УДК 343.211.3:004.738.5: 681.3.06

БРИЖКО В.М., *доктор філософії (Ph.D.) з юридичних наук, старший науковий співробітник*

ПРИВАТНІСТЬ ДАНИХ У ХМАРНИХ ТЕХНОЛОГІЯХ

Анотація. *Про приватність та захист персональних даних в умовах розвитку новітніх технологій. Надано пропозиції щодо запровадження в Україні інституту права приватної власності людини на свої персональні дані.*

Ключові слова: *приватність, захист персональних даних, цифрові технології, приватна власність, інформаційне суспільство.*

Аннотация. *О приватности и защите персональных данных в условиях развития новейших технологий. Предоставлены предложения относительно внедрения в Украине института права частной собственности человека на свои персональные данные.*

Ключевые слова: *приватность, защита персональных данных, цифровые технологии, частная собственность, информационное общество.*

Summary. *On the privacy and personal data protection in terms of modern technologies development. Suggestions are provided in relation to introduction of institute of right of private ownership of a person on the personal information in Ukraine.*

Keywords: *privacy, personal data protection, digital technologies, information relations, information right, information society.*

Постановка проблеми. Останніми роками в Інтернет-сфері поряд з “розумними” технологіями типу Інтернет речей [1], які характеризують те, що кількість матеріальних об’єктів, підключених до Інтернету, стала збільшуватися по відношенню до кількості людей, що взагалі користуються всесвітньою павутиною, набувають поширення й інші ІТ-технології, так звані “хмарні обчислення” або “хмарні сервіси-послуги”. Вони, в умовах збільшення об’ємів інформації та завдяки Інтернет, надають можливості обробки та зберігання значних обсягів даних не на жорстких дисках комп’ютерів, а на віддалених серверах [2]. Їх застосування свідчить про новий етап розвитку Інтернету, а разом з тим – про нові проблеми в сфері захисту персональних даних стосовно прав людини на недоторканність особистого (у європейському розумінні – “приватного”) життя.

Враховуючи те, що “спостерігається певна тенденція щодо спроб нівелювати право людини розпоряджатися власними персональними даними” [3], продовжує існувати поблажливе ставлення різних організацій до створення належних організаційно-правових умов захисту баз персональних даних, а також нерідка несанкціонована комерціалізація у їх збиранні та продажу, яка пропонується у Інтернеті[1], проблеми захисту приватності людини, зокрема щодо сфери персональних даних, все більше ускладнюються та потребують удосконалення, про що йдеться, зокрема, у [4].

[1] У наш час маркетинг персональних даних стає найбільшим посяганням на особисте життя. За оцінкою американських фахівців річний ринок персональних даних складає не менш як 3 мільярдів доларів [5]. Це означає, що в рамках інформаційного бізнесу сформувався сектор, що спеціалізується на зборі, обробці і продажу персональних даних. Комерційний успіх даного сектора полягає у тому, що зібрані у окремих осіб, нерідко не санкціоновано, персональні дані дозволяють мінімізувати витрати щодо цілеспрямованої реклами та продажу. Про становлення маркетингу персональних даних в Україні див. у [6].

Аналіз досліджень. У країнах Заходу, пострадянського простору та в Україні дослідження загального нормативно-правового впорядкування інформаційних відносин сфери обробки та використання персональних даних здійснювало багато осіб, про результати робіт деяких з них йдеться, зокрема, у [7 – 12].

Стосовно поширення та застосування хмарних (інформаційно-обчислювальних) технологій (послуг, сервісів) провідні позиції у світі займають країни США, Європейського Союзу. В України ці проблеми досліджували такі вчені, як Гнатюк С.Л., Гриценко В.И., Сейдаметова З.С., Темненко В.А., А.А. Урсатьев [13 – 15] та ін. Так щодо захисту персональних даних, Гнатюк С.Л. справедливо визначає що: “Розглядати індустрію хмарних послуг ….в контексті захисту персональних даних спонукають два моменти: 1) завдяки особливостям свого функціонування хмарні сервіси творять цілком специфічне середовище, в якому традиційні нормативно-правові механізми, практики та підходи стають здебільшого неефективними; 2) у глобальному вимірі індустрія хмарних обчислень вже зараз перетворилася на критично важливий ресурс ІТ-сфери, але, за одностайними прогнозами, найближчими роками її питома вага в бізнесі і багатьох інших сферах життя зросте в рази” [13].

Метою статті є узагальнення поглядів та розробка пропозицій у забезпеченні приватності в умовах застосування хмарних технологій.

Виклад основного матеріалу. Поняття “приватність” походить від англ. слова privacy (“прайвесі”), хоча має глибокі історичні корені. Численні посилання на це суспільно-соціальне явище можна знайти у Біблії. Приватність була об’єктом загального захисту людини за часів давньоєврейської культури, класичної Греції, древнього Китаю. Захист, головним чином, зводився до можливостей “усамітнення”.

У наш час “приватність” тісно пов’язана з людською гідністю й іншими цінностями, такими як свобода слова та свобода доступу до інформації, таємницею кореспонденції тощо. У певному розумінні, усі права людини є аспектами права на приватність.

Разом з зазначеним, узагальненого тлумачення слова “приватність” немає. У останніх документах ЄС стосовно захисту персональних даних, зокрема у Регламенті ЄС 2016/679 від 27.04.16 р. “Про захист фізичних осіб у зв’язку з обробкою персональних даних і вільним обігом цих даних та про скасування Директиви 95/46/ЄС (Загальні Положення про захист даних)” [16], слово “приватність” не використовується. Чинне українське законодавство поняття “приватність” в контексті “персональні дані” або “інформація” не застосовує. При цьому, згідно ст. 271 Цивільного кодексу України “приватне життя” віднесено до “особистих немайнових прав”, а згідно ст. 325 ЦК України “приватність” стосується лише права власності на майно, тобто на матеріально-речові об’єкти [17].

Нещодавно прийнято Закон України “Про ратифікацію Угоди між Кабінетом Міністрів України та Урядом Держави Ізраїль про тимчасове працевлаштування українських працівників в окремих галузях на ринку праці Держави Ізраїль” від 31.08.16 р. № 0108, де у ст. 8 сформульовано, що мова йде про “сферу охорони приватних персональних даних з метою захисту персональних даних” [18].

Зміст вищезазначеної фрази створює загальне розуміння про що мова, але, на жаль, не дає ясного уявлення, у чому полягає різниця між “приватними персональними даними” і просто “персональними даними”.

В українській “Юридичній енциклопедії” 2003 р. [19] слово “приватність” відсутнє.

У тлумачному словнику Ожегова С.І. [20, с. 585] є слово “приватный”, яке тлумачиться як “частный”, що визначається як “личный, не общественный, не государственный”, “принадлежащий отдельному лицу, не обществу, не государству” та

“относящийся к личному, индивидуальному владению“ [20, с. 875]. Згідно українсько-російського словнику українське слово “приватний” перекладається на рос. як “частный (относящийся к одному лицу)”, “личный” [21, с. 454] та навпаки [21, с. 267]. При цьому, у “приватних” відносинах суб’єкти самостійно їх упорядковують, діють на власний розсуд, який підпорядковується принципу “дозволено все, що не заборонене законом”. Тобто мірилом диспозитивності (упорядкованості) відносин є насамперед закон.

Стосовно словосполучення “персональні дані”, то воно походить від старогрецького слова “*prosopon*” – “маска актора”, Потім, під впливом латині, цим словом стали позначати соціальний аспект людини, як біосоціальної істоти, і з’явилося слово “*persona”* – “особа”, від якого утворилося слово “*personalitas”* – “особистість” [7, с. 20-22], що визначає індивідуально виражені якості окремої людини.

Виходячи з зазначеного, можна, на наш погляд, зробити висновок про те, що “приватні персональні дані” – це персональні дані які належать відповідній людині (особі), як продукту суспільних відносин, у будь-яких галузях публічного та приватного права. У цьому аспекті можна вести мову про наявність у них якості власності.

Сьогодні зустрічаються різні узагальнення категорії (поняття) “приватність”: таємниця, відокремленість або самітність приватного життя, право на приватне життя, недоторканність приватного життя. На наш погляд, філософський зміст цього слова включає, зокрема, наступне: “*приватність – це право бути наданим самому собі. Кожна людина має право на свій “куточок” в просторі, захищений від довільних посягань з боку інших. ...Можливо, з юридичної точки зору, найточніший варіант змістової сутності зазначеного терміну – це право на недоторканність приватного життя”* [24, с. 9].

В 1999 році, у звіті “Приватність і права людини”, зробленому суспільними організаціями “Privacy International and Electronic Privacy Information Center” [18], було запропоновано поділити приватність на такі чотири види: *фізична приватність* – стосується захисту людини від фізичного насильства, тортур, примусових медичних втручань та ін.; *територіальна приватність* – стосується недоторканності житла людини, обмежень на втручання в домашнє та навколишнє її середовище; *інформаційна приватність* – передбачає встановлення правил збору, використання, поширення та захисту відомостей про особу (персональних даних); *приватність комунікацій* – розуміється все те, що пов’язано з техніко-технологічними засобами та способами у аспекті телефонних розмов, електронних повідомлень, поштового листування та інших видів інформаційно-комунікаційних зв’язків.

В умовах програмно-технологічного розвитку Інтернету приватність комунікацій дедалі більше пов’язується з інформаційною приватністю, тобто з тим, що передбачає захист персональних даних людини, інформаційної безпеки суспільства та держави. Ця тенденція безпосередньо стосується нових поглядів у застуванні Інтернету – за його допомогою, організації переходу від використання окремих програмно-апаратних засобів, що належать окремим суб’єктам (компаніям), на модель створення та використання “відкритого об’єднання хмарних обчислень” [26], тобто “хмарних технологій”, “хмарних сервісів” тощо.

Концепція “хмарних” (інформаційно-обчислювальних) технологій (послуг, сервісів) з’явилася в 1960 році, коли американський учений, фахівець з теорії ЕОМ, Джон Маккарті виказав припущення, що “коли-небудь комп’ютерні обчислення (обчислювальні потужності) стануть надаватися подібно комунальним послугам” [27].

Метафора “хмара” давно використовується фахівцями з технологій для зображення на мережевих діаграмах складної обчислювальної інфраструктури (або ж Інтернету як такого), що приховує свою внутрішню організацію за певним інтерфейсом. Проте термін “хмарні обчислення” з’явився на світ відносно недавно.

Згідно з результатами аналізу пошукової системи Google, термін “хмарні обчислення” (“Cloud Computing”) почав поширюватися з кінця 2007 року, поступово витісняючи словосполучення “грід-обчислення” (“Grid Computing”). Однією з перших компаній, що дала світу даний термін, стала компанія IBM, яка розгорнула на початку 2008 року проект “Blue Cloud” і спонсорувала Європейський проект “Joint Research Initiative for Cloud Computing” [28].

У 2011 році у Лабораторії інформаційних технологій Національного інституту стандартів и технологій (NIST) Міністерства торгівлі США були розроблені “Рекомендації NIST (спеціальна публікація 800-145)” для використання федеральними відомствами та неурядовими організаціями – “Визначення хмарних обчислень” (автори Петр Мелл і Тимоти Гренс) [29].

У п. 1.2 Рекомендацій NIST зазначається, що хмарні обчислення є новою парадигмою. Вона визначає нову глобальну архітектурну моделі функціонування всесвітньої мережі та її можливості щодо доступу до загального пулу (“об’єднання”) обчислювальних ресурсів, що конфігуруються (наприклад, серверів, систем зберігання, обробки, додатків і послуг). Тобто, згідно наданого NIST визначення, *хмарні обчислення – це інформаційно-технологічна концепція, що має на увазі забезпечення повсюдного і зручного мережевого доступу на вимогу до загального пулу обчислювальних ресурсів (мереж передачі даних, серверів, пристроїв зберігання даних, додатків і сервісів – як разом, так і окремо), що конфігуруються, які можуть бути оперативно надані і звільнені з мінімальними експлуатаційними витратами або зверненнями до провайдера*.

Як ми розуміємо та іншими словами, поява хмарних технологій є свідченням переходу інформатизації суспільства від насиченості інформаційної інфраструктури апаратними і програмними продуктами до світової інформаційної кооперації – об’єднання напрацьованого інформаційно-ресурсного і програмного потенціалу в єдине віртуальне інформаційне середовище із намаганнями збереження індивідуальної автономії.

Визначення NIST вказує на важливі аспекти хмарних обчислень і покликане служити основою для широкого обговорення того, що таке хмарні обчислення (сервіси) та які стратегії їх розгортання, щоб найкращим чином їх використовувати, без обмежень конкретних методів надання послуг або бізнес-операцій. Основні характеристики хмарних обчислень передбачають:

самообслуговування на вимогу. Споживач може самостійно та без взаємодії з постачальником послуг (провайдером) визначати обчислювальні потреби (серверний час, швидкість доступу до мережевого пристрою обробки та зберігання даних);

універсальність доступу до мережі. Передбачає для споживача можливість доступу у мережу завдяки використанню різних цифрових пристроїв (мобільні телефони, планшети, ноутбуки та ін.);

об’єднання ресурсів. Передбачає об’єднання ресурсів постачальником послуг в єдиний пул, з метою обслуговування декількох споживачів для динамічного перерозподілу потужностей між ними. Споживач не має можливості контролювати розподіл ресурсів, який здійснює постачальник послуг, але має можливість вказувати на потребу підключення до відповідного центру обробки та зберігання даних;

гнучкість (еластичність) надання послуг. Передбачають їх автоматичне надання з можливостями змін у кількості та часі, згідно потреб споживача;

обчислення послуг (облік споживання). Передбачає автоматичне обчислення наданих постачальником послуг згідно відповідного типу сервісу та тарифу (обсяг даних, що зберігаються та обробляються, кількість транзакцій, пропускна спроможність, кількість користувачів).

До основних видів послуг щодо хмарних обчислень Рекомендації NIST відносять:

програмне забезпечення як послуга (з англ. – Software-as-a-Service). Споживачу надається можливість використання прикладного програмного забезпечення (далі – ПО) провайдера, що працює в хмарній інфраструктурі і доступного з різних клієнтських пристроїв. Контроль і управління основною фізичною і віртуальною інфраструктурою хмари, зокрема мережі, серверів, операційних систем, зберігання, або індивідуальних можливостей додатку здійснюється хмарним провайдером;

платформа як послуга (з англ. – Platform-as-a-Service). Включає надання послуг з сукупності застосування апаратних засобів та ПО. Споживачу надається можливість використання хмарної інфраструктури для розміщення базового ПО для подальшого розміщення на ньому інших додатків (власних, розроблених на замовлення або придбаних). До складу таких платформ (набору утиліт, що забезпечують надання хмарних сервісів) входять інструментальні засоби створення, тестування і виконання прикладного ПО (систем управління базами даних, зв’язку, середовища виконання мов програмування), що надаються провайдером. Контроль і управління основною фізичною і віртуальною інфраструктурою хмари, зокрема мережі, серверів, операційних систем, зберігання здійснюється провайдером, за винятком раніше встановлених додатків, а також параметрів платформної конфігурації середовища;

інфраструктура як послуга (з англ. – Infrastructure-as-a-Service). Надається як можливість використання хмарної інфраструктури для самостійного управління ресурсами обробки, зберігання даних, мережами і ін. обчислювальними ресурсами. Споживач може встановлювати і запускати інше програмне забезпечення, яке включає операційні системи, платформне і прикладне ПО. Споживач може контролювати операційні та віртуальні системи зберігання даних і встановлені додатки, а також володіти обмеженим контролем за набором доступних мережевих сервісів (наприклад, між мережевим екраном). Контроль і управління основною фізичною і віртуальною інфраструктурою хмари, зокрема мережі, серверів, типів операційних систем та систем зберігання даних здійснюється провайдером.

Згідно Рекомендацій NIST основними схемами (моделями) розгортання хмарних обчислень є:

приватна хмара. Стосується послуг для виключного використання однією організацією, що може забезпечувати декількох споживачів (бізнес-одиниць);

співтовариство хмари. Стосується послуг для використання конкретним співтовариством споживачів (організаціями), що мають загальні проблеми;

відкрита хмара. Стосується послуг для відкритого використання широкою громадськістю. Вона функціонує на території постачальника послуг та може знаходитися у власності будь-якої організації;

гібридна хмара. Є композицією з двох або більшої кількості інфраструктур (приватних, суспільних або державних), пов’язаних між собою стандартизованими або запатентованими технологіями.

У квітні 2012 року Міжнародна робоча група, у складі Комісарів захисту даних різних країн [30], з метою підвищення захисту даних у сфері телекомунікацій і засобів масової інформації, представила робочий документ з питань конфіденційності і захисту даних хмарних технологій (“Сопотський меморандум”) [31][2].

На основі цього документу у вересні 2012 року Європейська Комісія опублікувала прес-реліз “Нова стратегія для управління європейського бізнесу та продуктивності уряду за допомогою хмарних обчислень” [32]. Стратегія призначена для прискорення та збільшення використання хмарних обчислень у всіх галузях економіки. Основні положення стратегії, яка отримала назву “Розв’язання потенціалу хмарних обчислень в Європі” [33; 34], передбачають:

- створення для хмарних обчислень єдиних технічних та інших стандартів щодо можливостей функціональної сумісності та обігу даних;
- створення загальноєвропейських схем сертифікації для хмарних провайдерів;
- розвиток безпечних і справедливих моделей умов контракту для хмарних обчислень, включаючи домовленості про рівень обслуговування.

У прес-релізі до “Сопотського меморандуму” прямо зазначається, що сьогодні, в умовах відсутності загальних стандартів і чітких контрактів, багато потенційних користувачів утримуються від прийняття хмарних рішень. Вони не впевнені, які стандарти і сертифікати громадяни повинні шукати, щоб задовольнити їхні вимоги і правові зобов’язання, наприклад, щоб гарантувати, що їх персональні дані або дані їх клієнтів перебувають у безпеці, або що додатки сумісні один з одним. Хмарні провайдери і користувачі бажають мати більш чіткі правила щодо постачання хмарних сервісів, наприклад, щодо питань юрисдикції правових спорів, переміщення даних і програмного забезпечення між різними постачальниками хмарних технологій та ін.

Існують різні думки та висновки фахівців щодо переваг, недоліків та проблем у застосуванні хмарних послуг, див. [13 – 15; 35 – 39]. Наведемо основні з них.

Доступність. У принципі, хмарні сервіси доступні всім, хто має підключення комп’ютера до Інтернету. Це дозволяє користувачам (звичайно компаніям) економити на закупівлі високопродуктивних, дорогих комп’ютерів. Немає необхідності в придбанні ліцензійного ПО, його налаштуванні і оновленні – споживач має нагоду через браузер зайти на сервіс і, заплативши за фактичне використання, користуватися його послугами. Також співробітники компаній стають мобільнішими, оскільки можуть отримати доступ до свого робочого місця, використовуючи ноутбук, планшет або смартфон. З іншого боку, хмарні сервіси потребують постійного з’єднання з Інтернет, а також можуть обмежувати у використанні ПО провайдера, яке споживач не завжди може пристосувати під свої цілі.

Вартість. Передбачає можливість зниження витрат та зменшення штату на обслуговування інфраструктури у окремих компаніях, економії на придбанні ліцензій на ПО, що дозволяє користувачам зменшити витрати на закупівлю дорогого устаткування.

[2] Першим документом ЄС про упорядкування суспільних відносин у телекомунікаціях є Директива 97/66/ЄС Європейського Парламенту і Ради “Про обробку персональних даних і захист прав осіб у телекомунікаційному секторі” від 15.12.97 р. [40, с. 337-334] (призначення – захист мереж від спаму і гарантій таємниці зв’язку загального користування), яка є доповненням до Директиви 95/46/ЄС Європейського Парламенту і Ради “Про захист осіб у зв’язку з обробкою персональних даних і вільним обігом цих даних” від 24.10.95 р. ([40, с. 273-293] (призначення – захист усіх типів персональних даних за будь-яких засобів їх обробки тощо), що скасовані згідно нових правил і порядку захисту персональних даних (див. [4; 16]).

Однак, для побудови малими компаніями власної хмари необхідні значні початкові матеріальні ресурси.

Обчислювальні потужності. При аналізі великих обсягів даних користувач хмарної системи використовує її обчислювальні здібності, заплативши тільки за фактичний час використання.

Надійність функціонування. Хмарна система може мати надійність, оскільки звичайно обладнана в центрах обробки даних, які мають резервні джерела живлення, охорону, професійних працівників, регулярне резервування даних, високу пропускну спроможність Інтернет-каналу, певну стійкість до несанкціонованого доступу при належному її забезпеченні. Проте при недбалому ставленні ефект може бути цілком протилежним. Більш того, що стосується надійності зберігання інформації, то фахівці стверджують, що якщо інформація, що зберігається в хмарі, втрачена, то вона втрачена назавжди.

Разом з зазначеним, є ствердження про те, що “плюси хмари” полягають у: а) легкості у користуванні – інформація відкривається лише тим, хто має на це відповідний дозвіл, та б) існує повний захист конфіденційної інформації – можливості послуги дозволяють клієнту чітко регламентувати коло користувачів серверу та маніпуляції, які здійснюються з його даними. Тобто, в разі, коли хтось із співробітників провайдера вирішить скопіювати чи відправити якийсь файл з серверу, не маючи на те дозволу, його дії будуть заблоковані [38].

Як узагальнюється в [27], *з точки зору провайдера*, завдяки об’єднанню ресурсів і непостійному характеру споживання з боку споживачів, хмарні обчислення дозволяють економити на масштабах, використовуючи значно менші апаратні ресурси, аніж у моделі “один споживач – один пристрій”, а за рахунок автоматизації процедур виділення ресурсів істотно знижуються витрати на абонентське обслуговування. *З точки зору споживача*, хмарні технології в принципі дозволяють отримати послуги з високим рівнем доступності і низькими ризиками непрацездатності, забезпечити швидке масштабування обчислювальної системи завдяки еластичності без необхідності створення, обслуговування і модернізації власної апаратної інфраструктури і, нарешті, заощадити на абонентській платі, оскільки в хмарних сервісах вона нараховується лише за використані ресурси.

Недоліки хмарних рішень відносяться**,** в основному, до проблеми довіри до постачальника сервісу, від якого залежить як безперебійна робота, так і збереження даних користувача. Існує побоювання того, що з поширенням цієї технології виникне проблема неможливості контролю даних, коли інформація, залишена користувачем, буде зберігатися роками, або без його відома, або він буде не в змозі змінити якусь її частину. Прикладом є сервіси Google, де користувач не в змозі видалити не потрібні йому сервіси і навіть видалити окремі дані, створені в деяких з них (FeedBurner, Google Friend Connect). Поки споживач послуг не має засобу видалення своїх власних даних на подібних серверах [27].

Загалом, *до головних недоліків* у застосуванні хмарних послуг можна віднести проблеми інформаційної безпеки, конфіденційності та захисту персональних даних.

Інформаційна безпека. Хмарні сервіси, як вважають деякі фахівці, самі по собі є надійною системою. Проте, при проникненні до неї зловмисник може отримати доступ до величезного сховища даних. Ще один мінус – це використання систем віртуалізації, в яких застосовують ядра стандартних ОС таких, як Windows та ін., що може сприяти проникненню вірусів.

Конфіденційність та захист даних. Захист даних, що зберігаються у публічних хмарах, в теперішній час викликає багато суперечок, але в більшості випадків експерти сходяться у тому, що не слід зберігати цінніші документи у публічній хмарі, оскільки поки немає технології, яка б гарантувала 100 % захист даних. Як зазначається у роботі Гнатюка С.Л. [13], сьогодні саме проблеми захисту персональних даних на ринку хмарних послуг є найбільш серйозним бар’єром для його подальшого розвитку й про те мова йде у “Сопотському меморандумі” [31], а саме:

- технологія все ще у стадії розробки і не апробована остаточно;
- досі немає міжнародної угоди про єдину термінологію, хоча технологія є транскордонною, а обробка даних фактично стала глобальним процесом;
- діяльність провайдерів є недостатньо прозорою і не може бути повністю відстеженої. Це значно ускладнює оцінку ризиків і створення єдиних правил гри;
- дотримання конфіденційності, недоторканності інформації та режиму доступу до неї не може бути проконтрольоване у хмарах;
- під час передачі персональних даних вони потрапляють під юрисдикції, в яких не передбачено їх адекватного захисту;
- провайдери та їх партнери можуть використовувати дані у своїх інтересах без повідомлення про це володільця та його згоди; локальні (національні) контролюючі інститути з захисту даних фактично не мають можливості нагляду за процесом їх обробки провайдерами хмарних послуг.

До цього, як вказується у [41], має місце значний відсоток не доброчесних гравців на ринку хмарних послуг. Так, 77 % опитаних в рамках дослідження організацій щонайменше один раз стикалися з шахрайськими сервісами, а 40 % з цього числа стали жертвами викрадення конфіденційних даних.

Наведений, зокрема, перелік підштовхує до попереднього висновку: сьогодні захист приватності не має однозначного організаційно-нормативного вирішення. В кращому разі він закінчується рекомендаціями і побажаннями, як необхідно будувати систему захисту. І більшою мірою це пов’язано з давно відомою проблемою складнощів упорядкування відносин в Інтернеті. Також зрозуміло, що традиційні норми упорядкування відносин в віртуальному середовищі не бажають слідувати тим юридичним канонам, які створені століттями раніше й лише для світу матеріальних речей. Й сьогодні це наочно демонструють так звані “хмарні технології” та слабке, взагалі, упорядкування відносин у віртуальності, яке, на превеликий жаль, продовжує мати повчальний, а не юридичний характер, що відповідав би реаліям змін у сучасності.

Про необхідність нових підходів у створенні системи нормативно-правового регулювання відносин у сфері захисту персональних даних мова йдеться давно, зокрема у [7 – 10; 42]. Основна пропозиція передбачає надання суб’єкту персональних даних специфічного та фіктивного для інформаційно-електронного середовища “права приватної власності” на його дані, але лише на визначених законом умовах (обмеженнях). Важливо підкреслити, що інститут власності на майно[3] завжди був та є потужним (якщо не основним) юридичним інструментом, який реально в змозі

[3] З кінця позаминулого століття в юриспруденції існує ще інститут “власності”, у якому застосовується термін “інтелектуальна власність”, хоча “власності” як такої він не передбачає. Він був запроваджений для задоволення насамперед економічних потреб. Прийнято, що вживання цього терміну правомірне, якщо поставитися до нього як до умовної категорії – “юридичної фікції”, яка має економічний сенс. Строго кажучи, термін “інтелектуальна власність” визначає не права власності, а права по використанню результатів творчої праці.

стримувати негативні соціально-економічні фактори у суспільних відносинах, якщо він обов’язково забезпечений чітко визначеними заходами притягнення до відповідальності порушників власності.

Виходячи з головних принципів захисту персональних даних, відзначимо два аспекти:

а) Обробка персональних даних допускається, якщо на те є згода суб’єкта персональних даних. Згода суб’єкта-людини на обробку її персональних даних передбачає, як ми вважаємо, наявність у неї специфічно-унікального права, а саме – права на володіння, користування і розпорядження своїми персональними даними. А це ніщо інше як тріада повноважень традиційного права власності – згідно ст. 2 Закону України “Про власність” від 07.02.91 р. № 697-12: “Право власності – це врегульовані законом суспільні відносини щодо володіння, користування і розпорядження майном”. Якщо персональні дані збирають та торгують ними, як і де забажається, то в такому разі вони стають майном, що надає прибуток. Звідси й виникає специфічність “власності” на персональні дані, яке можна розглядати у якості “позитивного змісту прав людини на свої персональні дані”.

б) З іншого боку, для задоволення потреб забезпечення державних, суспільних та комерційних інтересів не може існувати монополії людини на свої персональні дані (тобто, абсолютна власність). Щоб це врахувати, обробка персональних даних допускається, якщо це дозволяє Закон. Іншими словами, за визначених Законом умов право власності людини на свої персональні дані скасовується, що визначає, у цьому випадку, “негативний зміст прав людини на свої персональні дані”.

Сполучення позитивного і негативного змісту прав людини на свої персональні дані дозволяє ввести категорію “право приватної власності людини на свої персональні дані”. Людина має право повного (виключного) користування своїми персональними даними. При передачі персональних даних іншим суб’єктам може переходити тільки право обмеженого їх використання. Таким чином, у сенсі нового підходу у юридичному захисті персональних даних, ми замкнули принцип недоторканності особи з принципом, який свідчить про те, що основою свободи є власність і замах на неї рівнозначний обмеженню свободи та будь-яких видів приватності.

В якості додаткового пояснення головної суті пропозиції щодо запровадження в законодавство категорії “право приватної власності людини на свої персональні дані” зазначимо наступне.

Єдиною реальною системою, здатною упорядковувати відносини в будь-якому суспільстві, була і є “система власності”. Виходячи з цього, слід в основу всієї системи захисту персональних даних покласти “стрижень” власності і виходячи з її змістовної сутності врахувати це у нормах законодавства, які стосуються прав людини. Ось тоді і можна говорити про дотримання ст. 3 Конституції України, яка визначає пріоритетність прав людини, і про можливість “регуляції у віртуальності”. Тільки коли у людей виникає звичайне питання – “моє це або не моє”, прокидається свідомість, інтерес і починають функціонувати сформульовані в нормах положення, вимоги моралі і культури.

Висновки.

1. Поява хмарних технологій є свідченням переходу інформатизації суспільства від насиченості інформаційної інфраструктури апаратними і програмними продуктами до світової інформаційної кооперації – об’єднання напрацьованого інформаційно-ресурсного і програмного потенціалу в єдине віртуальне інформаційне середовище із намаганнями збереження індивідуальної автономії. Проте, останнє досить складно здійснити в окремих малих компаніях. Для побудови власної (приватної) хмари, або участі у побудові так званого “співтовариства хмари” чи “гібридної хмари”, необхідні

значні початкові матеріальні ресурси. Тому можна вважати, що на сьогодні хмарні технології привабливіші для тих великих компаній, яким необхідно обробляти значні обсяги даних та тим, які можуть отримувати більш значні вигоди від їх застосування, в умовах звичайної потреби в зміцненні бізнес-позиції (можливо, посиленні монополізації) на відповідному ринку, зокрема, за допомогою маркетингу та збору будь-яких приватних (персональних) даних.

2. Враховуючи те, що у розвинених країнах поширюється пропаганда новітніх цифрових технологій та здійснюються техніко-технологічні та нормативні пошуки в упорядкуванні суспільних відносин в телекомунікаційних мережах, що зумовлює зростання ризиків, пов’язаних з автоматичною обробкою та зберіганням даних, та необхідністю врахування нових міжнародних правил щодо невтручання не лише у сферу захисту персональних даних, але, взагалі, у сферу приватного життя, постає потреба у розробці спеціальних правових, регулятивних та технічних положень щодо застосування в Україні нових технологій у телекомунікаціях та Інтернеті. Це може визначати потребу у внесенні змін до законів “Про телекомунікації” та “Про захист персональних даних”.

3. Вважаємо, що при розробці нормативно-правових змін, у законодавство України мають бути імплементовані положення не тільки “Пакету захисту даних” Європейського Парламенту і Ради від травня 2016 року (див. [4]), але й деякі положення, які стосуються принципів упорядкування відносин у телекомунікаціях, про що йде мова у Директиві 97/66/ЄС Європейського Парламенту і Ради від 15.12.97 р. “Про обробку персональних даних і захист прав осіб у телекомунікаційному секторі” [25, с. 337-334].

Вбачається, що найбільш важливим може вважатися необхідність встановлення конкретних обов’язків провайдерів, що забезпечують роботу з персональними даними. Для створення умов забезпечення приватності у хмарних технологіях, постачальник (провайдер) послуг повинен вживати відповідних техніко-технологічних та організаційних заходів для гарантування інформаційної безпеки при наданні послуг в тому, що стосується функціонування мережі, яку він використовує (застосовує). Він також повинен обов’язково повідомляти споживачів послуг про існуючі ризики порушення захисту персональних даних та можливі засоби захисту.

4. Щодо культури захисту персональних даних в Україні, про що у статті зазначалося раніше (див. [3]), на превеликий жаль, говорити багато не доводиться. Можливо, кодекси поведінки, запровадження яких передбачене вказаним “Пакетом”, хоч якось будуть спрямовувати до формування в організаціях більш відповідальної поведінки до захисту приватних та, зокрема, персональних даних.

5. В контексті сутності категорії “приватність”, як вважаємо, “приватні персональні дані” – це персональні дані які належать відповідній людині (особі), як продукту суспільних відносин, у будь-яких галузях публічного та приватного права. Звідси витікає можливість вести мову про наявність у них якості власності.

Проте, головне в питаннях нормативного упорядкуванні відносин щодо пріватності для будь-яких видів персональних даних – це співвідношення свободи і захисту.

Аргументи на користь абсолютної свободи та демократії звичайно переконливі, але не самоочевидні.

Пріоритетами держави є порядок, стабільність, безпека. Але необмежена свобода “сильної” влади веде до свавілля, деградування суспільства і людини, фальшивого морального стану, де звичайно застосовуються різні інформаційно-психологічні засоби впливу на розум і поведінку людини з метою маніпулювання її свідомістю.

З іншого боку, пріоритетами індивідуума є свобода, ініціатива і захищеність. Придушення або суб’єктивне обмеження свободи веде суспільство до поглиблюванню адміністративного зловживання і корупції, нігілізму у сприйнятті обіцянок влади.

Характер об’єктивної суперечливості та необхідність врахування як одного, так і іншого пріоритету, вимагає пошуку компромісу, пошуку балансу у правах та інтересах особи, суспільства та держави.

6. У контексті відміченого вище та виходячи з положень ст. 3 Конституції України, яка визначає природні права людини “найвищою соціальною цінністю”, персональним даним може бути наданий специфічний та унікальний статус права власності, що юридично виступає у формі “приватного права власності людини на свої персональні дані”, монополія на яку обмежується законом в інтересах дотримання прав та основоположних свобод інших осіб, а також – дотримання балансу прав людини, суспільства і держави.

У основі цього твердження лежить те, що справжня демократія та правова держава – це не розподіл благ (через, зокрема, субсидії, тарифи тощо), а встановлення і регулювання права власності, орієнтованого на розвиток малого підприємництва. Питання лише в ідейній сутності механізму політико-соціального застосування цього права, з якого витікають рівень демократії, свободи та реального захисту прав людини.

Використана література

1. Баранов О., Брижко В. Захист персональних даних в сфері Інтернет речей // Інформація і право. – № 2(17)/2016. – С. 75-81.

2. Cloud computing. – Режим доступу : https://en.wikipedia.org/wiki/Cloud_computing

3. 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.

4. Брижко В. Сучасні основи захисту персональних даних в європейських правових актах // Інформація і право. – № 3(18)/2016. – С. 45-57.

5. Михеев В. Проблема правовой защиты персональных данных. – Режим доступу : //www.kiev-security.org.ua/box/4/136.shtml ; Цена персональных данных. – Режим доступу : //www.i2r.ru/article.shtml?id=1384

6. Брижко В. Економічні та правові аспекти захисту персональних даних // Правова інформатика. – № 1(29)/2011. – С. 25-33.

7. Права человека и защита персональных данных / А. Баранов. В. Брыжко, Ю. Базанов. – Харьков : Фолио, 2000. – 280 с.

8. Брижко В. Правовий механізм захисту персональних даних : монографія ; за ред. М. Швеця та Р. Калюжного. – К. : Парлам. вид-во, 2003. – 120 с.

9. Інформаційне право та правова інформатика в сфері захисту персональних даних / В. Брижко, М. Швець [та ін.] ; за ред. М. Швеця. – К. : ТОВ “ПанТот”, 2005. – 451 с.

10. е-майбутнє та інформаційне право / [В. Брижко, Ю. Базанов та ін.] ; за ред. д.е.н., проф. М. Швеця. – [2-е вид., доп.]. – К. : ТОВ “ПанТот”, 2006. – 234 с.

11. Порівняльно-правове дослідження відповідності законодавства України законодавству ЄС у сфері персональних даних / [В. Брижко, А. Радянська, М. Швець]. – К. : Тріумф, 2006. – 256 с.

12. Електронний банкінг у контексті захисту персональних даних / В. Брижко, Ю. Базанов [та ін.] : за ред. чл.-кореспондента АПрН України М. Швеця. – К. : ТОВ “ПанТот”, 2008. – 141 с.

13. Гнатюк С.Л. Актуальні питання захисту персональних даних у віртуальному середовищі (на прикладі технологій та сервісів “хмарного” обчислення) : аналітична записка. – Режим доступу : http://www.niss.gov.ua/articles/1090

14. Гриценко В.И., Урсатьев А.А. Cloud computering и облачная модель представления ИТ-услуг // Кибернетика и вычислительная техника. – 2013. – Вып. 171. – С. 5-19.

15. Сейдаметова З.С., Темненко В.А. Cloud computering : основные концепции и тенденции развития // Ученые записки Крымского инженерно-педагогического университета. – Вып. 28. – Симферополь : НИЦ КИПУ, 2011. – С. 43-48.

16. On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) : Reglament (EU) 2016/679 of the European Parlament and of the Council, of 27 April 2016. – Режим доступу : http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

17. Цивільний кодекс України : Закон України від 16.01.03 р. № 435-IV // Відомості Верхової Ради України (ВВР). – 2003. – №№ 40-44. – Ст. 271, 325.

18. Про ратифікацію Угоди між Кабінетом Міністрів України та Урядом Держави Ізраїль про тимчасове працевлаштування українських працівників в окремих галузях на ринку праці Держави Ізраїль : Закон України від 31.08.16 р. № 0108. – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/ webproc4_1?pf3511=59911

19. Юридична енциклопедія : в 6 т. / редкол. : Ю.С. Шемшученко (голова редкол.) та ін. – К. : Видавництво “Українська. енциклопедія, 2003. – Т. 5 : П–С. – 736 с.

20. Ожегов С.И. Словарь русского языка : 70000 слов / С.И. Ожегов ; под ред. Н.Ю. Шведовой. – [21-е изд., перераб. и доп.]. – М. : Рус. яз., 1989. – 924 с.

21. Там же, с. 875.

22. Галич Д.І. Російсько-український і українсько-російський словник / Д.І. Галич, Олійник І.С. – [6-е вид. стереотипне]. – К.: МП “Феникс”, 1993. – 560 с.

23. Там же, с. 267.

24. Смирнов С. Приватность / С. Смирнов. – (Межрегиональная группа “Правозащитная сеть)”. – М. : “Права человека”, 2002. – 96 с.

25. Priacy & Human Rights. Privacy International and Electronic Privacy Information Center, 1999. – Режим доступу : //www.epic.org

26. Модель коллектора и архитектура для открытого объединения облачных вычислений / [В. Рохвергер, Д. Брейтганд, Е. Леви, А. Галис, К. Нагин, И. Льоренте, Р. Монтеро, Ю. Вульфсталь, Е. Елтрох, Ю. Касерес, М. Бен-Иегуда, В. Эммерих, Ф. Галан] // Журнал исследований и разработок IBM, 2009. – 53 (4): 4:1-4:11.DOI:10,1147 / JRD.2009.5429058.

27. Хмарні обчислення. – Режим доступу : https://uk.wikipedia.org/wiki/%D0%A5%D0%BC%D0%B0%D1%80%D0%BD%D1%96_%D0%BE%D0%B1%D1%87%D0%B8%D1%81%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F

28. Joint Research Initiative for Cloud Computing. – Режим доступу : http://www.k504.xai.edu.ua/html/ucheba/rss/RSS_Lekciya_10.pdf

29. The NIST Definition of Cloud Computing. – Recommendations of the National Institute of Standards and Technology. – Special Publication 800-145. – Gaithersburg, MD : National Institute of Standards and Technology, January 2011. – 7 p. – Режим доступу : http://csrc.nist.gov/publications/drafts/ 800-145/Draft-SP-800-145_cloud-definition.pdf

30. International Working Group on Data Protection in Telecommunications (IWGDPT). – Режим доступу : http://clck.ru/8aXVe; https://datenschutz-berlin.de//content/europa-international /international-working-group-on-data-protection-in-telecommunications-iwgdpt

31. Working Paper on Cloud Computing – Privacy and data protection issues (“Sopot Memorandum”). International Working Group on Data Protection in Telecommunications 51st meeting, 23-24 April 2012, Sopot (Poland). – Режим доступу : http://clck.ru/8aJ9c

32. Нова стратегія для управління європейського бізнесу та продуктивності уряду за допомогою хмарних обчислень : прес-реліз Європейській Комісії, 2012 р. – Режим доступу : http://europa.eu/rapid/press-release_IP-12-1025_en.htm?Loca le=en

33. Unleashing the Potential of Cloud Computing in Europe. European Commission / Brussels, 27.9.2012 COM(2012) 529 final. – Режим доступу : http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf

34. European Commission. Unleashing the Potential of Cloud Computing in Europe – What is it and what does it mean for me? Memo. – Режим доступу : http://www.abbl.lu/sites/abbl.lu/files/FAQCloud_Computing.pdf

35. Хмарні технології. Переваги і недоліки. – Режим доступу : http://valtek.com.ua/ua/system-integration/it-infrastructure/clouds/cloud-technologies

36. Облачные вычисления : лекция. – Режим доступу : http://www.k504.xai.edu.ua/html/ucheba/rss/RSS_Lekciya_10.pdf;

37. Що корисного принесли хмарні CRM-системи? – Режим доступу : http://j.parus.ua/ua/379

38. Хмарні технології на захисті бізнесу. – Режим доступу : http://www.epravda.com.ua/publications/2012/05/7/322884

39. Digital Agenda : New strategy to drive European business and government productivity via cloud computing. – Режим доступу : http://europa.eu/rapid/press-release_IP-12-1025_en.htm?Locale=en

40. Системна інформатизація правоохоронної діяльності : європейські нормативно-правові акти та підходи до упорядкування інформаційних відносин у зв’язку з автоматизованою обробкою даних : посіб. / В. Брижко, М. Швець [та ін.]. – Кн. 2. – К. : ТОВ “ПанТот”, 2006. – 509 с.

41. Мошеннические облачные сервисы – бич 77 % компаний. – SecurityLab.ru. 23.01.13. – Режим доступу : http://www.securitylab.ru/news/436587.php

42. Персональні дані та право власності // Українське право. – 2002. – № 1. – С. 152-157; Про економічний аспект захисту персональних даних у контексті права власності на інформацію // Правова інформатика. – № 1(9)/2006. – С. 45-54; До питання е-торгівлі та захисту персональних даних // Правова інформатика. – № 1(13)/2007. – С. 14-27; Інформаційна безпека : економічні та правові аспекти проблеми захисту персональних даних // Інформація та безпека. – № 1-2(5-6)/2011. – С. 67-72. – (Інформ.-аналіт. журнал ТОВ “Академпрес”); Захист персональних даних : реалії та практика сучасності // Інформація і право. – № 3(9) 2013. – С. 31-48; Особливості ознак та матеріальна специфічність у сфері інформаційного права // Інформація і право. – № 1(13)/2015. – С. 15-26.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~