обробкою персональних даних у інформаційних супермагістралях від 9 грудня 1997 року. URL: http://www.europa.eu.

9. Рекомендація № R(99)5 Комітету Міністрів державам-членам Ради Європи «Про захист недоторканності приватної власності в Інтернеті» від 23 лютого 1999 року. URL: http://zakon5.rada.gov.ua/laws/show/994_357.

10. Рекомендація № R(95)4 Щодо захисту даних особистого характеру в сфері телекомунікаційних послуг. Ухвалена Комітетом Міністрів 7 лютого 1995 року. URL: http://cedem.org.ua/library/rekomendatsiya-r-95-4-shhodo-zahystu-danyh-osobystogo-harakteru-v-sferi-telekomunikatsijnyh-poslug/

11. Рекомендація № R(91)10 Щодо передачі третім особам інформації особистого характеру, яка знаходиться в розпорядженні органів влади Схвалено Комітетом міністрів 9 вересня 1991 року. URL: http://cedem.org.ua/library/rekomendatsiya-r-91-10-shhodo-peredachi-tretim-osobam-informatsiyi-osobystogo-harakteru-yaka-znahodytsya-v-rozporyadzhenni-organiv-vlady/

12. Рекомендація R11(97)5 щодо захисту медичних даних від 13 лютого 1997 року. URL: http://www.umj.com. ua/article/37381/rekomendacii-radi-yevropi-shhodo-zaxistumedichnix-danix.

13. Рекомендацію № R(87)15 Комітету Міністрів державам-членам, що регулює використання персональних даних у секторі поліції від 17 вересня 1987 року. URL: http://cyberpeace.org.ua/files/rekomendacia_km_radi_evropi_sodo_vikoristanna_personal_nih_danih__sektori_policii.pdf.

14. Пазюк А.В. Захист прав людини стосовно обробки персональних даних: міжнародні стандарти. МГО Прайвесі Юкрейн. К.: Інтертехнодрук, 2000. 69 с.

**ОТДЕЛЬНЫЕ АСПЕКТЫ ЗАКОНОДАТЕЛЬСТВА О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЕВРОПЕЙСКОМ СОЮЗЕ**

*В статье изучается и дается научный анализ действующего законодательства Евросоюза, предназначенного для урегулирования порядка сбора, обработки, распространения и защиты персональных данных. В частности, исследуется содержание, основные средства и правовые подходы, применяемые при вынесении рекомендаций Комитета министров Совета Европы. Выявляются особенности реализации принципа уважения права на приватность в этой плоскости. Даются рекомендации по адаптации указанных подходов к отечественной правовой системе.*

***Ключевые слова:*** *охрана частной жизни, защита персональных данных.*

**CERTAIN ASPECTS OF LEGISLATION ON THE PROTECTION OF PERSONAL DATA IN THE EUROPEAN UNION**

*In this paper, a study and a scientific analysis of the current legislation of the European Union, designed to regulate the collection, processing, dissemination and protection of personal data, is conducted. In particular, the content, fixed assets and legal approaches used in making recommendations of the Committee of Ministers of the Council of Europe are examined. The peculiarities of the realization of the principle of respect for the right to privacy in this plane are revealed. Recommendations are given on the adaptation of these approaches to the domestic legal system.*

***Key words:*** *protection of privacy, protection of personal data.*