УДК 342.9:347.121.1

Михайло Різак,

канд. юрид. наук, помічник-консультант народного депутата України Верховної Ради України

ПРАКТИКА КРАЇН ЄВРОПЕЙСЬКОГО СОЮЗУ ТА УКРАЇНИ У СФЕРІ СУДОЧИНСТВА ЩОДО ГАРАНТУВАННЯ БЕЗПЕКИ ОБІГУ ТА ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

У статті визначено поняття обігу та обробки персональних даних; охарактеризовано деякі показові рішення національних судів країн ЄС та України з аналізованої проблематики; розглянуто світову практику щодо обігу та обробки персональних даних у соціальних мережах; встановлено види застосовуваних санкцій за порушення в цій сфері.

Ключові слова: персональні дані, безпека, обіг, обробка, Європейській Союз, судочинство.

Постановка проблеми. У сучасному європейському просторі забезпечення та захист прав людини посіли чільне місце серед пріоритетів державної політики. Україна приєдналася до низки міжнародно-правових актів у цій сфері, а Конституція проголосила людину, її життя і здоров'я, честь і гідність, недоторканність і безпеку найвищою соціальною цінністю[1].

У вітчизняному правовому полі використано типове європейське правове розуміння персональних даних, існує відповідна дефініція. Більше того, триває його адаптація до європейських норм. Ефективне гарантування безпеки обігу та обробки персональних даних неможливо забезпечити, розглядаючи його тільки як окрему, самодостатню мету і не беручи до уваги те, що в кінцевому результаті вся система безпеки обігу та обробки персональних даних – це невід'ємна складова частина загальної системи забезпечення фундаментальних прав людини і громадянина. Адже йдеться про одну з найважливіших ліберально-демократичних свобод – право на недоторканність приватного життя.

Окремі питання у сфері захисту персональних даних досліджували такі вчені, як: Л. В. Борисова, В. М. Брижко, І. О. Вельдер, В. Д. Гавловський, В. С. Гербут, Р. Кірін, О. В. Кохановська, А. В. Кучеренко А. М. Чернобай та інші. Натомість проблеми обігу та обробки персональних даних, що знайшли своє відображення в судочинстві країн ЄС та України, залишилися недослідженими, хоча за своєю значущістю для забезпечення безпеки у зазначеній сфері судова практика посідає важливе місце.

Метою статті є дослідження практики країн Європейського Союзу та України у сфері національного судочинства щодо гарантування безпеки обігу та обробки персональних даних. Досягнення поставленої мети передбачало вирішення таких завдань: визначити поняття обігу та обробки персональних даних; охарактеризувати деякі показові рішення національних судів країн ЄС та України з аналізованої проблематики; розглянути світову практику щодо обігу та обробки персональних даних у соціальних мережах; встановити види застосовуваних санкцій за порушення з аналізованої проблематики.

Виклад основного матеріалу. Слід констатувати, що обіг та обробка персональних даних є взаємозв'язаними правовими категоріями. Згідно зі ст. 2 Закону України «Про захист персональних даних», обробка персональних даних – будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем [3]. Наведене визначення є занадто розпливчастим і логічно непослідовним, адже насправді обробка передбачає здійснення з персональними даними певних дій для отримання якісно нової інформації.

Під обігом персональних даних слід розуміти будь-яку дію або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, вилучення, поновлення, копіювання і поширення (розповсюдження, реалізація, передача), у тому числі з використанням інформаційних (автоматизованих) систем, щодо персональних даних, у результаті яких ці дані не змінюються, у свою чергу обробка персональних даних – це будь-яка дія або сукупність дій щодо персональних даних з метою отримання нової інформації [2, с. 26]. Отже, основним критерієм розмежування обігу та обробки персональних даних є змінюваність останніх (у разі обігу персональні дані поширюються без зміни їх змісту та суті, а в разі обробки створюються нові дані, які можуть мати статистичний або персональний характер).

Оскільки вказані правові категорії є різними за значенням, необхідно їх розмежовувати у Законі України «Про захист персональних даних», що позитивно вплине на правозастосовну практику.

Переходячи до розгляду зазначеної практики, розглянемо судочинство щодо гарантування безпеки обігу та обробки персональних даних у країнах ЄС та України.

Приміром, Суд Європейського Союзу 06.10.2015 оголосив недійсною угоду про обмін даними між США та країнами ЄС, відому під назвою "Safe Harbor". Підставою для такого рішення стали значно нижчі, ніж в ЄС, стандарти та норми гарантування безпеки обігу та обробки персональних даних у США. Згідно з рішенням суду, громадяни країн ЄС можуть тепер звертатися з відповідними позовами до національних судів своїх країн, а профільні органи влади з безпеки персональних даних окремих країн ЄС правомочні перевіряти, чи дійсно дані тієї чи іншої особи в Сполучених Штатах захищаються відповідним чином. Утім, рішення суду може зачепити не так великі, як насамперед маленькі компанії, які користувалися "Safe Harbour" для безпроблемного і швидкого трансферу даних на американські сервери. Таким гігантам, як Google чи Facebook, що мають великий штат юристів, імовірно, значно легше розробити нові угоди про передачу даних і без правил "Safe Harbor" та запропонувати користувачам погодитися на нові умови. Аргументацією обвинувачення у суді, яку зрештою було взято до уваги, послужив, зокрема, той факт, що у США державні спецслужби, такі як АНБ, мають порівняно легкий доступ до особистих даних користувачів Інтернету ніж у Євросоюзі [4]. Таким чином, в ЄС створено прецедентну судову практику, на підставі якої кожен громадянин держави, що входить до складу ЄС, може захистити своє право на безпеку персональних даних та на їх нерозголошення третім особам.

Іншим показовим прикладом, коли найвищі судові інстанції ЄС стають на бік захисту персональних даних конкретних осіб, є рішення Європейського суду, за яким користувач, незадоволений інформацією, отриманою в результаті інтернет-пошуку про себе, може звернутися безпосередньо до пошукової системи. Якщо компанія вважатиме зайвим видалення даних, громадянин ЄС має право оскаржити рішення компанії-пошукової системи в прокуратурі або в суді.

У 2010 р. Маріо Костеха Гонсалес подав у Іспанське агентство захисту даних (AEPD) скаргу на Google Inc., Google Spain і видавничий дім La Vanguardia Ediciones SL. Він звернув увагу на те, що за запитом його імені в Google пошукова система видала посилання на дві сторінки каталонської газети La Vanguardia, що датуються 1998 р. і містять інформацію про те, що на його будинок накладено арешт за борги. Позивач вимагав видалити або приховати відомості, що стосуються його персональних даних таким чином, щоб вони більше не з'являлися в результатах пошуку. За його словами, розгляд, пов'язаний з арештом майна, давно припинено, тому інформація La Vanguardia 16-річної давності втратила актуальність. AEPD відхилило скаргу іспанця на газету, але зажадало від Google Inc. і Google Spain припинити індексацію зазначених сторінок. Інтернет-корпорація у відповідь подала позов стосовно AEPD у Національний високий суд Іспанії, заявивши про незаконність рішення агентства. Іспанський суд скерував серію запитів до Європейського суду, який постановив, що за певних обставин пошукові системи повинні видаляти посилання на веб-сторінки, які опубліковані третіми особами і містять інформацію, що стосується людини, на основі імені якої зроблений пошуковий запит. Згідно з рішенням суду, в деяких випадках пошукові системи повинні видаляти посилання навіть за умови, якщо інформація, на яку вони ведуть, є законною. Суд зазначає, що слід шукати справедливий баланс між інтересами користувачів і людей, які захищають свої персональні дані. Суд підкреслює, що видаленню підлягають неадекватні і застарілі дані, а також надмірні стосовно цілей, для яких вони одного разу були розміщені в Інтернеті [5].

Так було створено ще один судовий прецедент в інтересах позивача та невизначеного кола осіб щодо гарантування безпеки персональних даних.

На жаль, дослідження вітчизняної судової практики щодо захисту персональних даних свідчить про недостатній рівень нормативного забезпечення прав фізичних осіб у цій сфері. Показовим є рішення Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ у справі № 6-25324ск14 щодо внесення персональних даних до автоматизованої системи бази даних «Укрзалізниці». Зокрема, зазначено, що прізвище та ім'я особи не є персональними даними, оскільки за ними неможливо ідентифікувати особу. Для ідентифікації конкретної особи за прізвищем та іменем необхідні додаткові дані про неї. Відповідно до листа Міністерства юстиції України від 15 листопада 2013 року № 13232-0-26-13/61, у якому зазначено, що Рекомендацією CM/Лес (2010) Комітету Міністрів Ради Європи державам-членам щодо захисту осіб у зв'язку з автоматизованою обробкою персональних даних у контексті їх профілювання визначено, що під персональними даними розуміється виключно інформація, за допомогою якої особа ідентифікується або може бути ідентифікована. Прізвище та ім'я пасажирів зазначаються у проїзному документі з метою оформлення проїзних, перевізних документів відповідно до вимог чинного законодавства, а саме Закону України «Про залізничний транспорт», Порядку обслуговування громадян залізничним транспортом, затвердженого Постановою КМУ від 19 березня 1997 року № 252, та Правил перевезення пасажирів, багажу, вантажобагажу та пошти залізничним транспортом України, затверджених наказом Міністерства транспорту та зв'язку України від 27 грудня 2006 року № 1196, тобто прізвище та ім'я пасажирів обробляються на підставі та у порядку, передбаченому чинним законодавством [6].

Вказане рішення викликає низку зауважень, серед яких основними є такі: 1) суд віддає перевагу не захисту прав людини, а потребам державного залізничного транспорту, так би мовити, «входить у становище»; 2) наявна колізія

юридичних норм могла бути вирішена шляхом внесення змін до Закону України «Про залізничний транспорт» та підзаконних нормативно-правових актів; 3) прізвище та ім'я є достатніми персональними даними, за якими можна не просто ідентифікувати, а конкретно ідентифікувати фізичну особу з-поміж інших пасажирів, а тому такі дані мають бути належно захищеними. У зв'язку з цим національне законодавство у сфері безпеки обігу та обробки персональних даних потребує подальшого розвитку, а нормативно-правові акти мають бути приведені у відповідність до міжнародних стандартів гарантування безпеки персональних даних.

Необхідно відзначити, що загальний інтерес до права на приватність зріс ще у 60-70-ті роки XX століття з появою перших інформаційно-комунікативних технологій (в їх сучасному розумінні) і активізацією інформаційних обмінів. Потенційні можливості стеження та збору за допомогою комп'ютерних систем вимагали встановлення спеціальних правил щодо обробки та обігу інформації особистого характеру. Основи сучасного законодавства в цій сфері закладено першим у світі законом про захист даних, який було введено в дію на землі Гессен у Німеччині в 1970 році. Наступними були національні законодавчі акти Швеції (1973), Сполучених Штатів (1974), Німеччини (1977) та Франції (1978) [7, с. 13]. Із часом процеси розвитку інформаційного суспільства поглиблювалися, а на перший план вийшли питання балансу забезпечення інформаційної безпеки людини та держави.

За оцінками фахівців, станом на початок 2017 року кількість користувачів глобальної інформаційної системи Інтернет сягає більше 3,7 мільярдів осіб [8].

Безумовно, розвиток мережі Інтернет і прагнення до забезпечення безпеки персональних даних на національному та міжнародному рівнях в окремих європейських країнах зумовили формування національного законодавства та вироблення власної судової практики у досліджуваній сфері. Так, федеральний закон Німеччини «Про захист даних» 1977 р. передбачав два основних завдання: по-перше, попередити втручання у приватну сферу громадян Німеччини за допомогою нової інформаційної техніки; по-друге, не допустити зміни визначених конституцією країни розподілу повноважень у зв'язку з виникненням «інформаційних переваг» виконавчих органів влади перед парламентськими органами. Громадяни Німеччини з приводу розголошення своїх персональних даних мають право самостійно приймати рішення, а захист їхніх прав із цього питання здійснює незалежний уповноважений із захисту персональних даних. Сьогодні захист персональних даних у країні здійснюється відповідно до положень федерального закону «Про подальший розвиток обробки і захисту даних» від 20.12.1990, згідно з яким персональні дані перебувають під захистом тільки тоді, коли вони застосовуються у приватному житті й виконують певну громадську чи економічну функцію життєдіяльності [9].

Основними організаційно-правовими елементами системи захисту персональних даних у Німеччині є: 1) ведення реєстру файлів (§ 26 Закону 1990 р.) і баз персональних даних (§ 32 Закону 1990 р.) щодо державних і недержавних структур; 2) ведення реєстру пристроїв ЕОМ і нагляд за застосуванням програм обробки персональних даних (§ 18 Закону 1990 р.); 3) здійснення контролю (перевірки) діяльності з персональних даних у різних організаціях (§ 24, 38 Закону 1990 р.), оскарження порушень щодо положень Закону, заява протесту на незаконні дії (§ 25, 38 Закону 1990 р.) [9].

3 липня 2009 року парламентом Німеччини прийнято зміни до федерального закону «Про захист даних», що стосувалися даних, які використовуються в маркетингу, у повідомленнях про порушення безпеки, в оформленні договорів, а також даних працівників. Зміни передбачають нові повноваження для органів захисту персональних даних та встановлюють нові суми штрафів за порушення в цій сфері.

Зокрема, обробка та використання персональних даних маркетинговими службами з метою просування різних товарів і послуг, якто адреси та контактні дані, дозволені тільки в тому разі, якщо людина дала на це окрему особисту згоду. Встановлено вимоги про повідомлення про порушення інформаційної безпеки: зокрема, оператор персональних даних є суб'єктом вимог про обов'язкове повідомлення постраждалих у разі витоку їх персональних даних. Вимоги про повідомлення поширюються на такі категорії даних: 1) конфіденційні дані; 2) персональні дані з урахуванням професійних або службових обов'язків (наприклад, дані, що зберігаються в юридичних та медичних організаціях); 3) дані, що стосуються кримінальних або адміністративних правопорушень; 4) дані щодо банківських або кредитних карт; 5) дані клієнтів або дані трафіку згідно з визначенням в телекомунікаційному законодавстві (наприклад, дані, що зберігаються в операторів зв'язку, такі як персональні дані абонента і дані трафіку); 6) дані клієнтів або експлуатаційні характеристики згідно з визначенням у Законі про теле- і радіомовлення (наприклад, дані, які використовуються для надання електронних інформаційних та комунікаційних послуг, включаючи реєстраційні та інші використовувані дані, за якими можна ідентифікувати окремих користувачів). Повідомлення потрібне в разі незаконної передачі даних або несанкціонованого доступу третьої сторони, якщо витік даних може мати серйозні наслідки для захисту прав та інтересів зацікавлених осіб. За необхідності оператор персональних даних повинен негайно повідомити відповідний орган із захисту даних, а також постраждалих осіб.

Вищевказані сторони повинні бути повідомлені про витік після: (а) вжиття відповідних заходів щодо захисту скомпрометованих даних і (б) закінчення кримінального розслідування. Крім того, закон встановлює певні мінімальні вимоги до змісту повідомлення [10].

Федеральний конституційний суд ФРН 02.03.2017 ухвалив, що німецький закон щодо

масового зберігання даних про будь-які телефонні переговори і листування електронною поштою в його нинішній формі неприйнятний і суперечить конституції. Судді також зажадали негайно знищити ту інформацію, яка вже накопичена в банках даних. Річ у тому, що телекомунікаційні компанії з 2008 року були зобов'язані протягом півроку зберігати інформацію про всі переговори своїх клієнтів за звичайними і мобільними телефонами, а також електронною поштою і через Інтернет, а за необхідності передавати цю інформацію в розпорядження поліції і спецслужб. Цей закон у рамках найбільшого на сьогодні колективного позову оскаржили 35 тисяч громадян Німеччини. Конституційний суд зазначив, що саме по собі зберігання таких даних допустимо, але за умови, якщо в законі буде ясно прописано, в яких випадках і для чого саме можуть бути використані ці дані, і якщо під час їх збирання і зберігання буде дотримано суворих заходів безпеки і прозорості, повідомляє агентство AFP[11].

Ці та інші непоодинокі факти сприяють забезпеченню прав громадян Німеччини щодо недоторканності приватного життя, нерозголошення персональних даних тощо. Вирішуючи конкретні справи, суди виходять із принципів справедливості та верховенства права, що відповідає європейським цінностям. Однак дедалі частіше трапляються випадки порушення прав людини щодо безпеки персональних даних з боку провайдерів, інтернет-компаній, соціальних мереж, операторів телефонного зв'язку тощо. Водночас серед різноманіття застосовуваних заходів переважають штрафи у певній сумі або у відсотках з обороту.

Так, Нацкомісія з інформаційних технологій і свободи Франції (CNIL) оштрафувала соцмережу Facebook на 150 тис. євро за результатами вибіркової перевірки документів соцмережі з метою контролю дотримання закону про захист персональних даних користувачів після змін у політиці Facebook у 2015 році. За даними французького регулятора, виявлено численні порушення компанією законодавства. Так, Facebook масово використовувала особисті дані користувачів для адресної реклами. Крім того, соцмережа стежила за пошуковими запитами своїх користувачів за допомогою cookies, що містять історію відвідин сайтів і, відповідно, інформацію про вподобання [12].

Незрозумілим залишається критерій, за яким визначено суму штрафу. За офіційною інформацією, в 2016 році компанія Facebook отримала $10,217 млрд. чистого прибутку, дохід становив $27,638 млрд. Зростання чистого прибутку порівняно з 2015 роком сягнув 177 %, доходів – 54 % [13]. За таких обставин розмір штрафу для транснаціональної компанії є незначним та не відповідає характеру правопорушення. Доцільно було б застосувати штрафні санкції залежно від отриманих доходів компанії в Європі, і зокрема у Франції, за проміжок часу, коли мало місце порушення законодавства про захист персональних даних.

Стандартами захисту персональних даних Євросоюзу (European Data Protection Regulation) встановлено, що в якості санкцій недобросовісному операторові персональних даних може бути виписано попередження за перше порушення, накладено штраф у розмірі від 250 тис. євро або 0,5 % від обороту за незначні порушення і штраф у розмірі до 1 млн. євро або до 2 % від загальносвітового річного обігу компанії у разі завдання збитку суб'єктам персональних даних [14, с. 26].

З урахуванням викладеного, удосконалюючи вітчизняне законодавство, слід запроваджувати не фіксовані штрафні санкції, а стягнення у відсотках з доходу, розмір якого може становити від 0,5 % до 2 % доходу залежно від ступеня тяжкості правопорушення та інших обставин, помножений на проміжок часу, коли тривало порушення законодавства у сфері захисту персональних даних. Запровадження таких санкцій може стати ефективним інструментом гарантування безпеки персональних даних.

Список використаних джерел:

1. Конституція України від 28.06.1996 № 254к/96-ВР // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.

2. Різак М.В. Співвідношення понять «обіг» та «обробка» персональних даних: термінологічні аспекти / М. Різак // Віче. – 2013. – № 8. – С. 25–26.

3. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – С. 1188. – Ст. 481.

4. Суд ЄС: дані користувачів Facebook недостатньо захищені в США [Електронний ресурс]. – Режим доступу : http://www.dw.com/uk/%D1%81%D1%83%D0%B4-%D1%94%D1%81%D0%B4%D0%B0%D0%BD%D1%96-%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D1%83%D0%B2%D0%B0%D1%87%D1%96%D0%B2-facebook-%D0%BD%D0%B5%D0%B4%D0%BE%D1%81%D1%82%D0%B0%D1%82%D0%BD%D1%8C%D0%BE-%D0%B7%D0%B0%D1%85%D0%B8%D1%89%D0%B5%D0%BD%D1%96-%D0%B2-%D1%81%D1%88%D0%B0/a-18763358

5. Суд ЄС зобов'язав Google видаляти застарілі персональні дані [Електронний ресурс]. – Режим доступу : http://zib.com.ua/ua/84960-sud_es_zobovyazav_google_vidalyati_zastarili_personalni_dani.html

6. Рішення Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ по справі №6-25324ск14 від 18.07.2014 [Електронний ресурс]. – Режим доступу : http://www.reyestr.court.gov.ua/Review/39797551

7. Свобода інформації та право на приватність в Україні / Харківська правозахисна група ; худож.-оформлювач О. Герчук. – Харків: Фоліо, 2004. – Том 2. Право на приватність: conditio sine qua non. – 200 с.

8. TOP 20 стран с наибольшим числом пользователей Интернета Internet world stats [Електронний ресурс]. – Режим доступу : http://www.internetworldstats.com/top20.htm

9. Гуз А.М. Історія захисту інформації в Україні та провідних країнах світу: навчальний посібник / А.М. Гуз. – К.: КНТ, 2007. – 260 с.

10. Парламент Германии принял поправки к федеральному закону о защите данных [Електронний

ресурс]. – Режим доступу : https://www.infowatch.ru/analytics/legislation_news/152

11. ФРГ: Массовое хранение данных о телефонных переговорах признано неконституционным [Електронний ресурс]. – Режим доступу : http://www.dw.com/ru/%D1%84%D1%80%D0%B3-%D0%BC%D0%B0%D1%81%D1%81%D0%BE%D0%B2%D0%BE%D0%B5-%D1%85%D1%80%D0%B0%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5-%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85-%D0%BE-%D1%82%D0%B5%D0%BB%D0%B5%D1%84%D0%BE%D0%BD%D0%BD%D1%8B%D1%85-%D0%BF%D0%B5%D1%80%D0%B5%D0%B3%D0%BE%D0%B2%D0%BE%D1%80%D0%B0%D1%85-%D0%BF%D1%80%D0%B8%D0%B7%D0%BD%D0%B0%D0%BD%D0%BE-%D0%BD%D0%B5%D0%BA%D0%BE%D0%BD%D1%81%D1%82% D0%B8%D1%82%D1%83%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D0%BC/a-5310694

12. Франція оштрафувала компанію Facebook на 150 тис. євро за збір даних про користувачів соцмережі [Електронний ресурс]. – Режим доступу : http://espreso.tv/news/2017/05/16/150_tys_yevro_shtrafu_franciya_pokarala_facebook_cherez_stezhennya_za_korystuvachamy

13. Чистая прибыль Facebook в 2016 году выросла на 177 % [Електронний ресурс]. – Режим доступу : http://www.rbc.ru/business/02/02/2017/58925e399a79476d519af7f5

14. Гнатюк С.Л. Особливості захисту персональних даних в сучасному кіберпросторі: правові та технікотехнологічні аспекти : аналітична доповідь / С. Л. Гнатюк [Електронний ресурс]. – Режим доступу : www.niss.gov.ua/public/File/2013_table/1010_dopov.pdf

В статье определено понятие оборота и обработки персональных данных; охарактеризованы некоторые показательные решения национальных судов стран ЕС и Украины по анализированной проблематике; рассмотрена мировая практика относительно обращения и обработки персональных данных в социальных сетях; установлены виды применяемых санкций за нарушения в этой сфере.

Ключевые слова: персональные данные, безопасность, обращение, обработка, Европейский Союз, судопроизводство.

In the article the term "turnover" and "processing" of personal data; describes some exemplary decisions of national courts of the EU and Ukraine in the field; reviewed international practice regarding treatment and processing of personal data in social networks; set types applicable sanctions for violations in this area.

Key words: personal data security, circulation processing, European Union justice.