УДК 347.2/3

ГУЙВАН П. Д.,
кандидат юридичних наук, заслужений юрист України,
докторант
Національного юридичного університету імені Ярослава Мудрого

ОКРЕМІ ПИТАННЯ МІЖНАРОДНО-ПРАВОВОГО РЕГУЛЮВАННЯ ОБОРОТУ ТА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Анотація. Статтю присвячено питанням регулювання обороту і захисту персональних даних у правових актах міжнародного законодавства, які мають локальне та галузеве призначення. Проводиться аналіз положень окремих Рекомендацій Комітету Міністрів ЄС, спрямованих на встановлення правил обігу даних про особу в різних сфераї діяльності, також аналізується світова та європейська правотворча робота в царині обробки та захисту персональних даних в електронних мережах, зокрема в Інтернеті. Проведено узагальнення юридичних підходів, відмічено спільні позиції до визначеності механізмів. Розглянуто їх практичне застосування Європейським судом із прав людини.

Ключові слова: оборот персональних даних, правовий захист особистої інформації.

Постановка проблеми. Захист права на приватність стосовно обробки персональних даних є необхідною складовою частиною фундаментальних прав людини. Організація відносин стосовно врегулювання порядку обігу та захисту цих взаємин є обов'язком національних законодавчих органів, а позаяк наразі відбувається активне переміщення даних через кордони держав, що пов'язано з інтенсифікацією ділової, політичної та культурної активності, до цієї проблематики активно залучаються і міжнарожно-правові інституції. Тож справедлива, усталена й очікувана регламентація порядку обробки та охорони персональних даних забезпечить функціонування гуманного демократичного суспільства, в якому гарантується захист людської гідності, свободи і безпеки особи.

Право конкретної людини на захист персональних даних у світі розглядається в контексті реалізації права на недоторканність приватного життя. Дані права тісно пов'язані між собою і співвідносяться як категорії часткового і загального, адже персональні дані особи є невід'ємним елементом приватності. Саме для охорони і захисту права на недоторканність особистого життя в умовах автоматизованої обробки даних про громадян в Європі близько 30 років тому був введений особливий інститут правової охорони особистості – так званий інститут захисту персональних даних [1, с. 217]. В Європі та світі впродовж тривалого часу відбувалося та нині продовжується становлення спеціального законодавства, присвяченого

регламентуванню обороту, обробки, використання та захисту персональних даних. Наразі склався комплексний механізм регулювання цих питань. Зокрема, в царині захисту особистої інформації про особу напрацьована єдина система засад, котра визначає дієвість відповідного правового інструментарію. Це наявність загальноєвропейської нормативної бази, дія національних законодавчих актів, що регулюють питання обороту персональних даних, правова чіткість основних принципів права щодо їхнього захисту, наявність європейських консультативних і наглядових органів, а також створення національних адміністративних органів щодо захисту особистої інформації, нормативна визначеність правового статусу – основних прав, свобод і обов'язків; наявність правової визначеності під час передачі даних третім особам [2, с. 109].

Європейське та світове законодавство регулює питання обороту та захисту персональних даних також у рамках універсальних міжнародних договорів у сфері захисту прав людини та актів спеціального галузевого призначення. Так, вимоги щодо незаконності свавільного втручання в приватне життя та недоторканності персональних даних про особу, включаючи таємницю кореспонденції та незаконне посягання на її честь і гідність, містяться в Конвенції Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних», прийнятій у 1981 році, ст. 8 Конвенції «Про захист прав людини і основоположних свобод» 1950 року, ст. 16 Конвенції про права дитини 1989 року [3]. Правові приписи, спрямовані на захист персональних даних, містяться в ст. 7 Хартії основних прав Європейського Союзу [4], Керівних принципах з приватності, прийнятих у вигляді Рекомендації Ради ОЕСР 23 вересня 1980 року.

Аналіз останніх досліджень і публікацій. Разом із тим інструментарій досягнення урегульованості та безпеки обороту і використання персональних даних встановлюється не лише в загальних міжнародних актах, а впорядковується також документами галузевої спрямованості та локальної компетенції. Вказані питання опосередковуються і внутрішнім законодавством багатьох зарубіжних країн. Дослідження даного законодавства та визначення його характерних засадничих принципів формування та застосування, відзначення спільних підходів різних легіслатур та адаптація світових правил до української правової системи є метою даної праці. У науковій літературі дослідження іноземного законодавства в контексті його впливу на охорону та захист права особи на приватність, у тому числі на персональні дані, здійснювали такі науковці, як О. Волков, А. Пазюк, А. Чернобай, Б. Кормич, Р. Калюжний, А. Марущак, І. Бачило, М. Кравчук, В. Іванський, М. де Сальвіа, А. Пазюк, А. Тунік, В. Цимбалюк, М. Швець та інші. Разом із тим дані публікації в основному присвячені проблематиці застосування основних конвенцій та принципів Європейського суду з прав людини для регулювання питань охорони інформації про особу. Між тим актуальність проблеми набагато ширша. У даній роботі аналізуються загальносвітові підходи до запровадження регулятивних механізмів захисту

даних не лише в міжнародних договорах, а і в національному законодавстві, регіональних угодах, у тому числі і стосовно захисту інформації про особу в електронних мережах.

Виклад основного матеріалу. Значне коло питань із тематики, що розглядається, врегульоване на рівні Рекомендацій Комітету міністрів державам-членам Ради Європи щодо використання персональних даних. Попри те, що вони адресовані країнам-учасникам ЄС і не мають обов'язкового характеру, ці документи можуть бути взірцем оформлення відносин із охорони персональних даних у конкретному напрямку їх використання. Це особливо важливо, враховуючи прагнення України до вступу в Євросоюз. Рекомендації охоплюють різні напрямки захисту персональних даних. Приміром, Рекомендація № R (87) 15 [5] регулює порядок використання персональних даних поліцією. Вона спрямована на збалансування інтересів влади стосовно дотримання громадського порядку та суспільства і конкретної особи щодо права на недоторканність приватного життя. У цьому правовому акті конкретизуються положення Конвенції 1981 року, зокрема в частині виключень, передбачених статтею 9. Рекомендація має на меті визначити та гарантувати запровадження певних принципів захисту даних у звичайних та особливих справах поліції, забезпечити їхнє використання для запобігання кримінальним правопорушенням.

У вересні 1991 року Комітет Міністрів ЄС прийняв Рекомендацію № R (91) 10 щодо передачі третім особам інформації особистого характеру, яка знаходиться в розпорядженні органів влади [6]. Вказаний документ передбачає механізми повідомлення, зокрема засобами електронного зв'язку, даних особистого характеру чи файлів із даними особистого характеру третім сторонам. Це має супроводжуватися гарантіями, що приватне життя суб'єкта даних не буде порушуватися в незаконному порядку. Зокрема, дані особистого характеру та файли з даними особистого характеру не повинні повідомлятися третім сторонам, окрім випадків, коли: а) це передбачено спеціальним законом; б) громадськість має доступ до них відповідно до правових положень, що регулюють доступ до інформації публічного сектора; в) повідомлення здійснюється відповідно до національного законодавства про захист інформації; г) 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 дані зібрані (п. 2).

Як регулятор обігу особистої інформації про здоров'я особи використовується Рекомендація № R (97) 5 Комітету Міністрів державам-членам Ради Європи щодо захисту медичних даних [7]. У п. 6 даного акту визначено гарантований перелік прав суб'єкта даних. Він 1) має бути поінформованим про файл з інформацією про його медичні дані, тип зібраних, або таких, що мають бути зібрані, даних; 2) має володіти інформацією про мету обробки; 3) мати інформацію про осіб чи органи, в яких є дані; 4) має

можливість надати згоду та відкликати її; 5) може володіти інформацією про здійснення права на доступ та внесення поправок до даних. Суб'єкт повинен бути поінформований не пізніше моменту збору даних, окрім випадків, коли медичні дані отримуються не від суб'єкта, тоді інформування повинно відбутись якомога раніше (п. 7). У Рекомендації R 89 (2) КМ Ради Європи встановлено пріоритети щодо процедури збору та обробки персональних даних, що використовуються для потреб працевлаштування. Зокрема, встановлено, що в процесі наймання працівника дані, що збираються, повинні обмежуватися тим обсягом, який є необхідним для оцінки придатності кандидатів та їхнього потенціалу з точки зору кар'єри, здачі іспитів та аналогічних процедур, необхідних для оцінки характеру та особистості людини. Усе це має відбуватися лише за її згодою та у випадку, коли внутрішнє законодавство передбачає належні застережні заходи (п. 4) [8].

На законодавчому рівні врегульовані окремі питання надання телекомунікаційних послуг із дотриманням вимог законодавства про захист персональних даних. Міжнародне законодавство приділяє значну увагу регулюванню обігу та юридичного захисту інформації про особу в електронних мережах, включаючи Інтернет. Так, Генеральна Асамблея ООН винесла резолюцію № 95 (XLV), якою затвердила «Керівні принципи регулювання комп'ютерних файлів, які містять персональні дані» (Guidelines for the Regulation of Computerized Personal Data Files [9]). У зазначеному керівному документі запроваджується застосування основоположних принципів електронної обробки, зберігання персональних даних та доступу до них суб'єктів. Це: 1. Принцип законності та справедливості, за яким інформація про осіб не повинна бути зібрана чи оброблена несправедливо або незаконно і не повинна використовуватися для цілей, що суперечать цілям та принципам Статуту Організації Об'єднаних Націй. 2. Принцип точності, який передбачає, що особи, відповідальні за складання файлів або за їх зберігання, зобов'язані проводити регулярні перевірки точності та відповідності даних, які зафіксовано, та щоб вони були максимально повними, щоб уникнути помилки пропущення і щоб вони оновлювалися регулярно або коли інформація, що міститься в файлі, використовується або обробляється. 3. Принцип призначення-специфікації, за яким мета, якій файл повинен служити, має бути визначеною, законною і, коли вона встановлена, має бути доведеною до відома зацікавленої особи, аби згодом забезпечити, щоб: (а) усі зібрані та зареєстровані особисті дані залишалися актуальними та адекватними зазначеній меті; (б) жодне із зазначених особистих даних не використовується та не розголошується (крім випадків, коли це було за згодою зацікавленої особи) для цілей, несумісних із зазначеними; (с) період, протягом якого зберігаються персональні дані, не перевищує такий, що буде дозволяти досягнення поставлених цілей. 4. Принцип доступу зацікавлених осіб, який вказує, що кожен, хто пропонує докази ідентифікації, має право знати, чи інформація щодо нього обробляється та про її отримання в зрозумілій формі, без зайвих затримок;

також мати можливість зробити відповідні виправлення або стирання у випадку незаконних, непотрібних або неточних записів і, коли дані комусь повідомляються, бути поінформованим про адресатів. 5. Принцип недискримінації, який передбачає, що дані, які можуть призвести до незаконної або довільної дискримінації, включаючи інформацію про расову чи етнічну приналежність, походження, колір, сексуальне життя, політичні погляди, релігійні, філософські та інші вірування, не повинні бути складеними.

Питання захисту персональних даних у мережі Інтернет та відповідні принципт, якими в цій діяльності повинні керуватися країни-учасниеи ЄС, викладені в Рекомендації № (99) 5 Комітету Міністрів Ради Європи щодо захисту недоторканності приватного життя в інтернеті [10]. Попри те, що вони мають рекомендаційний характер, їх можна використовувати під час визначення загальних процедур обробки персональних даних у мережі Інтернет. Керівні принципи рекомендують користувачам та постачальникам послуг порядок поведінки в цій мережі. Користувачам слід пам'ятати, що Інтернет – небезпечна мережа. Зокрема, необхідно використовувати всі доступні засоби для захисту даних та ліній зв'язку, легально доступні засоби шифрування для конфіденційності електронної пошти, коди доступу до власного персонального комп'ютера. Будь-яка трансакція, будь-яке відвідування сайту залишає в інтернеті слід. Подібні «електронні сліди» можуть бути використані без відома суб'єкта персональних даних для створення профілю про нього і його інтереси. Якщо такий збір інформації є небажаним, варто використовувати новітні технічні досягнення, що дозволяють проінформувати суб'єкта персональних даних про будь-який випадок можливості залишення відповідних «слідів» і відмовитися від подальших дій. При цьому найкращий спосіб забезпечення недоторканності приватного життя – це анонімний доступ і анонімне використання послуг, анонімні засоби здійснення платежів. За можливістю слід з'ясовувати наявність технічних засобів для забезпечення анонімності. Повна анонімність не завжди можлива через певні законодавчі обмеження. У такому випадку, якщо це дозволено законодавством, варто використовувати псевдонім, що дозволить знати персональні дані суб'єкта тільки постачальникові послуг інтернету (п. 1-4).

На забезпечення поваги до приватного життя спрямована і Рекомендація № R (95) 4 щодо захисту даних особистого характеру у сфері телекомунікаційних послуг 1995 року [11]. Так, вона встановлює, що телекомунікаційні послуги і, зокрема, телефонні послуги, що розвиваються, повинні бути запропоновані з повагою до приватного життя користувачів, дотриманням таємниці листування та свободи комунікаційних обмінів даними. Оператори мережі і постачальники послуг або матеріального і програмного обладнання мали б отримувати користь від інформаційних технологій для продукування і експлуатації мереж, устаткування і програмного забезпечення дотримуючись права на приватне життя користувачів. Можливості анонімного доступу до мережі і до телекомунікаційних послуг повинні

бути надані в доступне розпорядження. Будь-яке втручання в зміст комунікації або операторами мережі, або постачальниками послуг повинно бути заборонене, за винятком, якщо це не є дозволеним із 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 (п. 2). У даному напрямку діє і низка інших Рекомендацій КМ ЄС.

Ураховуючи високу актуальність досліджуваної проблематики, за ініціативою Комісару ЄС із захисту даних у різних країнах для покращення конфіденційності та захисту відомостей у телекомунікаціях та ЗМІ була створена Міжнародна робоча группа на захист даних у телекомунікаціях. Вона напрацювала і затвердила Рекомендації з питань захисту персональних даних у телекомунікаційній сфері (Берлінська група) від 7 вересня 2010 року [12]. Вони містять окремі організаційно-технічні принципи обробки та зберігання персональних даних. Зокрема, рекомендації стосуються застосування механізмів глибокої перевірки пакетів (DPI) – технології, яка автоматизує інспекцію інформаційних пакетів у реальному або майже реальному часі. Незважаючи на те, що ДПІ не можна вважати новою технологією, вона використовувалася протягом багатьох років під час виявлення вторгнення і системи профілактики, а також у системах брандмауера, що надало додаткові можливості: це дозволило збільшити потужність і зробити більш ефективними алгоритми для керування трафіком, посилити контроль над розповсюдженням незаконного чи небажаного вмісту, в тому числі захищеного авторським правом матеріалу.

Разом із тим застосування цієї технології може поставити під загрозу конфіденційність користувачів Інтернету. Зокрема, певне використання технологій ДПІ постачальниками послуг Інтернету може призвести до серйозних порушень конфіденційності користувачів. Провайдери доступу є «шлюзом до віртуального світу», вони технічно здатні стежити за вмістом всього спілкування користувача Інтернету. Тому дуже важливо, щоб провайдери доступу до мережі поважали секретність телекомунікацій, як це передбачено в правових рамках із багатьох юрисдикцій. У світлі вищесказаного Робоча група закликає постачальників послуг Інтернету спеціально утримуватися від використання технології DPI для цілеспрямованої / поведінкової реклами. Крім того, Робоча група закликала до більш широкого застосування безпечного повного коду застосовуваних механізмів.

До міжнародно-правового регулювання питань щодо захисту права особи на недоторканність приватного життя особи загалом і захисту її персональних даних зокрема віднесено і рішення Європейького суду з прав людини. Адже саме цей орган компетентний застосовувати, тлумачити та конкретизувати положення Конвенції про захист прав людини і основоположних свобод. В окремих державах-членах Ради Європи згідно з внутрішніми законами прецедентні рішення ЄСПЛ поряд із нормами Конвенції визнано складовою частиною національного законодавства. Зокрема,

то встановлено українським законом «Про виконання рішень та застосування практики Європейського суду з прав людини» від 23 лютого 2006 року (ст. 17). Європейський суд із прав людини приділяє досить серйозну увагу захисту особистої інформації про особу і досить активно реагує на порушення державами-учасниками Конвенції прав громадян на охорону їхніх персональних даних. Так, у справі «Копланд проти Сполученого Королівства» ЄСПЛ визнав порушення статті 8 Конвенції щодо моніторингу інформації про телефонні дзвінки, використання електронної пошти чи інтернету працівницею за відсутності відповідного закону для такого втручання, хоча не виключив ситуації, що такий моніторинг може в деяких випадках бути визнано «необхідним у демократичному суспільстві» і із законною метою, проте з огляду на відсутність законності втручання ЄСПЛ не розглядав питання необхідності в цій справі [13, п. 44]. Відповідно до практики Суду телефонні дзвінки з ділових приміщень охоплюються поняттями приватного життя та кореспонденції в цілях ч.1 ст. 8 Конвенції [14, п. 42, 44]. Звідси логічно випливає, що відправлені з роботи електронні листи також повинні захищатися на підставі ст. 8 Конвенції, як і інформація, отримана з відстеження приватного використання мережі Інтернет. Заявниця в цій справі не була попереджена про те, що її дзвінки можуть бути піддані відстеженню, тому вона обґрунтовано сподівалася на приватність дзвінків, зроблених із її робочого телефону. Таке ж очікування мала заявниця і щодо електронної пошти та використання мережі Інтернет. Відповідно, Суд вважає, що збирання та збереження особистої інформації щодо телефонних контактів заявниці, а також щодо її електронної пошти та користування мережею Інтернет, без її відома становлять втручання в право на повагу до приватного життя та кореспонденції в розумінні ст. 8 Конвенції.

ЄСПЛ застосовує положення Конвенції про захист персональних даних у разі вчинення державами-відповідачами правопорушень у даній царині, які можуть мати різні прояви. Свої пріоритети Суд виклав у п. 43 Рішення в справі «Ротару проти Румунії», зазначивши, що мета Конвенції про захист прав фізичних осіб під час автоматизованої обробки персональних даних полягає в тому, щоб гарантувати кожній приватній особі дотримання її прав і основних свобод, і особливо права на особисте життя в аспекті автоматизованої обробки даних особистого характеру. Це ще більш вірно в разі, коли мова йде про дані, що зачіпають віддалене минуле особи [15, п. 43]. Порушення порядку доступу до персональних даних фізичних осіб часто отримують правову реакцію Європейського суду з прав людини і стосовно держави України. У рішенні «Сергій Волосюк проти України» Суд, встановивши недотримання державою принципів щодо таємниці спілкування, розкрив основні вимоги до права на повагу до приватного і сімейного життя і кореспонденції, гарантованого статтею 8 Конвенції. Зокрема, Суд зазначає, що сторони не заперечували того, що перевірка кореспонденції заявника, здійснювана посадовими особами установи, в якій

його тримали під вартою, становила втручання в право заявника на повагу до своєї кореспонденції, гарантоване пунктом 1 статті 8 Конвенції. ЄСПЛ також зазначив, що таке втручання суперечить статті 8 Конвенції, якщо воно здійснюється не «згідно із законом», не має однієї або кількох легітимних цілей, зазначених у пункті 2 статті 8 Конвенції, а також не є «необхідним у демократичному суспільстві» для досягнення цих цілей [16, п. 81].

Із проведеного в даній роботі дослідження можемо зробити певні висновки. Згідно з міжнародно-правовими актами, які регулюють механізми обороту та захисту особистої інформації про людину, поняття захисту персональних даних розуміється досить широко та багатогранно. За усталених правових підходів воно охоплює такі єлементи, як обов'язок володільця здійснювати організаційні та технічні заходи задля належного з легітимною метою збирання та обробки даних, отримання згоди суб'єкта даних, запобігання їх випадкової втрати, пошкодження чи знищення, обробки в незаконний спосіб, неправомірного доступу до персональних даних. Також, за практикою міжнародного правотворення та правозастосування, важливим є обов'язок володільця і розпорядника не допускати розголошення персональних даних, які стали йому відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків. Дане зобов'язання конфіденційності є ключовим елементом під час дотримання прав суб'єкта персональних даних. При цьому володілець персональних даних самостійно повинен визначати, яких заходів слід вживати з метою забезпечення їхнього захисту. Для реалізації вказаних функцій вбачається за необхідне кожному володільцеві або розпоряднику здійснити розробку моделей можливих загроз і потенційних категорій порушників. Конкретні характеристики вказаного моделювання, звісно, будуть залежати від порядку обробки інформації (наприклад, від того, обробляються дані в електронних системах чи в картотеках), різних рівнів технічних ознак інформаційних систем, а також враховувати постійний стрімкий розвиток інформаційних технологій і програмного забезпечення, а відтак – підвищення рівня посягань та виникнення нових видів загроз.

Література:

1. Садикова И.С. Защита персональных данных в аспекте обеспечения неприкосновенности частной жизни. Вестник экономики, права и социологии. 2012. № 3. Серия право. С. 217–219.
2. Вельдер И.А. Система правовой защиты персональных данных в Европейском Союзе: дис. ... канд. юрид. наук. Казань, 2006. 165 с.
3. Конвенція про права дитини. ООН; Конвенція, від 20 листопада 1989 року. URL: http://zakon5.rada.gov.ua/laws/show/995_021.
4. Хартія основних прав Європейського Союзу Європейський Союз; Хартія, Міжнародний документ від 07 грудня 2000. року. URL: http://zakon2.rada.gov.ua/laws/show/994_524.
5. Рекомендація № 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.
6. Рекомендація № R (91) 10 Щодо передачі третім особам інформації особистого характеру, яка знаходиться в розпорядженні органів від 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/.
7. Рекомендація R11(97) 5 щодо захисту медичних даних від 13.02.1997. URL: http://www.umj.com.ua/article/37381/rekomendacii-radi-yevropi-shhodo-zaxistumedichnix-danix.
8. Рекомендація R 89(2) Комітету Міністрів Ради Європи державам-членам про захист персональних даних, що використовуються для потреб працевлаштування. Порівняльно-правове дослідження відповідності законодавства України законодавству ЄС у сфері персональних даних. К.: 2006. С. 239–242.
9. Guidelines for the Regulation of Computerized Personal Data Files Adopted by General Assembly resolution 45/95 of 14 December 1990. URL: http://www.refworld.org/pdfid/3ddcafaac.pdf.
10. Рекомендація N R (99) 5 Комітету Міністрів державам-членам Ради Європи «Про захист недоторканності приватної власності в Інтернеті». Міжнародний документ від 23.02.1999 року. URL: http://zakon2.rada.gov.ua/laws/show/994_357.
11. Рекомендація № R (95) 4 Щодо захисту даних особистого характеру в сфері телекомунікаційних послуг від 7 лютого 1995 року. URL: http://cedem.org.ua/library/rekomendatsiya-r-95-4-shhodo-zahystu-danyh-osobystogo-harakteru-v-sferi-telekomunikatsijnyh-poslug/.
12. International Working Group on Data Protection in Telecommunications. Report and Guidance on Data Protection and Privacy on the Internet 48th meeting, September 6-7, 2010. "Budapest – Berlin Memorandum". URL: http://www.datenschutz-berlin.de/attachments/138/bbmem_en.pdf?1200577389.
13. Рішення ЄСПЛ від 3 квітня 2007 року у справі «Копланд проти Сполученого Королівства» (Copland v. the United Kingdom), заява № 62617/00. URL: https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001.
14. Рішення ЄСПЛ від 25 червня 1997 року у справі «Халфорд проти Сполученого Королівства» (Halford v. the United Kingdom), заява № 20605/92. URL: http://swarb.co.uk/halford-v-the-united-kingdom-echr-25-jun-1997/.
15. Рішення ЄСПЛ від 4 травня 2000 року у справі «Ротару проти Румунії» (Rotaru v Romania), заява № 28341/95. URL: http://eurocourt.in.ua/Article.asp?AIdx=212.
16. Рішення ЄСПЛ від 12 березня 2009 року у справі «Сергій Волосюк проти України» (Sergey Volosyuk v. Ukraine), заява № заява № 1291/03. URL: old.minjust.gov.ua/file/1716.docx.

Гуйван П. Д. Отдельные вопросы международно-правового регулирования оборота и защиты персональных данных

Аннотация. Статья посвящена вопросам регулирования оборота и защиты персональных данных в правовых актах международного законодательства, которые имеют локальное и отраслевое назначение. Проводится анализ положений отдельных Рекомендаций Комитета Министров ЕС, направленных на установление правил обращения данных о личности в различных сферах деятельности, также анализируется мировая и европейская

правотворческая работа в области обработки и защиты персональных данных в электронных сетях, в частности в Интернете. Проведено обобщение юридических подходов, отмечены общие позиции к определенности механизмов. Рассмотрено их практическое применение Европейским судом по правам человека.

Ключевые слова: оборот персональных данных, правовая защита личной информации.

Guyvan P. Separate issues of international legal regulation of turnover and protection of personal data

Summary. The article is devoted to the regulation of turnover and the protection of personal data in legal acts of international law, which have a local and industrial purpose. The analysis of the provisions of the individual Recommendations of the Committee of Ministers of the EU aimed at establishing rules for the circulation of personal data in various fields of activity is also being analyzed, and global and European law-making work is being analyzed in the field of processing and protecting personal data in electronic networks, particularly on the Internet. A generalization of legal approaches has been made, general positions have been noted for the certainty of the mechanisms. Considered their practical application by the European Court of Human Rights.

According to international legal acts that regulate the mechanisms for the circulation and protection of personal information about a person, the concept of protecting personal data is understood quite widely and multifaceted. According to the established legal approaches, it covers such elements as the duty of the owner to carry out organizational and technical measures for properly collecting and processing data, obtaining consent of the data subject, preventing their accidental loss, damage or destruction, illegal processing, unauthorized access to personal data . Also, in the practice of international lawmaking and law enforcement, it is important that the owner and the manager do not allow the disclosure of personal data that he or she has become aware of in connection with the performance of professional or official or work duties. This confidentiality obligation is a key element in respect of the rights of the subject of personal data. At the same time, the owner of personal data must independently determine what measures should be taken to ensure their protection.

Key words: turnover of personal data, legal protection of personal information.