ОСОБЛИВОСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В СУЧАСНОМУ КІБЕРПРОСТОРІ: ПРАВОВІ ТА ТЕХНІКО-ТЕХНОЛОГІЧНІ АСПЕКТИ

Аналітична доповідь

Гнатюк С.Л.,

головний консультант відділу досліджень
інформаційного суспільства та
інформаційних стратегій, к. і. н.

ЗМІСТ

ВСТУП

На сьогодні в країнах Європейського Співтовариства склалася досить однозначна і стереотипна юридично-правова дефініція самого поняття «персональні дані» (далі в тексті можливе скорочення – ПД), а також консенсус щодо основних принципів і процедур їх обробки та захисту. Для країн Центральної та Східної Європи, що запроваджують або модернізують власну систему захисту ПД (до них відноситься і Україна) саме ця модель слугує певним стандартом і взірцем.[*] Насамперед модернізація стосується національних профільних законодавств держав регіону ЦСЄ, які адаптуються до відповідних базових актів Ради Європи та ЄС.

Для порівняння – декілька визначень з відповідних законодавчих актів різного походження. *Європейська Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних*, підписана в Страсбурзі 28 січня 1981 року: Персональні дані – це інформація, що стосується конкретної або такої, що може бути ідентифікованою, особи. Класична для європейського галузевого права *Директива Європейського Союзу 95/46/ЄС «Про захист осіб у зв'язку з обробкою персональних даних і вільним обігом цих даних»* 1995 року: Персональні дані – будь-яка інформація, що стосується встановленої фізичної особи чи фізичної особи, яку можна встановити. *Закон Литовської Республіки про правовий захист особистих даних* від 11.06.1996 року: «Особисті дані – будь-яка інформація, пов'язана з фізичною особою - суб'єктом даних, ідентичність особи якого встановлена або може бути встановлена безпосередньо або непрямим шляхом з використанням таких даних як особистий код, один або декілька фізичних, фізіологічних, психологічних, економічних, культурних або соціальних ознак, характерних для особи.» *Закон Російської Федерації «Про персональні дані»* від 27.06.2007 року: Персональні дані – це будь-яка інформація, що відноситься до визначеної або визначуваної на підставі такої інформації фізичної особи (суб'єктові персональних даних), у тому числі його прізвище, ім'я, по батькові, рік, місяць, дата і місце народження, адреса, сімейний, соціальний, майновий стан, освіта, професія, доходи, інша інформація. *Закон України «Про захист персональних даних»* від 21.09.2012: Персональні дані – відомості або сукупність відомостей про фізичну особу, яку ідентифіковано або може бути конкретно ідентифіковано.

Таким чином, в українському законодавстві закріплене типово європейське правове розуміння ПД і присутня відповідна дефініція, більше того, триває його адаптація до європейських норм (докладніше про це – нижче). Разом з тим, треба усвідомлювати, що справді ефективний захист

[*] Специфічна модель захисту персональної інформації, що збереглася у деяких державах англосаксонського права (США, країни Тихоокеанського регіону) відрізняється від сучасної європейської особливостями законодавчого забезпечення та адміністрування, але жодним чином не суперечить їй на рівні основних правових трактувань, духу закону. Навпаки, саме у США наприкінці XIX століття вперше отримали науково-правову розробку ідеї «прайвесі» (англ. - «*privacy*»), сприйняті й в континентальній Європі.

персональних даних неможливо налагодити, розглядаючи його тільки як окрему, самодостатню мету і не беручі до уваги той факт, що в кінцевому рахунку вся система захисту ПД – це невід'ємна складова загальної системи забезпечення фундаментальних прав людини і громадянина. І в даному разі йдеться про одну з найважливіших ліберально-демократичних свобод – право на недоторканість приватного життя.

Саме на цю обставину звертає увагу Марі Жорж, експерт з питань захисту даних Національної комісії Франції з інформаційних технологій та свобод, аналізуючи одну з редакцій Закону України про захист персональних даних: «Назва Закону говорить про те, що у ньому йдеться про «захист персональних даних». Цей вираз […] дещо заплутує, адже здається, що мова йде тільки про питання безпеки даних, у той час як ані Конституція України, ні Конвенція №108 чи Директива ЄС [1] не використовують цей термін. Європейські тексти визначають мету/предмет, використовуючи набагато ширше та чіткіше формулювання: «забезпечення захисту основних прав громадян, зокрема, на їх особисте життя, у зв'язку з обробкою персональних даних».[2]

Ці слова добре ілюструють сучасне європейське розуміння кореляції між захистом ПД і правами людини, а також ту величезну увагу, що приділяють у Раді Європи і особливо в ЄС їх дотриманню. Логіка тут досить прозора: сучасна демократія з її приматом поваги до прав та гідності людини є немислимою без повноцінного забезпечення недоторканності її особистого життя, приватності, а це, в свою чергу, неможливе без ефективного захисту її персональних даних.

Довідково. В європейській правовій традиції захист приватного життя як норма законодавства має досить глибокі корені. Її елементи можна знайти вже у практиці англійських мирових суддів XIV століття, які визнавали за провину підглядання та підслуховування. Законодавство Швеції вже у XVIII ст. зобов'язувало державні органи використовувати особисту інформацію лише у спеціально обумовлених законом цілях.[3] Остаточне оформлення й широке розповсюдження права на недоторканість приватного життя відбулося в Європі в епоху буржуазних революцій. Наприкінці XIX сторіччя, у 1890 році, у США вперше було сформульоване науково-правове обґрунтування категорії «прайвесі» (англ. - *«privacy»*) і запропонований відповідний концепт, що зводився до формули про право особи «бути залишеною у спокої» («right to be left alone»). Один з авторів цього визначення, суддя Верховного Суду США Луїз Брандез вважав прайвесі найціннішою з демократичних свобод і виступав за те, щоб її особливий статус був відображений в Конституції.[4] У 1990 році британський Calcutt Committee, провівши якнайретельніше дослідження трактувань прайвесі в рамках різних епох, культур та політичних систем, констатував, що «ніде не було знайдено абсолютно прийнятного правового визначення» цього поняття. Разом з цим, комітет запропонував власне сучасне

[1] Маються на увазі Конвенція Ради Європи про захист осіб стосовно автоматизованої обробки персональних даних (Страсбург, 28 січня 1981 року, № 108) та Директива Європейського Союзу 95/46/ЄС «Про захист осіб у зв'язку з обробкою персональних даних і вільним обігом цих даних» 1995 року.

[2] Аналіз Закону України про захист персональних даних / Європейський Союз. Рада Європи. - Страсбург, 19 січня 2012. [Електронний ресурс]. - Режим доступу : http://zpd.gov.ua/dszpd/doccatalog/document?id=51482

[3] Свобода інформації та право на приватність в Україні. Том 2. Право на приватність: conditio sine qua non / Харківська правозахисна група; Худож.-оформлювач О.Герчук - Харків: Фоліо. 2004. – С. 12.

[4] Див.: Там само. – С. 5.

визначення прайвесі: «Право особи чи її родини бути захищеною від втручання в її особисте життя та стосунки безпосередньо фізичним шляхом або через публікацію інформації.»[5]

В черговий раз інтерес до права на приватність зріс в 60-70-ті роки XX століття з появою перших ІКТ (в їх сучасному розумінні) і активізацією інформаційних обмінів. Потенційні можливості стеження та збору за допомогою комп'ютерних систем вимагали встановлення спеціальних правил щодо збору та обігу інформації особистого характеру. Основи сучасного законодавства в цій сфері було закладено першим у світі законом про захист даних, який було введено в дію на землі Гессе в Німеччині в 1970 році. Наступними були національні законодавчі акти Швеції (1973), Сполучених Штатів (1974), Німеччини (1977) та Франції (1978).[6]

Нині ця позиція є загальновизнаною: **недоторканість приватного життя, в тому числі особистої інформації людини як одне з її фундаментальних прав закріплене в основоположних міжнародних актах сучасності** – Загальній декларації прав людини ООН, Міжнародному пакті про громадянські й політичні права, Конвенції ООН про права дитини, багатьох інших міжнародних і регіональних угодах. Право на приватність тією чи іншою мірою визнається також в абсолютній більшості національних законодавств світу, причому, як правило, на рівні конституцій.[7]

У статті 8 Європейської Конвенції з прав людини це право сформульоване таким чином:

1. Кожна людина має право на повагу до її особистого і сімейного життя, житла і таємниці листування.

2. Держава не може втручатися у здійснення цього права інакше ніж згідно із законом та у випадках, необхідних в демократичному суспільстві в інтересах національної і громадської безпеки або економічного добробуту країни, з метою запобігання заворушенням і злочинам, для захисту здоров'я або моралі чи з метою захисту прав і свобод інших людей.»[8]

Як бачимо, у цій правовій нормі присутня складова *інформаційної приватності*, що включає в себе встановлення правил збору та обігу персональних даних.

Основи ідеології захисту ПД в правовій практиці сучасних демократичних держав можна звести до таких двох положень: 1) пріоритетним є право особи розпоряджатися своїми персональними даними; їх використання без дозволу володільця карається згідно з законодавством; 2) для будь-кого, хто здійснює користування персональними даними фізичних осіб, з їх дозволу, встановлено відповідальність у разі

---

[5] Report of the Committee on Privacy and Related Matters, Chairman David Calcutt QC, 1990, Cmnd. 1102, London: HMSO, page 7.

[6] Свобода інформації та право на приватність в Україні. Том 2. Право на приватність: conditio sine qua non / Харківська правозахисна група; Худож.-оформлювач О.Герчук - Харків: Фоліо. 2004. – С. 13.

[7] Свобода інформації та право на приватність в Україні. Том 2. Право на приватність: conditio sine qua non / Харківська правозахисна група; Худож.-оформлювач О. Герчук - Харків: Фоліо. 2004. – С. 5.

[8] Рада Європи. Конвенція про захист прав людини і основоположних свобод [Електронний ресурс]. - Режим доступу : http://zakon4.rada.gov.ua/laws/show/995_004

умисного розголошування цих даних третім особам (якщо тільки фізична особа не дала дозвіл на таке розголошування).*

З цих основ випливають основні **права володільця персональних даних**. Володілець має право знати:

- *хто* і *де обробляє* його ПД;
- *кому передаються* його ПД;
- *де зберігаються* його ПД;
- як реалізувати право на *доступ* до своїх ПД (право на доступ як такий також належить до основних);
- *механізми обробки* його ПД (у разі їх автоматичної обробки).

Крім того, до основних прав володільця відноситься право *вимагати знищення чи виправлення* ПД, якщо вони обробляються незаконно чи є недостовірними.[9]

З означеними пріоритетами й правами прямо корелюють **вісім основних принципів обробки персональних даних**, сформульованих ще 1981 року у Конвенції Ради Європи про захист осіб стосовно автоматизованої обробки даних особистого характеру (статті 5-8). Згідно з ними, ПД повинні:

1. Оброблятися сумлінно і законно, причому тільки за наявності підстав та з дотриманням вимог *(принцип законності)*.
2. Отримуватися із конкретними законними цілями та не оброблятися у способи, несумісні із цими цілями *(принцип конкретності цілей)*.
3. Бути адекватними, не надлишковими, відповідати цілям обробки *(принцип пропорційності)*.
4. Бути точними та своєчасно оновлюватися *(принцип якості даних)*.
5. Не зберігатися довше, ніж це необхідно *(принцип обмеження терміну обробки)*.
6. Оброблятися з дотриманням прав фізичної особи, включаючи право на доступ до даних та заперечення щодо їх обробки *(принцип прозорості та опозиції)*.
7. Оброблятися з дотриманням технічних вимог щодо захисту даних *(принцип захисту даних)*.
8. Не передаватись за межі країни без відповідного захисту *(принцип обмеження передачі іноземним суб'єктам)*.[10]

Цих норм, принципів та процедур цілком вдавалося дотримуватись у «доцифрову» епоху, коли повсякденні інформаційні обміни відбувалися безпосередньо у фізичному середовищі, або за допомогою пристроїв і мереж,

---

* У рамках національних законодавств, однак, зазвичай є спеціально прописані випадки винятків з цих двох фундаментальних правил.

[9] Див.: Козак В. Захист персональних даних: право, практика, нагляд [Електронний ресурс]. - Режим доступу : http://zpd.gov.ua/dszpd/doccatalog/document?id=51760

[10] Рада Європи. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних. Страсбург, 28 січня 1981 року. [Електронний ресурс]. - Режим доступу : http://zakon4.rada.gov.ua/laws/show/994_326

які можна було відносно легко ідентифікувати та відстежити (наприклад, телефон чи радіо). Але **технологічний прогрес і глобалізація значною мірою змінили те, як збираються персональні дані, як до них здійснюється доступ і яким чином вони використовуються (обробляються)**.

Практично в усіх країнах та міждержавних об'єднаннях **найбільш проблемною сферою захисту ПД є сьогодні ІТ і кіберпростір** як нове специфічне інформаційно-комунікаційне середовище, яке стрімко розвивається і збільшується. У цій галузі нормативно-правове регулювання хронічно відстає від якісного (технології) та кількісного (пропускна здатність і поширеність інфраструктур) розвитку. Це відставання намітилося ще в 80-90ті роки минулого століття, але воно **стало справді системною проблемою протягом 2000-х років** разом із революційними винаходами та змінами в інформаційно-комунікаційних технологіях (ІКТ), лавиноподібним поширенням всесвітньої мережі і міграцією цілих галузей людської діяльності в онлайн-сектор. Виникло й продовжує швидко зростати цілком нове, унікальне середовище, в якому традиційні нормативно-правові механізми, практики та підходи щодо захисту персональних даних стають здебільшого неефективними.

Розділ І. Проблематика та специфіка захисту персональних даних у кіберпросторі.

У наш час Інтернет остаточно став глобальною – не лише за принципами організації, але й за кількісними показниками – мережею, кількість його користувачів вже значно перевищила 2 млрд й продовжує швидко зростати. Так само швидко вдосконалюються ІТ, їх виробничі потужності, до того ж масового розповсюдження набула багатофункціональна і високопродуктивна мобільна електроніка. Сьогодні веб-середовище – «критичний ресурс» людства, що відіграє величезну й щодалі більшу роль у його повсякденній діяльності.

Визнання права людини на анонімність в онлайні завжди було одним із стовпів архітектури та філософії Інтернету. Водночас, за логікою цієї ж архітектури, **без розміщення особою персональних даних на віддалених серверах (а, відтак – у Мережі) повноцінне послуговування всіма її вигодами є неможливим**. У переважній більшості випадків користувач не може здійснити найпростіших речей – встановити програмне забезпечення, завантажити контент, здійснити купівлю, – не залишивши взамін хоча б мінімальних відомостей про себе. Зрештою, **навіть ті дані (здавалося б, суто технічні і необхідні системі для нормальної роботи онлайн), що ними пристрій користувача в автоматичному режимі обмінюється з віддаленими серверами, є такими, за якими «особа може бути конкретно ідентифікованою», себто, з нормативно-правової точки зору, – *персональними***.

Так, кожного разу, підключаючись до Мережі, пристрій користувача автоматично реєструється в мережі, вказуючи унікальний ідентифікатор, а відтак – IP-адресу, телефонний номер комутованого з'єднання, абонентський номер договору з оператором доступу та інші, необхідні для реєстрації в Мережі, дані. Далі, мандруючи Інтернетом, особа залишає за собою інформаційний «шлейф», що складається вже зі значно більшої кількості відомостей. Нижче наведений мінімальний перелік даних, які автоматично передаються і залишаються в мережі при кожному відвіданні будь-якого веб-ресурсу:

- веб-адреса сторінки, що переглядається (URL);
- веб-адреса сторінки, що посилається на першу;
- унікальна IP-адреса, найменування провайдера, країна реєстрації, місцезнаходження пристрою;
- параметри браузера (тип, версія, мова, налаштування, підтримка додатків) та комп'ютера (основні апаратні можливості, операційна система, роздільна здатність екрану тощо);
- дані проксі-сервера;
- дані про підтримку cookie і Java;
- часовий пояс.

Нагадаємо, ідеться не про цілеспрямований пошук ПД, а лише про той мінімум даних, що в режимі онлайн передається комп'ютером користувача *в штатному режимі, постійно і автоматично*.

Зрозуміло, що рівень втручань у сферу приватності (або принаймні потенційні можливості для цього) збільшується пропорційно обсягам комунікацій та інформаційних обмінів в Інтернет-просторі. **Тотальна комп'ютерізація** телекомунікацій, систем транспортування, фінансів, обліку населення, медичного обслуговування, численних баз даних **постійно збільшує кількість та якість інформації, що опрацьовується відносно кожної особи, причому зазвичай без її відома**. Утім, зараз бурхливо розвиваються також **онлайн-сектори, де людина залишає свої персональні дані цілком усвідомлено та добровільно**: електронний бізнес, банкінг та шопінг, цілий спектр онлайн-послуг, електронна пошта, соціальні медіа, різноманітні мережні спільноти, інтерактивні служби та інші веб-сервіси другого покоління (Web 2.0)[*], хмарні сервіси, онлайн-аутсорсинг і багато іншого. Рівень «деанонімізації» користувачів в такому середовищі стає практично стовідсотковим, навіть якщо вони дотримуються вимог безпеки. Апаратні можливості ІТ-обладнання вже досить давно дозволяють *не видаляти* ці відомості, і, відповідно, *автоматично зберігати* їх. З технічної точки зору так само **не складає жодної проблеми створення детального досьє на будь-яку особу, та/або збір інформації про неї в режимі реального часу**. Уже не перший рік це здійснюється та аналізується комп'ютерними системами в автоматичному режимі. **Для зацікавленої людини чи організації питання полягає лише в доступі (законному чи ні) до потрібних інформаційних ресурсів**.

При цьому можуть оброблятися персональні дані надзвичайно широкого діапазону: від анкетних, які явно є відомостями про особу яка ідентифікована, так і відомостей, які можуть стосуватися особи опосередковано або які можуть використовуватися в процесі ідентифікації особи: інформації про оплату послуг з використанням платіжних карт, логіни та паролі, записи в соціальній мережі, номери телефонів, електронні адреси, тощо.

Якщо звернутися до суто технічних подробиць, то найчастіше ПД з використанням веб-ресурсів обробляються саме в рамках таких процесів як:

- заповнення відвідувачами веб-ресурсів анкет;
- реєстрація та отримання логіна та пароля;
- реєстрація з використанням облікового запису соціальної мережі;
- надання електронної адреси відвідувача для зворотного зв'язку.

Зазвичай така інформація залишається в Мережі і пересічний користувач-володілець цих персональних даних, як правило, не в змозі проконтролювати їх подальше використання та обробку. Крім того, існує і

[*] ***Web 2.0*** – за визначенням одного з головних його ідеологів Тіма О'Рейлли, це «методика проектування систем, які шляхом обліку мережевих взаємодій стають тим краще, чим більше людей ними користуються». Власне, терміном "Web 2.0" прийнято називати сукупність онлайн-проектів і сервісів, що розвиваються і вдосконалюються самими користувачами : блоги, wiki, соціальні мережі і т. д.

постійно вдосконалюється **ціле сімейство технологій для створення баз даних й індивідуальних «онлайн-портретів»** на основі збору та аналізу всіх відомостей, що мають будь-який (хай і непрямий) стосунок до користувачів. Так, наприклад, з метою відстеження особливостей поведінки відвідувачів веб-ресурсів традиційно використовуються такі – вже класичні – методики як:

- надсилання до пристрою користувача файлів «cookies»* першої та «cookies» третьої сторони (при транзиті через посередницькі проксі-сервери);
- збирання в базах веб-ресурсів детальної інформації протягом тривалого часу про відвідані сторінки, вибрані режими, натиснуті клавіші тощо, та її подальша обробка;
- збирання в базах веб-ресурсів інформації про апаратні та програмні засоби, які встановлено у користувача, та інше.

Довідково. Проведене ще в 2010 році розслідування газети The Wall Street Journal показало, що до встановлення імені і особи користувача за його «Інтернет-портретом», зібраним автоматичними сервісами поведінкового таргетинга*, нерідко залишається буквально пара кроків. У зв'язку з цим розслідуванням експерти Electronic Frontier Foundation, американської неурядової організації з захисту приватного життя в онлайн-просторі, наводять такі дані: з теорії мереж відомо, що для повної «деанонімізації» особи досить 33 «біт» інформації. Такі «біти», як поштовий індекс або дата народження, мають більшу «вагу» (апроксимуючу цінність), ніж інші. При цьому [x+1] Inc., логістичний сервіс Capital One Financial Company збирає на одного з вісьмох (за єдиний клік на сайті) 26,5 «біта» – це означає, що особу вдається встановити з точністю 1 до 64, тобто у всьому світі не знайдеться більше 64 чоловік з тим же поєднанням параметрів профілю. Однозначна «деанонімізація» цієї людини потребувала б лише ще одного «важкого» біта – наприклад, даних про точний вік.[11]

Навіть у країнах найбільш демократичних і з найсуворішим законодавством щодо захисту ПД **завжди було поширеним незаконне знімання інформації з електронних каналів зв'язку**. Свідченням тому – пов'язані з цим **численні скандали, шлейф яких тягнеться у 80-90ті роки минулого століття**, в часи, коли з'явилися перші великі електронні бази даних і поштові сервіси*. Але незрівнянно більших масштабів ця проблема

---

* ***HTTP-cookies, «Кукі, кукіз»*** - (англ. *Cookies* - тістечка, печиво) – в комп'ютерній термінології – невеликі фрагменти текстових або бінарних даних, що відправляється веб-сервером і зберігається на комп'ютері користувача. При кожній спробі відкрити сторінку відповідного сайту веб-клієнт (браузер) користувача пересилає такий фрагмент даних веб-серверу у вигляді HTTP-запиту. Заявлене призначення і сфера застосовування є такою: а) збереження даних на стороні користувача; б) аутентифікації користувача; в) зберігання персональних переваг і налаштувань користувача; г) відстеження стану сесії доступу.

* ***Поведінковий таргетинг*** – технологія збору та обробки інформації суть якої зводиться до впровадження механізму збору даних про дії користувача в Інтернеті за допомогою cookie-файлів. Інформація збирається в спеціальних «профілях» і містить дані про проглянуті сайти, пошукові запити, покупки в інтернет-магазинах і т. д. Сформувавши такий профіль, можна не лише стати власником контактних даних об'єкту, але й досить чітко уявити собі його соціопсихологічний портрет (звички, смаки, пристрасті, суспільно-політичні преференції, коло контактів, рівень доходів тощо).

[11] Див.: Эпоха анонимности в сети заканчивается. Marketing Media Review. 5 серпня 2010. [Електронний ресурс]. - Режим доступу : http://mmr.net.ua/news/id/20861/

* Згідно з останніми даними ця історія має ще більш глибоке коріння. Зокрема у вересні 2013 року АНБ США (головна безпекова структура США з радіоелектронної розвідки) визнало, що слідкувало в 70-і роки за правозахисниками та журналістами.

набула після 2000 року, особливо в зв'язку з бурхливим розвитком середовища Web 2.0 та його найпопулярнішої складової – **соціальних медіа**. **Уже наприкінці 2012 року 6 з 10 користувачів Інтернету (що склало майже півтора мільярда осіб) хоча б раз на день відвідувала свої акаунти** у тих чи інших соціальних мережах, залишаючи власні та/чи оброблюючи чужі дані. Оскільки сегмент соціальних медіа нині стабільно зростає, то немає жодного сумніву, що протягом поточного року їх аудиторія стала ще більшою. Середньостатистичний користувач цих сервісів зареєстрований в 1-3 мережах, але приблизно кожний десятий – у п'яти і більше.[12] Таким чином, **ідеться про обіг у віртуальному середовищі гігантської кількості персональних даних значної частини населення Земної кулі**.

У цьому контексті досить закономірними виглядають **пов'язані з несанкціонованим витоком персональних даних численні скандали і судові конфлікти між провідними соціальними мережами (Facebook, Twitter, Google+ та ін.) з глобальним охопленням і окремими країнами, пересічними фізичними чи юридичними особами**, – причому нерідко йшлося про незаконний «злам» сотень тисяч акаунтів.

Кількість подібних інцидентів є занадто великою, а самі вони – надто стереотипними для того, щоб наводити тут докладну інформацію про них. Останній гучний скандал (або, скоріше, низка скандалів) такого роду пов'язаний з ім'ям Едварда Сноудена. На початку червня поточного року Guardian отримала й опублікувала текст секретного судового вироку, згідно з яким американській телекомунікаційній компанії Verizon належало упродовж трьох місяців щодня передавати державним структурам США дані про дзвінки своїх клієнтів. Washington Post, у свою чергу, повідомила про існування секретної програми PRISM, у рамках якої спецслужби дістають доступ до даних найбільших світових IT-корпорацій. Також повідомлялося, що спецслужби США мають прямий доступ до серверів провідних інтернет-компаній – Microsoft, Yahoo!, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple.* Компанії спростували ці повідомлення. Інформацію виданням надав колишній співробітник ЦРУ Едвард Сноуден, який вже в якості співробітника приватної компанії Booz Allen мав доступ до системи збору цих користувачів. За його власною версією, він вирішив розкрити інформацію про порушення прав громадян з боку спецслужб, зібрав усі можливі підтвердження цих порушень і, переїхавши в Гонконг, почав звідти передавати ці відомості до медіа.

Скандал навколо PRISM продемонстрував і інше: ступінь співпраці таких корпорацій та спеціальних служб державних органів. Рівень такого співробітництва, його динаміка та глибина, а також обсяги та характер

[12] Social Media Around the World 2012 / InSites Consulting [Електронний ресурс]. - Режим доступу : http://www.slideshare.net/slideshow/embed_code/14426292?rel=0#

* Крім агрегації величезної кількості даних сучасні комунікаційні онлайн-сервіси в принципі дають змогу автоматичної ідентифікації будь-якої особи в мережі, перманентного збору та довічного збереження даних про неї, включаючи слідкування за її переміщеннями в режимі реального часу, причому ці технологічні можливості нині масово використовуються як правоохоронними та спеціальними органами, так і злочинними суб'єктами.

відомостей про особу, що надаються приватними компаніями спецслужбам мимоволі наводять на думку про те, що захист «персональних даних» людини в тому вигляді як вони розуміються зараз є якщо не повністю марною, то дуже і дуже складною справою.

Додаткові і дуже серйозні ступені ризику щодо безпеки даних несуть у собі елементи новітньої третьої IT-платформи, яка принципово орієнтована на: а) зберігання основної частини інформації користувачів не на особистих фізичних носіях, а у віртуальному середовищі; б) повсюдний швидкісний доступ до Інтернету, а також автоматизацію і підключення до нього всієї виробничої, транспортної, адміністративної, бізнесово-фінансової, побутової (аж до помешкань і пральних машин) інфраструктури.[13] Зрозуміло, що модель розгортання веб-середовища з подібними характеристиками передбачає формування масової (аж до стовідсоткового охоплення) онлайн-аудиторії, озброєної такими пристроями доступу, що завжди можуть бути «під рукою». Сьогодні це вже стає реальністю: при й без того дуже високих темпах зростання користувачів і підключень до Всесвітньої Мережі* найвища динаміка все ж спостерігається у тих її сегментах, що пов'язані з виходом в Інтернет за допомогою сучасних **мобільних пристроїв** і безпровідних мереж.

На даний момент практично все населення Земної кулі користується стільниковими телефонами: у першому кварталі 2013 року його кількість склала 7,1 млрд людей, а діючих підписок на послуги мобільного зв'язку тоді ж було зафіксовано 6,8 млрд.[15] Це – **96,2 % людства**.

У будь-якому сучасному «мобільніку» обов'язково присутня функція виходу в Інтернет, але глобальні ринки впевнено завойовує наступне покоління телефонів – орієнтовані на постійне перебування онлайн смартфони-мінікомп'ютери, в яких можливості веб-серфінгу максимально оптимізовані та урізноманітнені. Сьогодні апаратних та софтверних

---

[13] Докладніше див. зокрема: IDC Predictions 2013 – Competing on the 3rd Platform [Електронний ресурс]. - Режим доступу : http://www.idc.com/research/Predictions13/downloadable/238044.pdf; 2013-й — год конкуренции вокруг «третьей» платформы / PCWeek, 29.01.2013 [Електронний ресурс]. - Режим доступу : http://www.pcweek.ru/idea/article/detail.php?ID=146072; Третья платформа ИТ: «большая семерка» ОС, версия 2012 / «Открытые системы», № 10, 2011 [Електронний ресурс]. - Режим доступу : http://www.osp.ru/os/2011/10/13012228/; «Третья платформа»: что нам ждать в 2013-м / PCWeek, 15.04.2013 [Електронний ресурс]. - Режим доступу : http://www.pcweek.ru/idea/blog/idea/4695.php

* Останніми роками ці показники дійсно зростають в прогресії. Достатньо навести такі цифри: у 2008 році кількість унікальних користувачів Інтернету нарешті досягла 1 мільярда, на початку 2013 року – 2,75 мільярда (майже 40 % населення Землі), а до 2017 року, за прогнозами компанії Cisco Systems, онлайн-аудиторія зросте до 3,6 млрд осіб, склавши близько половини (48 %) людства. Згідно з тими ж прогнозами, у 2016 році глобальний трафік Всесвітньої мережі сягне 1,3 зеттабайт (1 зеттабайт дорівнює 1 мільярду терабайт), що перевищить сумарний трафік Інтернету з моменту його створення до 2012 року включно (Див.: ICT Facts and Figures - The World in 2013 / International Telecommunication Union (ITU) report [Електронний ресурс]. - Режим доступу : http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf; Cisco Visual Networking Index: Forecast and Methodology, 2012–2017 [Електронний ресурс]. - Режим доступу : http://clck.ru/8paTe).

[15] ICT Facts and Figures - The World in 2013 / International Telecommunication Union (ITU) report [Електронний ресурс]. - Режим доступу : http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf; Клепов А. Stealthphone: мобильность меняет вектор развития ИБ / Материалы конференции «Безопасность бизнеса. Технологии 2013» [Електронний ресурс]. - Режим доступу : http://bc.rbc.ru/msk/security2013/stuff.shtml

потужностей навіть середнього за класом смартфону цілком достатньо для перегляду будь-якого контенту та обміну ним, спілкування через акаунти користувача в поштових сервісах, соціальних мережах і Скайпі, завантаження додатків, користування GPS-навігатором та ін.. Тому, навіть без врахування суто «стільникової» складової комунікацій (розмови й повідомлення в мережах GSM), **сучасний смартфон є пристроєм, що з необхідністю, постійно, у тому числі без відома абонента, передає безпровідними інтернет-каналами його персональні дані** (включаючи навіть дані про поточне місцезнаходження користувача – якщо згадати про вбудовані функції GPS-навігації і геотегінгу фотознімків, зроблених камерою смартфона).* При цьому вже наприкінці минулого року у світі використовувалося 1,3 млрд смартфонів і було оформлено 1,1 млрд підписок на спеціальні онлайн-послуги для них.[16] І все ж очікується, що до 2015 року ці показники збільшаться майже втричі.[17]

Але ще швидше зростають продажі інших мобільних пристроїв з можливістю виходу в Інтернет. Їх вартість, функціональність та форм-фактор постійно вдосконалюються, стають чимдалі різноманітнішими – від звичайних «електронних книжок» і міні-планшетів до потужних ультрабуків, – і вже зараз ці «девайси» в принципі здатні задовольнити інформаційно-комунікаційні потреби будь-якого споживача. Вражаючими темпами даний сегмент IT зростає й кількісно: за прогнозами, **протягом наступних чотирьох років кількість продажів планшетних комп'ютерів збільшиться на 750 %, а електронних рідерів – на 550 %.**[18]

Відтак, цілком закономірними є цифри, що віддзеркалюють динаміку технологічної модернізації всесвітньої мережі. Станом на липень 2013 року на мобільні пристрої припало 17,4% світового інтернет-трафіку, при тому що роком раніше цей показник складав приблизно 11,1%.[19] Передбачається, що до 2016 р. обсяг глобального мобільного трафіку перевищить обсяг провідного, а в 2017 році їх співвідношення складе 55 % до 45 %.[20] Таким чином, **домінуючим трендом розвитку Інтернету є його перетворення на справді всюдисущу, загальнодоступну і абсолютно необхідну для нормальної життєдіяльності людства структуру**.

У тісній інтеграції з мобільними пристроями, безпровідними широкосмуговими інтернет-мережами, соціальними сервісами (Web 2.0) і обробкою «великих даних» (Big Data) розвиваються **сервіси т. зв. «хмарної»**

---

* При цьому, за статистикою, на 80 % мобільних телефонів, що використовуються нині у світі, не встановлено жодних засобів захисту.

[16] Internet 2012 in numbers / Posted in Tech blog on January 16th, 2013 by Pingdom [Електронний ресурс]. - Режим доступу : http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers/

[17] Mashable — Ожидается, что глобальный Интернет-трафик к 2015 возрастет в четыре раза [Електронний ресурс]. - Режим доступу : http://www.denwer.ru/ls/blog/mashable/324.html

[18] Там само.

[19] 17,4% глобального интернет-трафика приходится на мобильные устройства. 23 августа 2013 г. [Електронний ресурс]. - Режим доступу : http://internetua.com/17-4--globalnogo-internet-trafika-prihoditsya-na-mobilnie-ustroistva

[20] Cisco Visual Networking Index: Forecast and Methodology, 2012–2017 [Електронний ресурс]. - Режим доступу : http://clck.ru/8paTe

обробки даних (*cloud computing services*)[*], – один зі «стовпів» інфраструктури третього покоління.

Останніми роками ця технологія активно пропагується і масово впроваджується провідними світовими IT-корпораціями, проте справжній бум зросту хмарних ринків прогнозується у 2013-2015 рр. Достатньо сказати, що, за підрахунками авторитетної International Data Corporation (IDC), вже у 2015 році до 60 % всіх даних людства зберігатимуться у хмарах.[21] Більше того, за одностайними прогнозами провідних консалтингових компаній світу, **швидке вдосконалення та поширення хмарних технологій зараз є одним з тих ключових трендів, що в найближчі 5-8 років помітно вплинуть на глобальний розвиток** не лише IT-індустрії, але й бізнесу, фінансів, державного управління, медицини, освіти і багатьох інших сфер людського життя.[22] У найрозвиненіших регіонах світу вже прийняті стратегічні рішення та плани дій щодо системного та комплексного розвитку хмарних сервісів, розгорнута відповідна робота. Значне й стрімке зростання ринку хмарних послуг очікується найближчими роками і в Україні.[*] У контексті даної доповіді все це спонукає детальніше зупинитися на безпекових аспектах хмарних технологій.

Одразу треба підкреслити, що навіть порівняно з грід-системами, не кажучи вже про «проводово-апаратні» мережі попереднього покоління, сучасний хмарний сервіс та його архітектура є значно лаконічнішим, продуктивнішим, універсальнішим і, що суттєво, – дешевшим рішенням. Без сумніву, значні переваги хмар, розгляду яких буде приділена спеціальна увага в II розділі, стали однією з основних причин їх популярності й феноменально швидкого розповсюдження.

Разом з цим **фундаментальним недоліком хмарних сервісів є високі ризики їх використання**. У квітні 2012 року т. зв. «Берлінська група» – авторитетна міжнародна команда експертів з захисту персональних даних у

---

[*] ***Хмарні обчислення*** (англ. - *cloud computing*, також використовується термін «хмарна обробка даних») – технологія обробки даних, в якій комп'ютерні ресурси надаються користувачеві як Інтернет-сервіс. Користувач не повинен піклуватися про інфраструктуру, операційну систему, купівлю та оновлення програмного забезпечення, має доступ до власних даних онлайн, але, відповідно, не може повною мірою контролювати їх обробку і захист. Термін «хмара» використовується як метафора, ґрунтована на зображенні Інтернету як «хмарини» мережних зв'язків, або як образ складної інфраструктури, за якою ховаються усі технічні деталі. Згідно з визначенням Institute of Electrical and Electronics Engineers (IEEE), запропонованим в 2008 році, «хмарна обробка даних – це парадигма, у рамках якої інформація клієнта постійно зберігається на серверах в Інтернет і тимчасово кешується на клієнтській стороні, наприклад, на персональних комп'ютерах, ігрових приставках, ноутбуках, смартфонах і т. д» (Див.: Behl, A., Behl, K. Security Paradigms for Cloud Computing / CICSyN 2012: Fourth International Conference on Computational Intelligence, Communication Systems & Networks [Електронний ресурс]. - Режим доступу : http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=6273236).

[21] IDC Predictions 2013. Competing on the 3rd Platform: Opportunities at the Intersection of Mobile, Cloud, Social, and Big Data [Електронний ресурс]. - Режим доступу : http://clck.ru/8aXZM

[22] Докладніше про це див. зокрема: Symantec : Protecting a Cloudier Future. Market Report. November 2012. [Електронний ресурс]. - Режим доступу : http://www.symantec.com/content/en/us/enterprise/white_papers/esg-protecting-a-cloudier-future.en-us.pdf; Symantec. Avoiding the Hidden Costs of the Cloud. 15.12.2013. [Електронний ресурс]. - Режим доступу : http://www.symantec.com/connect/blogs/avoiding-hidden-costs-cloud; IDC Predictions 2013. Competing on the 3rd Platform: Opportunities at the Intersection of Mobile, Cloud, Social, and Big Data [Електронний ресурс]. - Режим доступу : http://clck.ru/8aXZM;

[*] Докладніше про розвиток хмарних технологій та ринків в Україні і світі – у наступних розділах.

телекомунікаційних мережах [23] – опублікувала результати спеціального профільного дослідження, що отримало назву «Сопотський меморандум». У документі фіксуються, зокрема, такі проблеми та ризики використання хмар:

- Технологія все ще знаходиться 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 відстежена. Це значно ускладнює оцінку ризиків і створення єдиних правил гри;
- Дотримання конфіденційності, недоторканості інформації та режиму доступу до неї не може бути проконтрольоване у хмарах;
- Під час передачі ПД потрапляють під юрисдикції, в яких не передбачено їх адекватного захисту;
- Провайдери та їх партнери використовують приватні дані у своїх інтересах без повідомлення про це володільця та його згоди;
- Локальні (національні) контролюючі інститути з захисту ПД фактично не мають можливості нагляду за процесом обробки даних провайдерами хмарних послуг.[24]

Висновки експертів цілком підтверджуються наявними цифрами та фактами. Результати глобального дослідження «Avoiding the Hidden Costs of the Cloud», здійсненого компанією Symantec на початку 2013 року, приводять до висновку про значний відсоток недоброчесних 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.[25]

В контексті прогнозів щодо значного збільшення обсягів та масштабів використання віртуальної інформації (освоєння т.зв. «великих даних») хмари стають критично важливим ресурсом завдяки можливості зберігання у них практично необмежених обсягів даних, доступних онлайн для особистого та/чи корпоративного користування. Більше того, тренди ІТ-індустрії вже сьогодні роблять такі «мегасховища» дуже актуальними для користувачів.

Між тим, проведений у 2012 році глобальний моніторинг британської Icomm Technologies засвідчив, що сьогодні хмарні сервіси зберігання даних здебільшого не відповідають як елементарним вимогам безпеки, так і нормам законодавств. На запити володільців щодо фізичного місцезнаходження їхніх даних (країна, точне розташування) та, відповідно, щодо їх поточної юрисдикції 70% провайдерів не змогли дати відповіді, або всіляко

[23] International Working Group on Data Protection in Telecommunications (IWGDPT) [Електронний ресурс]. - Режим доступу : http://clck.ru/8aXVe

[24] 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) [Електронний ресурс]. - Режим доступу : http://clck.ru/8aJ9c

[25] Мошеннические облачные сервисы - бич 77% компаний. SecurityLab.ru. 23.01.13. [Електронний ресурс]. - Режим доступу : http://www.securitylab.ru/news/436587.php

намагалися її уникнути. У матеріалах моніторингу підкреслюється, що прагнучи знайти найвигідніші умови для фізичного розміщення даних, більшість провайдерів практикують оренду площ та потужностей у віддалених країнах, нерідко з недосконалим законодавством у сфері кіберзахисту та захисту персональних даних. Зрозуміло, що в аспекті безпеки даних таке становище створює серйозні ризики щонайменше за двома напрямками: 1) нормативно-правовий (конфлікт юрисдикцій в частині регулювання транскордонної передачі даних та обмежень щодо їх захисту); 2) технологічний (ситуації, коли (а) надмірна віддаленість сервера може призвести до затримок транспортування даних і критичних помилок у роботі програм і (б) один потужний дата-центр обслуговує велику кількість споживачів по всьому світу[*]).[26]

Красномовним підтвердженням недостатньої надійності сучасних хмар для розміщення і зберігання приватних даних є обережне ставлення до них самих розробників. За даними дослідження, здійсненого компанією Lieberman Software, більше половини (51%) IT-спеціалістів, що мають безпосередній стосунок до розробки та обслуговування хмарних сервісів, відмовляються зберігати в них свої особисті дані, а 86% – критично важливу корпоративну інформацію.[27] У листопаді 2012 року компанія провела опитування учасників світового конгресу Cloud Security Alliance (CSA), причому з'ясувалося, що 88% з них вважають небезпечним зберігання даних у хмарі через високий ризик їх втрати та/або викрадення.[28]

Судячи з деяких відомостей, свою роль тут відіграє й певна парадоксальність сприйняття масовим Інтернет-користувачем «плюсів» та «мінусів» хмарних технологій. Так, згідно з дослідженням, проведеним в середині минулого року в США і Канаді компанією CA Technologies, у 2013 році більше половини американських організацій планують використання хмарних сервісів для реалізації своїх бізнес-стратегій. Основний відсоток тих опитаних, хто використовує для цього приватні хмари (84%) і переважна більшість тих, хто послуговується сервісами публічними (73%), переконані, що саме ці технології достатньо надійно захищають їхні дані. При цьому всі без виключення респонденти заявили, що стикалися з втратою та/або витоком корпоративних і особистих даних і в 76% випадків це було пов'язане з «відмовою IT-систем» (себто, у більшості випадків – тих самих хмарних сервісів).[29] Абсолютна ж більшість (91%) учасників вищезгаданого

---

[*] Тут доречно згадати про випадок, коли ураган «Сенді» пошкодив декілька дата-центрів у Нью-Йорку і це призвело до «падіння» багатьох веб-ресурсів в різних кінцях планети.

[26] Firms Run Data Protection Risk by Not Checking Where Information is Held in the Cloud. Icomm Technologies. 05.11.2012 [Електронний ресурс]. - Режим доступу : http://www.icomm.co.uk/Thought-Leadership/Press-Releases/Firms-Run-Data-Protection-Risk.aspx; Облачные провайдеры прячут данные от заказчиков [Електронний ресурс]. - Режим доступу : http://www.cnews.ru/news/top/index.shtml?2012/11/21/510449

[27] IT-специалисты не спешат доверить свои данные "облаку". NEWS.ru.com. Технологии. 14.12.2012. [Електронний ресурс]. - Режим доступу : http://hitech.newsru.com/article/14dec2012/cloudrisk

[28] Lieberman Software: IT-специалисты не доверяют облачным сервисам. SecurityLab.ru. 14.12.2012. [Електронний ресурс]. - Режим доступу : http://www.securitylab.ru/news/435160.php

[29] U.S. Companies View Cloud Computing as Key to Improved Data Protection [Електронний ресурс]. - Режим доступу : http://investor.ca.com/releasedetail.cfm?releaseid=674043

світового конгресу Cloud Security Alliance (CSA), критикуючи хмарні сервіси, все ж визнала, що на даний момент вони є одним з найбільш ефективних, зручних та економних бізнес-рішень.[30]

Загалом, на даний момент весь комплекс проблем, пов'язаних з дотриманням безпеки персональних даних у хмарах, можна дещо умовно поділити на дві групи:

Системні, тобто такі, що випливають з самої архітектури хмари як техніко-технологічного рішення. Тут, за великим рахунком, невирішеними остаточно є питання щодо: а) **безпеки** ПД як такої, тобто принципової здатності сервісів гарантувати зберігання та обробку даних згідно з законом; б) фізичного **розміщення** ПД та їх **транскордонної передачі**, оскільки утримання дата-центра у будь-якій вигідній провайдеру точці Землі повністю відповідає самій ідеї хмари, але може бути небезпечним для користувача (див. вище); в) **доступу** користувача до своїх ПД, оскільки об'єктивно *не він* контролює цей доступ.

Ситуативні, тобто зумовлені поточними обставинами (фінансове та економічне становище, кон'юнктура ринків, недосконаліть законодавств, стихійні лиха, доступ до обладнання тощо). З наведених вище фактів видно, що в умовах формування ринку і бурхливого зростання, що його зараз переживає хмарна індустрія, значна кількість гравців – через свідому недоброчесність, або з інших причин – не забезпечує достатнього рівня захищеності споживачів та їх ПД. На відміну від об'єктивних, ці проблеми здебільшого не мають системного характеру і можна очікувати, що з подальшим розвитком ІТ і встановленням єдиних правил гри на ринку галузі вони значною мірою будуть розв'язані.

Судячи з усього, саме незаперечні і значущі переваги хмар – навіть при низькому рівні їх безпеки – є вирішальною причиною швидкого зросту їх популярності і роблять їх актуальним трендом глобального розвитку. Власне, над розвитком та оптимізацією хмарних технологій інтенсивно працюють нині кращі сили глобальної ІТ-індустрії. В тому числі постійно вдосконалюється їх безпекова складова, проте з викладеного вище зрозуміло, що **на даний момент, застосовуючи хмарну модель зберігання та обробки інформації, досить проблематично гарантувати володільцеві (а) постійний і стабільний доступ до його даних, (б) недоторканість цих даних, (в) контроль за їх обробкою, (г) точні відомості про їх місцезнаходження**, – іншими словами, проблематично гарантувати його фундаментальне право на «прайвесі».

Завершуючи цей огляд основних загроз недоторканості приватного життя людини у кіберпросторі, доречно хоча б коротко згадати про ще одну небезпеку, яка поки що не є цілком очевидною, проте обіцяє стати значущою в найближчому майбутньому. А саме: в умовах швидко прогресуючої «інтернетизації» технічних засобів та інфраструктур (насамперед – побутових), чимдалі важливішим джерелом пов'язаної з особою інформації

[30] Там само.

стають **віртуальні пошукові машини, що працюють з т. зв. «тіньовим Інтернетом»** – веб-адресами серверів, веб-камер, принтерів, роутерів та іншої підключеної до мережі ІТ-периферії, а також світлофорів, камер безпеки, домашніх систем автоматизації та опалення.[31] Всі ці відомості також можуть групуватися навколо «віртуального образу особи», лягаючи в контекст інших даних і надаючи додаткові подробиці про її приватне життя.

Підсумовуючи, підкреслимо, що якраз завдяки тому, що окреслені вище проблеми дотримання безпеки ПД стосуються кіберпростору, у найближчому майбутньому саме вони стануть ключовими і першочерговими у справі захисту. Справді, враховуючи хоча б ті факти, що (а) існування і подальший розвиток всіх основних інфраструктур та видів діяльності людства уже практично неможливі без Інтернету, (б) зараз більше третини населення Землі користується Інтернетом, а у 2015 році, за прогнозами, ним користуватиметься половина і (в) абсолютна більшість користувачів буде спілкуватися у соціальних та інших комунікативних веб-сервісах, причому здебільшого з мобільних пристроїв – **практично вся зафіксована інформація, включаючи персональні дані, надалі зберігатиметься та обертатиметься у Всесвітній Павутині**.

Безумовно, в цій ситуації для потенційних зловмисників виникає питання пошуку й обробки потрібної інформації, і нерідко це стає значною проблемою, оскільки може йтися про буквально астрономічні обсяги надзвичайно різноманітних, довільно структурованих і часто «нечитабельних» даних. Проте апаратна продуктивність і програмне забезпечення сучасних ІКТ в принципі дозволяють вирішити дану проблему.

Сьогодні вже існують **ІТ-платформи глибокого датамайнінга**[*], орієнтовані якраз на дуже тонке «просіювання» дуже великих невпорядкованих масивів даних, та/або на паралельну обробку всіх доступних баз даних з метою знаходження та аналізу пов’язаних між собою (звичайно, в контексті відповідного запиту оператора платформи) фрагментів інформації. У цих надпотужних системах застосовуються алгоритми та методи аналізу, базовані на апроксимованій моделі людського мислення, що дозволяє їм адекватно та гнучко реагувати на семантично складні запити і їх динамічні зміни. Яскравим прикладом таких апаратно-програмних рішень є продукція американської фірми Palantir, серед замовників якої – ЦРУ, ФБР, Міністерство оборони США, аналітичні служби американської армії, морської піхоти і військово-повітряних сил, а також ціла низка фінансових інститутів.[32] На даний момент подібні системи є одиничними і достатньо дорогими, але це жодним чином не означає, що «закладені» в них інноваційні технології залишаться без подальшого розвитку і поширення. Вся історія

---

[31] Однією з таких пошукових систем є, наприклад, Shodan (http://www.shodanhq.com/). Докладніше див.: Shodan – самый страшный поисковик Интернета [Електронний ресурс]. - Режим доступу : http://habrahabr.ru/post/178501/

[*] ***Датамайнінг*** (англ. - *Data Mining*) – термін приблизно можна перекласти на українську як «видобуток даних», «глибинний аналіз даних», «інтелектуальний пошук даних».

[32] Palantir, или Говорящие камни на службе ЦРУ / 3D news [Електронний ресурс]. - Режим доступу : http://www.3dnews.ru/621533

розвитку сучасної ІТ-індустрії свідчить, що скоріше за все буде навпаки. Поява ж таких технологій в загальному доступі ознаменує собою появу цілого кола нових загроз для безпеки персональних даних.

Загалом, **чимдалі ширша прірва між безпрецедентними «шпигунськими» можливостями сучасних онлайн-сервісів та ІТ і традиційними, «доцифровими» юридичними практиками, базованими на традиційному ж уявленні про межі й засоби забезпечення «прайвесі»**, є, мабуть, найскладнішим випробуванням для сучасної демократії. У Мадридській декларації про захист особистих даних «*Глобальні стандарти по захисту особистих даних для глобального світу*» від 3 листопада 2009 року прямо визнається, що законодавство в галузі захисту ПД, а також інститути, які цим опікуються, сьогодні вже не в змозі повною мірою враховувати нові методи спостереження, включаючи «поведінковий таргетинг», бази даних ДНК і інших біометричних показників, об'єднання даних державного і приватних секторів, а також особливі ризики, до яких схильні уразливі групи населення (діти, мігранти, представники меншин).[33]

Але будь-яка дієва демократія – це завжди баланс інтересів. І знаходження такого балансу задля **забезпечення інформаційних прав особи є достатньо складним завданням навіть у фізичному (невіртуальному) середовищі**: тут треба досягти певної динамічної рівноваги між фундаментальними правами людини (де сполучаються право на доступ до інформації, право на свободу слова і право на прайвесі), національними інтересами, вимогами міжнародного права. Проте з викладеного вище очевидно, що **ця складність зростає на порядки і набуває нового сенсу та якості у кіберпросторі**. **Якщо найближчим часом не буде знайдено ефективного і при цьому демократичного рішення проблеми захисту персональних даних у веб-середовищі – в перспективі це може призвести до непередбачуваних і небезпечних переосмислень загальноприйнятих уявлень про приватність, її сенс та межі, а відтак – до перегляду правового змісту самого поняття «персональні дані»**.

На даний момент світ в цілому і Європейська спільнота зокрема перебувають у пошуку ефективних рішень даної проблеми.

[33] Мадридская декларация о защите личных данных «Глобальные стандарты по защите личных данных для глобального мира» (3 ноября 2009 года) [Електронний ресурс]. - Режим доступу : http://online.zakon.kz/Document/?doc_id=31067860

Розділ II. Європейський досвід захисту ПД у кіберпросторі.

1. Правове регулювання.

Традиційно законодавство країн ЄС та право ЄС не передбачають спеціальних нормативних механізмів регулювання захисту ПД у кіберпросторі. На це середовище розповсюджуються загальні принципи та вимоги, передбачені законодавством про захист персональних даних, але з урахуванням специфіки обробки ПД з використанням інформаційно-комунікаційних систем. Для оперативного реагування на нові виклики досить широко використовуються інструменти «непрямого права» (*soft law*): рекомендації, стратегії, меморандуми, «точки зору» (*opinions*) авторитетних експертних чи політичних організацій щодо нових об'єктів регулювання тощо.

Європейське право включає майже два десятки загальноєвропейських конвенцій, директив та рекомендацій з питань захисту персональних даних, хоча кожна країна ЄС має також свої базові нормативно-законодавчі акти, локальні закони щодо обробки персональних даних у медичній, статистичній, державній, журналістській, поліцейській та інших сферах. При цьому існує низка міждержавних актів, обов'язкових для всіх країн-членів ЄС та/чи Ради Європи. Основними з них є:

1. Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних (учасницею якої є і Україна).
2. Додатковий протокол 2001 року до Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних (прийнятий і Україною).
3. Директива Європейського Парламенту і Ради №95/46/ЄС про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних (принципи Директиви підтримані Україною).
4. Рамкове рішення Ради ЄС № 2008/977/JHA про захист персональних даних у рамках поліцейського та судового співробітництва у кримінальних справах.
5. Регламент № 45/2001 про захист осіб у зв'язку з обробкою персональних даних інституціями та органами Співтовариства та про вільний обіг таких даних.
6. Директива №2002/58/ЕС щодо обробки персональних даних та захисту приватності у телекомунікаційному секторі.
7. Директива №2009/136/ЕС, що змінює Директиву №2002/22/ЕС про загальні послуги та права споживачів, пов'язані з електронними комунікаційними мережами та послугами, Директиву №2002/58/ЕС щодо обробки персональних даних та захисту приватності у телекомунікаційному секторі та Регламент № 2006/2004 про співробітництво між національними

органами, відповідальними за дотримання законодавства про захист прав споживачів.

Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних 1981 року – перший обов'язковий для виконання і відкритий для підписання міжнародний документ, що був спрямований не лише на захист фізичних осіб від зловживань, пов'язаних з обробкою даних, але й на регулювання транскордонної передачі ПД. По суті, Конвенція встановлює певний баланс між свободою переміщення даних і захистом/забороною на їх обробку у разі, якщо національне законодавство країни-отримувача даних не забезпечує належних гарантій їх нерозголошення. Документом спеціально обумовлені права володільця ПД (див. Вступ), встановлено обмеження обробки «чутливих» даних стосовно расової належності, релігійних та політичних поглядів, сексуального життя.

Основна мета *Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних* (ETS № 181) – вдосконалити застосування принципів, що містяться в Конвенції шляхом впровадження двох нових діючих положень, а саме про створення одного чи більше органів нагляду кожною Стороною та про транскордонне переміщення персональних даних в країни або організації, які не є сторонами Конвенції. Додатковий протокол до Конвенції 108 супроводжується пояснювальним звітом (прийнятим 23 травня 2001 р.), який не є інструментом для офіційної інтерпретації Протоколу, втім може мати такий характер з метою сприяння застосуванню положень Протоколу. Протокол відкрито для підпису в Страсбурзі 8 листопада 2001 р.

Стаття 1 Протоколу подовжує термін дії органів нагляду, визначених Статтею 13 Конвенції 108, які відповідають за забезпечення дотримання положень національного законодавства, що втілюють принципи, викладені в Конвенції та Протоколі. З цією метою органи нагляду мають, зокрема, повноваження розслідування та втручання, а також право:

- брати участь у судовому розгляді або повідомляти компетентні судові органи про порушення умов внутрішньодержавного права;
- розглядати заяви будь-якої особи відносно захисту його/її прав і основних свобод відносно обробки персональних даних, в межах своєї компетенції;
- виконувати свої функції в повній незалежності. Рішення органів нагляду можуть бути оскаржені у суді.

Стаття 2 передбачає, що передача персональних даних користувачам, які підпадають під юрисдикцію Держави або організації, яка не є Стороною Конвенції, може відбуватися за умови, що ця Держава або організація забезпечить адекватний рівень захисту відповідної передачі даних. Відхилення від цього положення дозволяється при передачі даних у таких випадках:

(а) якщо внутрішньодержавне право забезпечує це у зв'язку зі специфічними інтересами суб'єкта даних, або перевагою законних інтересів, надто – важливих суспільних інтересів, або

(б) якщо гарантії, що, зокрема, можуть походити з договірних положень, надаються контролером, відповідним за передачу, та визнаються достатніми компетентними органами відповідно до внутрішньодержавного права.

Директива 95/46/ЄС Європейського Парламенту та Ради Європи від 24 жовтня 1995 р. *про захист фізичних осіб при обробці персональних даних та вільного переміщення таких даних* розвиває, уточнює і подекуди посилює принципи, закладені в Конвенції № 108.

Директива була прийнята на основі статті 100а Договору про Європейський Союз (на сьогоднішній день, після внесення поправок – стаття 95 ЄС) з метою сприяння вільному переміщенню персональних даних шляхом гармонізації законодавчих актів, розпоряджень та адміністративних положень Держав-членів стосовно захисту окремих осіб при обробці таких даних.

Директива стосується захисту основних прав та свобод у внутрішньодержавних законодавствах щодо обробки персональних даних, в першу чергу права на приватне життя (див. П. 2.1.1), яке визнається Статтею 8 Європейської конвенції про захист прав людини та основних свобод та загальними принципами законодавства Європейського співтовариства. Директива також уточнює принципи, викладені в Конвенції Ради Європи від 28 січня 1981 р. (Конвенція 108, див. п. 2.1.2) про захист фізичних осіб при автоматизованій обробці персональних даних. Директива 97/66/ЄС уточнює положення даної Директиви в телекомунікаційному секторі. Обидві Директиви стосуються обробки персональних даних, включаючи переміщення даних щодо абонентів та користувачів мережею Інтернет. Статті 6, 7, 13,17 (1) та (2) Директиви 95/46/ЄС та Статті 4, 5, 6 та 14 Директиви 97/66/ЄС стосуються законності такої обробки телекомунікаційними операторами та постачальниками послуг. Ці положення дозволяють операторам та постачальникам послуг обробляти такі дані за досить обмеженими умовами. Стаття 6(1) передбачає, що персональні дані можуть збиратися лише для встановлених, чітких і законних цілей і надалі не можуть оброблятися у спосіб, несумісний з цими цілями. Стаття 6(1) передбачає, що персональні дані можуть зберігатися не довше, ніж це необхідно для цілей, заради яких дані були зібрані чи заради яких вони надалі обробляються. Стаття 5 гарантує конфіденційність передачі даних через державні телекомунікаційні мережі. Держави-члени повинні ввести заборону на прослуховування, запис, зберігання та інші види перехоплення даних іншими (крім користувачів) особами без згоди користувача цих даних, за винятком випадків, визначених законом у відповідності зі Статтею 14 (1). Існує загальне правило, згідно з яким дані, що передаються телекомунікаційними каналами, мають бути стерті або мають зберігатися анонімно після закінчені їх передачі (Стаття 6 (1) Директиви 97/66/ЄС).

Національні правила стосовного того. Скільки мають зберігатися дані, варіюються від 14 днів (у Норвегії) до 18 місяців (у Сполученому Королівстві).

Директива Європейського Парламенту і Ради Європейського Союзу від 12 липня 2002 року № 2002/58/ЄС «*Відносно обробки персональних даних і захисту конфіденційності в секторі електронних засобів зв'язку*» (Директива щодо обробки персональних даних та захисту приватності у телекомунікаційному секторі) (у редакції Директиви 2006/24/ЄС Європейського парламенту і Ради ЄС від 15 березня 2006 р., Директиви 2009/136/ЄС Європейського парламенту і Ради ЄС від 25 листопада 2009 р.). Директива забезпечує гармонізацію національних положень, необхідних для гарантії відповідного рівня захисту основних прав і свобод, і, зокрема, права на приватне життя і конфіденційність інформації про приватне життя у зв'язку з обробкою персональних даних у сфері електронних комунікацій, і для забезпечення вільного руху таких даних, пересування устаткування для електронного зв'язку і послуг електронного зв'язку в Співтоваристві. Документ репрезентує третє покоління законодавства про персональні дані, спрямоване на забезпечення права самовизначення людини при автоматизованій обробці його персональних даних в умовах прогресуючої відкритості і універсальності онлайн-комунікацій. Як один з засобів захисту ПД в такому середовищі, пропонується мінімізація їх кількості в призначених для користувача мережах і їх анонімності скрізь, де це можливо.

На рівні інституційного оформлення системи захисту ПД **велику увагу у європейському праві приділено організації органів державного нагляду за обробкою даних** (контролерів).

Відповідно до статті 1 Додаткового протоколу 2001 року до Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних:

1. Кожна Сторона передбачає один чи більше органів нагляду, відповідальних за забезпечення дотримання заходів, які передбачено її внутрішньодержавним правом і які втілюють принципи, викладені в главах II і III Конвенції (994_326) та в цьому Протоколі.

2. a. Для цього зазначений вище орган нагляду має, зокрема, повноваження стосовно розслідування та втручання, а також право брати участь у судовому розгляді або повідомляти компетентним судовим органам про порушення положень внутрішньодержавного права, що втілюють принципи, викладені в пункті 1 статті 1 цього Протоколу.

2 b. Кожний орган нагляду в межах своєї компетенції після розгляду приймає рішення у зв'язку із заявами будь-якої особи стосовно захисту її прав та основоположних свобод стосовно обробки персональних даних.

3. Органи нагляду виконують свої функції в повній незалежності.

Також Директива №95/46/ЄС передбачає вимоги щодо наглядових органів держав-членів ЄС, відповідальних за захист персональних даних на

національному рівні. Зазначені вимоги розвивають положення Конвенції Ради Європи:

Стаття 28. Наглядовий орган

1. Кожна держава-член передбачає, що один чи більше державних органів відповідають за моніторинг застосування в межах її території положень, прийнятих державами-членами відповідно до даної Директиви.

Ці органи діють у повній незалежності при здійсненні функцій, якими вони наділені.

2. Кожна держава-член передбачає, що при розробці адміністративних заходів чи положень, що стосуються захисту прав і свобод фізичних осіб при обробці персональних даних, проводяться консультації з наглядовими органами.

Кожен орган, зокрема, наділений:

- такими слідчими повноваженнями, як право доступу до даних, що є предметом операцій із обробки, і право збирати всю інформацію, необхідну для виконання його обов'язків із здійснення нагляду,
- ефективними повноваженнями на втручання, як-от надання висновків до здійснення операцій із обробки відповідно до статті 20 і забезпечення відповідного опублікування таких висновків, видання розпоряджень про блокування, стирання чи знищення даних, накладення тимчасової чи остаточної заборони на обробку даних, попередження чи винесення догани контролеру або повноваження звертатися до національних парламентів чи інших політичних інститутів,
- право брати участь у судочинстві, якщо були порушені національні положення, прийняті відповідно до даної Директиви, чи довести ці порушення до відома судових органів.

Рішення наглядового органу, що викликали скарги, можуть бути оскаржені в суді.

4. Кожен наглядовий орган розглядає запити, зроблені будь-якою особою чи об'єднанням, що представляє інтереси цієї особи, про захист її прав і свобод при обробці персональних даних. Особа, якої це стосується, повинна бути поінформована про результати розгляду запиту.

Кожен наглядовий орган, зокрема, розглядає запити про перевірки законності обробки даних, зроблені будь-якою особою, у випадках, коли застосовуються національні положення, прийняті у відповідності до статті 13 даної Директиви. Така особа повинна в будь-якому випадку бути поінформована про те, що перевірка мала місце.

5. Кожен наглядовий орган регулярно складає звіт про свою діяльність. Звіт повинен оприлюднюватись.

6. Кожен наглядовий орган має право, незалежно від того, яке національне законодавство застосовується до відповідної обробки, виконувати на території власної держави-члена повноваження, якими він наділений відповідно до пункту 3. Кожен орган може отримати прохання про виконання його повноважень від органу іншої держави-члена.

Наглядові органи співпрацюють один з одним у тій мірі, наскільки це необхідно для виконання їхніх обов'язків, зокрема, шляхом обміну всією корисною інформацією.

7. Держави-члени передбачають, що навіть після звільнення на посадових осіб і персонал наглядового органу поширюється обов'язок зберігати професійну таємницю відносно конфіденційної інформації, до якої вони мають доступ».

Загалом, всі ці норми спрямовані на досягнення двоєдиної мети: **максимальна незалежність національного контролера захисту та обробки ПД від політичних, адміністративних, фінансових впливів при збереженні максимальної прозорості діяльності і підзвітності перед суспільством.**

Разом з цим, нині саме керівництво ЄС визнає, що в частині регулювання захисту персональних даних у віртуальному середовищі **класичне законодавство Євросоюзу є застарілим і малоефективним**. При цьому в кожній державі ЄС є і своє національне законодавство про захист персональних даних, і свій контролюючий орган. В сучасних умовах це скоріше перешкоджає гармонізації відносин в галузі.

За офіційно оприлюдненими даними спеціального дослідження Єврокомісії в країнах ЄС, 74 % європейців сприймають дедалі меншу захищеність персональної інформації як характерну ознаку сьогоднішнього часу, причому пов’язують це передусім з участю у соціальних мережах (61 %) та з онлайн-шопінгом (79 %);[34] 72 % опитаних стурбовані кількістю персональної інформації, викладеної в Інтернет і відсутністю повноти контролю над власними даними. [35] Характерно, що при цьому більше половини опитаних (54 %) знайомляться з оголошеними на онлайн-сервісах умовами збору та подальшого використання наданих ними даних.[36]

Нині ведеться інтенсивна робота з модернізації відповідної правової бази. 25 січня поточного року були опубліковані пропозиції Єврокомісії по реформуванню законодавства про захист персональних даних в Європі – єдині для всіх країн ЄС **Стандарти захисту персональних даних Євросоюзу (European Data Protection Regulation)**[37], які мають замінити Директиву № 95/46/ЕС та визначити основні вимоги законодавства ЄС у сфері захисту персональних даних. В основу проекту було покладено результати широких консультацій з громадськістю, національними органами захисту персональних даних, Європейським контролером з питань захисту персональних даних та іншими агенціями ЄС.

---

[34] How will the data protection reform affect social networks? [Електронний ресурс]. - Режим доступу : http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf

[35] Why do we need an EU data protection reform? Правовий портал Європейської Комісії. [Електронний ресурс]. - Режим доступу : http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf

[36] How will the data protection reform affect social networks? [Електронний ресурс]. - Режим доступу : http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf

[37] Commission proposes a comprehensive reform of the data protection rules. Правовий портал Європейської Комісії. [Електронний ресурс]. - Режим доступу : http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

Стандарти спрямовані, передусім, на гармонізацію режиму захисту ПД в Європі і надання споживачам можливості контролювати, яким чином їх персональні дані обробляються компаніями. Особливий *акцент в Стандартах робиться на надання громадянам більшого обсягу можливостей контролю їх ПД і на питаннях користування дітей Інтернетом*. Пропонується, наприклад, встановити, що доступ до веб-сайтів, реєстрація на них, а також отримання розсилок цільового маркетингу особами молодше 18 років може здійснюватись тільки зі згоди їх батьків.*

У Стандартах, зокрема, передбачена низка заходів щодо спрощення процедур захисту персональних даних та послаблення бюрократичного тиску на здійснення таких процедур, а саме:

- створюються єдині правила із захисту персональних даних, дійсні в усьому ЄС. Виключаються зайві адміністративні вимоги, такі як відправка компаніями-операторами персональних даних повідомлень про обробку персональних даних в контролюючі органи;
- знижуються вимоги щодо повідомлення операторами персональних даних контролюючих органів про прийняті заходи по захисту персональних даних;
- встановлюється час, рівний 24 годинам, впродовж якого операторові персональних даних бажано повідомити національний контролюючий орган про інциденти з даними;
- оператори персональних даних матимуть справу тільки з одним національним контролюючим профільним органом. Крім того, громадяни можуть звернутися в такий орган в країні свого перебування, навіть якщо їх дані обробляє компанія, що базується за межами ЄС або в інших країнах ЄС;
- для використання і передачі персональних даних третім особам, операторам персональних даних буде необхідно отримати однозначну згоду громадян на здійснення таких операцій з персональними даними.

Стандартами передбачено також розширення прав осіб-володільців персональних даних при одночасному посиленні контрольованості та відповідальності операторів ПД:

- Гарантування **вільного доступу до власних персональних даних** в будь-яких базах даних.
- **«Право на вільне перенесення персональних даних»**. За новим законодавством громадяни повинні отримати спрощену процедуру передачі своїх персональних даних від одного постачальника послуг до іншого (мобільність даних). Передбачається, що це підвищить конкуренцію серед постачальників послуг.
- **«Право бути забутим»**, тобто полегшення для громадян процедур знищення своїх персональних даних в базах даних із забороною їх

* Показово, що основною причиною даної ініціативи представники Європейської Комісії назвали систематичні інциденти та судові процеси між державами, що входять в ЄС і великими компаніями, які реалізують свої сервіси в мережі Інтернет. Наприклад, скандал, пов'язаний з сервісом Google Street View, проти діяльності якого серед цілої низки інших країн виступили Франція і Бельгія.

подальшого використання, якщо немає законних підстав для їх збереження.

- **Право на добровільне і відкрите волевиявлення власника персональних даних** щодо певних типів їх обробки.
- **Розширення повноважень національних контролюючих органів** із захисту персональних даних. Зокрема, передбачене посилення дисциплінарних заходів щодо компаній, які порушують відповідні правила ЄС. В якості санкцій недобросовісному операторові персональних даних може бути виписане попередження за перше порушення, накладений штраф в розмірі від 250 тис євро або 0,5% від обороту за незначні порушення і штраф в розмірі до 1 млн євро або до 2% від загальносвітового річного обігу компанії у разі нанесення збитку суб'єктам персональних даних.
- Вводяться загальні принципи і правила по захисту персональних даних задля опитмізації міждержавної співпраці поліції і правоохоронних органів в т.ч. і у кримінальних справах.
- Нові правила ЄС повинні прийматися також і нерезидентами ЄС, якщо вони активно працюють на ринку ЄС і надають свої послуги громадянам ЄС.[38]

Передбачається, що в найближчому майбутньому Стандарти захисту персональних даних ЄС буде введено в дію на заміну Директиви Європейського Союзу 95/46/ЄС «Про захист осіб у зв'язку з обробкою персональних даних і вільним обігом цих даних» 1995 року.

У вересні 2012 року Європейська Комісія виступила зі стратегією **«Вивільнення потенціалу хмарних обчислень в Європі»** ("Unleashing the potential of cloud computing in Europe")[39], що спрямована на прискорення імплементації та значне розширення використання «хмар» в економіці ЄС. Передбачається, що реалізація цих завдань принесе 2,5 млн робочих місць і 160 млрд євро чистого прибутку щороку. Основними цілями стратегії є:

- Запровадження вже у 2013 році єдиних технічних та інших стандартів задля забезпечення належної мобільності, функціональної сумісності й оборотності даних;
- Підтримка співробітництва з достойними довіри провайдерами «хмарних» послуг в масштабах всього ЄС;

---

[38] European Commission. Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Правовий портал Європейської Комісії. [Електронний ресурс]. - Режим доступу : http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf; How will the data protection reform affect social networks? [Електронний ресурс]. - Режим доступу : http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf; Евросоюз предлагает реформирование законодательства в сфере защиты персональных данных [Електронний ресурс]. - Режим доступу : http://club.cnews.ru/blogs/entry/import_evrosoyuz_predlagaet_reformirovanie_zakonodatelstva_v_sfere_zashchity_personalnyh_dannyh_0de4

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

- Розвиток та підтримка моделі «безпечно і справедливо» (“safe and fair”) при укладенні угод на ринку «хмарних» послуг:
- Запровадження спеціальної інституції – Європейського «хмарного» партнерства (European Cloud Partnership – ECP) – за участю країн-членів та представників індустрії задля залучення потенціалу приватного сектора, оформлення європейського галузевого ринку, стимулювання європейських провайдерів з метою підвищення їхньої конкурентоздатності і запровадження оптимальної системи е-урядування.[40]

Спеціальну увагу у Стратегії приділено питанням безпеки користувачів і, зокрема захисту персональних даних. Як розробник документу, Європейська Комісія офіційно оголосила, що:

- Сьогодні саме проблеми захисту персональних даних на ринку «хмарних» послуг є найбільш серйозним бар’єром для його подальшого розвитку;
- Одним з ключових завдань, заявлених в Стратегії, є розробка особливої моделі «положень та умов» (terms and conditions) контрактів для сфер, які не регулюються Європейським законом про купівлю та продаж (Common European Sales Law). До таких належить і весь комплекс питань, пов’язаних із захистом персональних даних. Розробка адекватних юридичних рішень в цій сфері розглядається як «шлях до широкої популярності «хмарних» сервісів за рахунок зростання довіри користувачів»;
- Положення та завдання Стратегії «дбайливо узгоджені» з вищезгаданими Стандартами захисту персональних даних Євросоюзу (European Data Protection Regulation). Заявлено, що в Стандартах закладений «добрий загальний базис» для майбутнього розвитку європейського ринку «хмарних» послуг. У зв’язку з цим констатується важливість прийняття цього документа Радою Міністрів ЄС та Європейським Парламентом вже у 2013 році.[41]

В перспективі Європейська Комісія планує за участі ENISA та інших профільних організацій підтримувати постійні діалоги та консультації на міжнародних майданчиках, проводити дослідження задля відпрацювання оптимальних механізмів безпечного та ефективного використання «хмарних» технологій.[42]

В основу зазначених пропозицій було покладено результати широких консультацій з громадськістю, національними органами захисту персональних даних, Європейським контролером з питань захисту персональних даних та іншими агенціями ЄС.

В якості **основних напрямків реформи** слід відзначити такі:

[40] Digital Agenda: New strategy to drive European business and government productivity via cloud computing [Електронний ресурс]. - Режим доступу : http://europa.eu/rapid/press-release_IP-12-1025_en.htm?locale=en

[41] European Commission. Unleashing the Potential of Cloud Computing in Europe – What is it and what does it mean for me? Memo. [Електронний ресурс]. - Режим доступу : http://www.abbl.lu/sites/abbl.lu/files/FAQ_Cloud_Computing.pdf

[42] Там само.

- забезпечення прав осіб на захист персональних даних;
- економічний вимір захисту персональних даних;
- захист персональних даних у діяльності правоохоронних органів;
- міжнародний вимір захисту персональних даних.

Наведені законодавчі пропозиції Європейської Комісії викликали значний резонанс у пресі та серед окремих європейських політиків, лунають думки про надмірність, ба-навіть, нездійсненність запропонованих ЄК заходів.

На даний момент **ці законодавчі пропозиції оцінюються як найбільш складні проекти, які коли-небудь опрацьовувались Європейським Парламентом – євродепутатами було запропоновано близько 4000 поправок та пропозицій**. Серед держав-членів ЄС відсутня одностайність не тільки щодо остаточного тексту, але і щодо форми та правового статусу майбутніх законодавчих актів (зокрема, чи матимуть вони форму регламентів, які містять норми прямої дії, чи директив, які передбачають лише напрямки та цілі, проте імплементацію залишають на розсуд національних урядів). Окремі експерти, наближені до переговорного процесу, навіть висловлюють побоювання, що остаточні тексти міститимуть нижчі за передбачені чинними документами стандарти захисту персональних даних.[43]

Попри це, один з ініціаторів даних ініціатив єврокомісар з питань юстиції Вівіан Редінг незмінно наполягає на необхідності якнайшвидшого їх прийняття та імплементації у законодавство ЄС. У вересні поточного року вона закликала завершити цей процес вже до травня 2014 р., тобто до чергових виборів у Європейський Парламент.[44]

Але в будь-якому разі немає сумніву, що **ці дискусії і робота в євроінституціях визначать передові світові стандарти захисту персональних даних**. Водночас, враховуючи наявні контраверсійні позиції, **питання остаточної транспозиції нових європейських підходів у національне законодавство України доцільно було б опрацювати після завершення зазначених дискусій**.

[43] Представництво України при Європейському Союзі. Щодо актуальних питань захисту персональних даних. Лист від 11 червня 2013 р. №3111/16-600-1513.

[44] УНІАН. Єврокомісар закликала Євросоюз ввести загальні правила захисту даних [Електронний ресурс]. - Режим доступу : http://www.unian.ua/news/593894-evrokomisar-zaklikala-evrosoyuz-vvesti-zagalni-pravila-zahistu-danih-zmi.html

2. Техніко-технологічні рішення

Цілком закономірна неоднорідність кіберпростору як віртуального і технологічного середовища дозволяє дещо умовно виділити в його межах декілька зон, що відрізняються за критеріями (а) особливостей обробки/збереження ПД і (б) режиму доступу до них третьої сторони. А саме:

1) *автоматизована зона* – рівень мережного протоколу і локатора веб-ресурсів URL, куди дані про комп'ютер, місцезнаходження та історію відвідань користувача потрапляють «за замовчуванням», що обумовлено суто технічними потребами роботи Мережі;

2) *відкрита зона*, де особа добровільно розміщає в публічному доступі свої дані (сайти, блоги, чати);

3) *частково відкрита зона* – передусім комунікативні сервіси (e-mail, соціальні мережі, Skype, ICQ), де особа сама обирає режим доступу третьої сторони до своїх ПД;

4) *закрита зона* – локальні сховища підключених до Інтернету персональних пристроїв користувача (ПК, планшет, мобільний телефон тощо), до контенту яких в технічно можливий несанкціонований доступ.

Зазвичай, захист персональних даних в третій та четвертій зонах Інтернет-середовища регулюється узгодженими між собою міжнародними правовими актами та локальними законодавствами держав, де знаходяться володілець і розпорядник ПД. В ідеалі такого адміністративно-правового регулювання повинно бути достатньо для забезпечення повноцінного і повсюдного захисту персональних даних. У фізичному середовищі, можливо, так воно і є, але у віртуальному, для того щоб досягти хоча б базового рівня захисту ПД (контроль їх місцезнаходження, транзиту, доступу до своїх даних, можливість їх відкликати тощо) необхідні додаткові суто технічні інструменти.

Практика свідчить, що найчастіше персональні дані з використанням веб-ресурсів обробляються (санкціоновано чи ні) в рамках таких цілком добровільних з боку користувачів процесів як:

- заповнення відвідувачами веб-ресурсів анкет;
- реєстрація та отримання логіна та пароля;
- реєстрація з використанням облікового запису соціальної мережі;
- надання електронної адреси відвідувача для зворотного зв'язку.

При цьому можуть оброблятися ПД надзвичайно широкого діапазону: від анкетних, які явно є відомостями про особу яка ідентифікована, так і відомостей, які можуть стосуватися особи опосередковано або які можуть використовуватися в процесі ідентифікації особи: відомостей про оплату послуг з використанням платіжних карт, логіни та паролі, записи в соціальній мережі, номери телефонів, електронні адреси, тощо.

Поряд з тим, існує також надзвичайно широкий спектр **прихованих способів онлайн-доступу до персональних даних**, які користувач під час онлайн-сесії просто не в змозі зафіксувати і, отже, проконтролювати – від

класичного надсилання на пристрій «cookies»* до використання для доступу, нібито, цілком респектабельних ліцензійних програм, або «підселення» у пристрій спеціальних вірусів, ім'я яким легіон.

Але протиборство тих, хто бажає дістати чужі дані з тими, хто не бажає ними ділитися і взагалі воліє зберігати анонімність в онлайні, ніколи не припиняється. І хоча прийнято вважати, що в цій «гонці озброєнь» хакери завжди будуть на крок попереду, уже давно утворилося і продовжує поповнюватись не менш репрезентативне, ефективне та різноманітне **сімейство PETs – «технологій захисту приватності»** (приблизний переклад на українську усталеної англійської назви Privacy Enhancing Technologies – PETs). Грамотне і комплексне застосування цих технологій зазвичай дозволяє досягти безпечного перебування онлайн. [45] Щоправда, це передбачає наявність у користувача таких спеціальних знань та кваліфікації, які просто відсутні у сучасного пересічного відвідувача Мережі. Але в будь-якому разі, використання PETs схвалено і навіть рекомендовано спеціальним меморандумом Європейської Комісії. [46]

Свою специфіку має дотримання безпеки даних в новітніх онлайн-середовищах, про які уже згадувалося вище. Враховуючи тенденції та прогнози розвитку сучасної IT-сфери, спеціальної уваги заслуговує питання підвищення безпеки даних у хмарних сервісах.

Загалом сама архітектура хмарного сервісу є значно лаконічнішим, продуктивнішим і дешевшим рішенням порівняно з мережами попереднього покоління.

По-перше, хмари дозволяють істотно знизити капітальні витрати на побудову центрів обробки даних, закупівлю серверного та мережевого обладнання, апаратних і програмних рішень тощо. «Левова частка» цих видатків поглинаються провайдером хмарних послуг.* Додатково їхній клієнт економить на утриманні IT-персоналу, адмініструванні тощо. *По-друге*, хмарні технології забезпечують можливість надзвичайно оперативно змінювати конфігурацію корпоративної IT-інфраструктури в залежності від поточних потреб, споживаючи (і купуючи) рівно стільки ресурсів, скільки

---

* ***HTTP-cookies, «Кукі, кукіз»*** - (англ. *Cookies* - тістечка, печиво) – в комп'ютерній термінології – невеликі фрагменти текстових або бінарних даних, що відправляється веб-сервером і зберігається на комп'ютері користувача. При кожній спробі відкрити сторінку відповідного сайту веб-клієнт (браузер) користувача пересилає такий фрагмент даних веб-серверу у вигляді HTTP-запиту. «Офіційно» заявлене призначення і сфера застосовування є такою: а) збереження даних на стороні користувача б) аутентифікації користувача; в) зберігання персональних переваг і налаштувань користувача; г) відстежування стану сесії доступу.

[45] Ця проблематика має величезну літературу. Докладніше див. наприклад: Способы идентификации в интернете [Електронний ресурс]. - Режим доступу : http://javascript.ru/unsorted/id#primer; Советы по безопасной работе в интернете [Електронний ресурс]. - Режим доступу : http://www.windxp.com.ru/articles56.htm; Защита конфиденциальных данных и анонимность в интернете [Електронний ресурс]. - Режим доступу : http://clck.ru/8rWPJ; Как не оставлять следов в Сети [Електронний ресурс]. - Режим доступу : http://www.chip.ua/stati/kak-ne-ostavlyat-sledov-v-seti/;

[46] European Commission. Privacy Enhancing Technologies (PETs). The existing legal framework / MEMO/07/159 02/05/2007 [Електронний ресурс]. - Режим доступу : http://europa.eu/rapid/press-release_MEMO-07-159_en.htm

* Наприклад, De Novo, один з крупних українських хмарних провайдерів, гарантує скорочення витрат на IT-інфраструктуру до 50% у разі користування їхніми сервісами (Див.: http://www.de-novo.biz/arenda-servernoj-infrastruktury). Це досить типовий показник на сучасних галузевих ринках.

потрібно на даний момент. Ресурсів хмари зазвичай цілком вистачає для замовлення віртуального «суперкомп'ютера» або інфраструктури для великої корпорації, і при цьому не виникає проблем з оновленням програмного забезпечення (завжди доступні його останні версії), сумісністю різних операційних систем тощо. *По-третє*, хмарні сервіси надають можливість в буквальному сенсі носити своє робоче місце з собою – за наявності мобільного термінального пристрою і доступу до Інтернет користувач, незалежно від свого місцезнаходження, завжди має доступ до власного віртуального комп'ютера, зконфігурованого у хмарі, корпоративних мереж, баз даних тощо. *По-четверте*, постійно розширюється спектр послуг, пропонованих виробниками та провайдерами хмарних рішень. Як правило, їх «асортимент» цілком відповідає постійно зростаючим можливостям сучасної комп'ютерної техніки.[47]

Все це лише найвагоміші технологічні переваги хмарних сервісів, список яких можна продовжити. Понад це, виробникам та провайдерам хмар вдалося сформувати достатньо гнучку та адекватну потребам сучасного ринку систему надання послуг.[48]

У найрозвиненіших регіонах світу вже прийняті стратегічні рішення та плани дій щодо системного та комплексного розвитку хмарних сервісів, розгорнута відповідна робота. У глобальному вимірі ринок хмарних обчислень стає полем чимдалі жорсткішої конкуренції між провідними світовими IT-корпораціями (Google, Yahoo, Amazon, Microsoft, Zoho, Cisco, Symantec, Fujitsu і ціла низка інших). Крупні бізнес-гравці, які ще не мають своєї «долі» на цьому ринку, готуються завойовувати її в найближчому майбутньому. Така ситуація додатково інтенсифікує техніко-технологічну гонку, тому нові апаратні рішення, стартапи, програмне забезпечення, розробляються і просуваються у хмарному секторі справді випереджаючими темпами.

Ведуться активні роботи з міжнародної стандартизації хмарних обчислень. У двох технічних підкомітетах Об'єднаного технічного комітету №1 «Інформаційні технології» (Joint Technical Committee 1) Міжнародної організації зі стандартизації (International Organization for Standardization – ISO) йде робота над групою стандартів та технічних звітів стосовно хмарних технологій. Її результати передбачається оприлюднити наприкінці 2014 року.[49]

---

[47] Див. наприклад: http://www.fujitsu.com/ua/cloud/; http://www.sap.com/cis/solutions/technology/cloud/index.epx; http://www.symantec.com/cloud-computing-software;

[48] Докладніше про це див. зокрема: Гнатюк С. Перспективи розвитку ринку хмарних обчислень в Україні: переваги та ризики / Аналітична записка [Електронний ресурс]. - Режим доступу : http://www.niss.gov.ua/articles/1191/

[49] Докладніше див.: ДСЗПД України. Міжнародний досвід: Проводиться робота над групою стандартів, що стосуються хмарних обчислень. 19 березня 2013 року. [Електронний ресурс]. - Режим доступу : http://zpd.gov.ua/dszpd/uk/publish/article/53913;jsessionid=ABF5CECAF86F57E8E8E4B04651C56EDB; ИСО: Идет работа над группой стандартов, касающихся облачных вычислений [Електронний ресурс]. - Режим доступу : http://rusrim.blogspot.com/2013/03/blog-post_14.html; ISO/IEC CD 27040 Information technology -- Security techniques -- Storage security [Електронний ресурс]. - Режим доступу : http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44404

Хмарні технології вже зараз є одним із суттєвих чинників міжнародного розвитку, вплив якого найближчими роками багатократно зросте. Варто підкреслити, що як самий цей глобальний тренд, так і проблеми, пов'язані з його розвитком, **є дуже актуальними і для України**. За результатами опитування, проведеного у вересні 2012 року партнерами компанії «Майкрософт Україна» – «Софтлайн-ІТ» та Intecracy Group – вже через рік хмарні технології використовуватимуть 30% українських компаній. До 2015 року доля таких компаній зросте в Україні до 40% і більше.[50]

Разом з цим, **фундаментальним недоліком хмарних сервісів є високі ризики їх використання**, на розгляді яких автор спеціально зупинився у І розділі цієї доповіді. Це обумовлене як особливостями самої технології, так і тим фактом, що вона все ще недостатньо апробована для масового використання. Разом з цим, не можна заперечувати, що в організації та архітектурі хмарного сервісу існують ланки, що здатні стати потенційною основою потужної та ефективної системи захисту даних. Більше того, їх цілком можна розглядати як безпекові переваги порівняно з технологічним веб-середовищем попереднього покоління.

По-перше, в сучасних хмарних сервісах всі дані й трафік обов'язково шифруються (зазвичай – з використанням протоколу SSL - Secure Sockets Layer). Відтак, у персоналу хмарних дата-центрів, як і у будь-яких інших третіх осіб, немає прямого доступу до персональних даних користувача – без введення унікального пароля вони являють собою просто набір символів. До того ж, споживачеві завжди доступний додатковий ступінь захисту – шифрування інформації за допомогою електронного цифрового підпису, що, крім пароля, передбачає введення особливого електронного ключа, розміщеного на фізичному носії – спеціальній флешці, яка є тільки у володільця ПД. Все це робить прямий несанкціонований доступ до даних користувача, розміщених у віддалених сховищах достатньо проблематичним.

По-друге, професійному хакеру набагато простіше отримати доступ до інформації на локальному комп'ютері (наприклад, відправивши електронною поштою программу-троян), ніж намагатися зламати системи захисту хмарного дата-центра, де він, зокрема, зіткнеться з протидією фахівців – системних адміністраторів.

По-третє, на випадок втрати даних унаслідок надзвичайної ситуації в сучасних дата-центрах, як правило, робиться резервне копіювання інформації на інші сервери.

По-четверте, сьогодні на рівні глобальних ІТ-підприємств ведеться постійна й масштабна робота з розробки щоразу досконаліших апаратно-програмних комплексів захисту даних у хмарах. Менеджер Cisco з маркетингу мережевих обчислень і віртуалізації Джеймс Уркхарт констатує: «Крупні постачальники хмарних послуг, такі як Amazon, CSC, HP, IBM,

[50] Прогноз: к 2015 году треть украинских компаний будут использовать облачные технологии [Електронний ресурс]. - Режим доступу : http://www.marrero.com.ua/oblachnye-tekhnologii/149-prognoz-k-2015-godu-tret-ukrainskikh-kompanij-budut-ispolzovat-oblachnye-tekhnologii

Salesforce.com, Verizon Business та інші, створили потужні механізми безпеки. Вони працюють не лише на прикладному, але і на інфраструктурному рівні і включають до свого складу такі інфраструктурні засоби, як міжмережеві екрани і системи шифрування».[51] Експерт Cisco твердить, що нині вже існують рішення для достатньо ефективного захисту будь-яких хмарних послуг.

Довідково. Серед сучасних високоефективних систем захисту даних можна назвати сімейство спеціалізованих апаратно-програмних рішень CloudSpan від компанії Layer 7 (CloudConnect, CloudProtect та CloudControl), а також JaxView for Cloud Management від компанії Managed Methods. Такі компанії, як Altor Networks, Catbird Networks і Reflex Systems, також адаптували свої продукти для безпеки центрів обробки даних до роботи в хмарному середовищі, яке дозволяє компаніям забезпечити безпеку використання хмарних сервісів. Платформа Symantec O_3 Cloud Identity and Access Control створює єдину точку доступу до будь-яких хмарних рішень та сервісів, застосовуючи при цьому трирівневий захист: контроль доступу, інформаційна безпека, управління інформацією.[52] Узагалі, системи безпеки стають дедалі більш диверсифікованими й гнучкими. Так, архітектура Cisco для хмарної безпеки дозволяє організаціям задавати системі складні індивідуалізовані налаштування. У документах компанії наводиться приклад такого налаштування: «віце-президент з продажів має право на доступ до глобальних прогнозів продажів, але якщо він спробує отримати такі дані через смартфон з території країни ім'ярек за допомогою невідомого протоколу і при цьому двома годинами раніше він виходив в мережу з повною аутентифікацією з Каліфорнії – запит має бути відхилено».[53] Цікаво, що нині хмарні технології вже самі по собі використовуються для створення надпотужних і надшвидкісних антивірусних мереж – наприклад, розподіленої мережі Kaspersky Security Network.[54]

Іншим словами, якщо в основі ідеології перших систем захисту даних у хмарах лежала ідея захисту корпоративних мереж за допомогою брандмауерів, то більшість сучасних рішень в цій галузі зорієнтовані передусім на захист точок доступу за рахунок поєднання міжмережевих екранів і засобів шифрування даних на рівні користувача. В результаті – яким би пристроєм не користувався абонент для доступу в хмару, дані будуть захищені на всіх стадіях їх обробки.

Усе вищевикладене – типовий набір аргументів, що зазвичай висувається виробниками й вендорами хмарних рішень на користь безпеки їх використання. Вони одностайно запевняють, що вже на даній фазі розвитку технології вірогідність втрати персональних даних, розміщених у хмарних дата-центрах набагато нижче, ніж у випадку, коли вони зберігається у традиційному персональному комп'ютері «під столом».

У будь-якому разі, не підлягає сумніву, що засоби захисту даних у хмарах швидко еволюціонують і вдосконалюються. Цей факт помітно

---

[51] SoftLine Company. Cebit-2013. Безопасность в «облаках» [Електронний ресурс]. - Режим доступу : http://www.softline.kiev.ua/ru/blog/blog-kompanii/cebit-2013/729-cebit-2013-bezopasnost-v-oblakakh.html

[52] Докладніше див.: Symantec создает новую систему безопасности для облаков [Електронний ресурс]. - Режим доступу : http://www.symantec.com/ru/ru/about/news/release/article.jsp?prid=20120314_01

[53] Cisco. Безопасность в облаке [Електронний ресурс]. - Режим доступу : http://www.cisco.com/web/UA/about/news/2011/11152011b.html

[54] Докладніше див.: Защита из облака — что такое Kaspersky Security Network [Електронний ресурс]. - Режим доступу : http://blog.kaspersky.ru/ksn/

збільшує рівень оптимізму серед експертів. Один з відомих IT-фахівців, член наглядової ради консорціуму Intecracy Group Антон Марреро, наприклад, впевнений, що «новітні розробки в області безпеки хмар мають повністю розвіяти побоювання клієнтів». За словами експерта, сьогодні провідні постачальники хмарних послуг зберігають у себе на серверах петабайти конфіденційних даних і за весь час не сталося жодної вагомої втрати/витоку даних.[55]

З іншого боку, важко не погодитись і з Річардом Стинноном (Richard Stiennon), аналітиком компанії GigaOM Pro і засновником фірми IT-Harvest, що веде дослідження в області інформаційної безпеки: «Досі ми не бачили жодного серйозного злому систем безпеки в хмарі, але рано чи пізно це обов'язково станеться. Це лише питання часу».[56]

Техніко-технологічна й інфраструктурна специфіка хмар обумовлює і специфічність ризиків, пов’язаних з їх використанням, – вони значною мірою відрізняються від інформаційних небезпек, типових для систем попереднього покоління і на даний момент є більш критичними. Але не варто забувати, що хмарні технології постійно та інтенсивно вдосконалюються, причому чи не найшвидше – саме той їх сегмент, що пов’язаний з безпекою персональних та корпоративних даних.

Крім того, суттєво підвищити рівень захисту даних у хмарі можливо, ретельно дотримуючись, так би мовити, певних правил виробничої гігієни. Резюмуючи міркування експертів у цьому питанні, можна виділити низку умов, що необхідні для досягнення прийнятного (хоча й не стовідсоткового) рівня безпеки сучасного хмарного сервісу для персональних даних користувача. Сьогодні це можливо за наявності таких обов’язкових складових:

- *Апаратна (фізична, хардверна) складова*: а) обладнання, на якому реалізована хмарна IT-інфраструктура, повинне знаходитися в захищеному приміщенні, з клімат-контролем, безперебійним живленням, ефективним протипожежним захистом; б) має бути забезпечене цілодобове обслуговування усієї інфраструктури; в) необхідним є фізичне розділення ресурсів, наприклад, інфраструктура, в якій обробляються критично важливі і конфіденційні дані, фізично повинна розташовуватися окремо від загальної інфраструктури, посилена безпека якої не передбачається.
- *Програмна (софтверна) складова*: а) повномасштабний антивірусний захист, особливо у разі користування такими сервісами як SaaS (програмне забезпечення як послуга) і PaaS (платформа як послуга); б) наявність спеціальних налагоджених мережевих екранів (брандмауерів, файрволів) для віртуальних машин, а також для усіх операційних систем, що задіяні в інфраструктурі; в) захист систем та програм в частині хоча б найпоширеніших уразливостей; г) обов’язкове

[55] Там само.

[56] Cisco. Безопасность в облаке [Електронний ресурс]. - Режим доступу : http://www.cisco.com/web/UA/about/news/2011/11152011b.html

шифрування принаймні важливої і конфіденційної інформації, розташованої в хмарі.

- *Адміністративно-нормативна складова*: а) пропускний режим в приміщеннях дата-центру (аж до біометричного контролю доступу), максимальна обмеженість, регламентація та облік доступу до інформації, що зберігається в спеціалізованих сховищах і базах даних; б) аутентифікація користувачів за логіном і паролем з обов'язковим шифруванням цього процесу; в) запровадження системи статусів користувачів з відповідною диверсифікацією прав та рівнів доступу до ресурсів інфраструктури; г) чітке дотримання провайдером норм діючого законодавства (в аспекті безпеки українського користувача – насамперед Закону України «Про захист персональних даних»).

Як видно, дотримання безпеки даних хмарного сервісу вимагає від провайдера, крім високого рівня уваги, відповідальності та професіоналізму, ще й постійних додаткових зусиль. Але в сучасному кіберпросторі (не має значення – хмарний це чи «традиційний» апаратно-провідний його сегмент) це твердження справедливе і по відношенню до пересічного володільця ПД. **В сучасному Інтернеті ефективний захист власних персональних даних залежить від користувача не менше ніж від національного контролера чи провайдера онлайн-послуг**. Для цього користувач також повинен бути відповідальним, уважним, мати певну суму спеціальних знань для грамотного використання і комбінування доступних йому інструментів дотримання безпеки, дотримуватись певної «гігієни» використання мережних ресурсів тощо. Іншими словами, **ідеться про своєрідну культуру онлайн-безпеки користувача та необхідність її популяризації в глобальному масштабі**.

Розділ III. Тенденції та проблеми розвитку системи захисту ПД в Україні.

Статтею 32 Конституції України прямо заборонене втручання «в особисте і сімейне життя» людини, в тому числі «збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди» крім випадків, передбачених Конституцією України та/чи визначених законом.[57] Разом з цим, треба визнати, що як саме поняття «персональні дані», так і правові практики, пов'язані з їх захистом та обробкою, є відносно новими, а отже, малознайомими для українського суспільства. Системна робота над створенням національних наглядових інституцій та законодавства у сфері захисту ПД триває в Україні лише з 2010 року.[*] Таким чином, наша держава знаходиться на початковій фазі цього процесу, і тому, для того щоб оцінити для неї перспективи захисту ПД у кіберпросторі, потрібно розглянути стан і тенденції розвитку системи в цілому.

6 липня 2010 року Україна ратифікувала базові європейські стандарти у сфері захисту персональних даних, зокрема *Конвенцію Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних* (Страсбург, 28 січня 1981 року, № 108) та *Додатковий протокол* до неї *щодо органів нагляду та транскордонних потоків даних* (ETS № 181). Крім того, нею було офіційно підтримано принципи Директиви 95/46/ЄС Європейського Парламенту і Ради ЄС «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року. Таким чином, **Україна взяла на себе зобов'язання адаптувати національне законодавство та систему захисту персональних даних до** положень цих актів, наблизивши його таким чином до європейських стандартів.

Одразу треба підкреслити, що **від створення дієвої, гармонізованої з європейським законодавством вітчизняної системи захисту персональних даних напряму залежить успішність інтеграції України в ЄС**. Насамперед, це стосується трьох основних аспектів.

По-перше, наявність такої системи є **підставою успіху т. зв. «безвізового діалогу» між Україною і ЄС**, що був офіційно започаткований на Самітах Україна - ЄС 9 вересня 2008 р. у Парижі та 29 жовтня 2008 р. у Брюсселі. Така умова прямо передбачена *Планом дій щодо лібералізації Європейським Союзом візового режиму для України*, прийнятого 22 листопада 2010 р. у Брюсселі.

---

[57] Конституція України / Верховна Рада України; Конституція, Закон від 28.06.1996 № 254к/96-ВР [Електронний ресурс]. - Режим доступу : http://zakon4.rada.gov.ua/laws/show/254к/96-вр

[*] Власне, першу редакцію Закону України «Про захист персональних даних» було прийнято 9 січня 2007 року, однак уже 30 січня 2007 року Президент України наклав вето на цей акт. 22 лютого 2007 року була прийнята Постанова Верховної Ради України про доопрацювання Закону України «Про захист персональних даних». Редакція Закону за № 2297-VI, що згодом стала основою українського профільного законодавства вперше була подана на розгляд ВР України 1 червня 2010 року (див.: http://zakon4.rada.gov.ua/laws/card/2297-17).

По-друге, імплементація європейських норм та принципів щодо захисту ПД є також передумовою для подальшого **розширення участі України в цілій низці європейських та міжнародних профільних організацій** (докладніше про це – нижче).

По-третє, створення єдиних для України та ЄС нормативно-правових «правил гри» у галузі захисту ПД абсолютно необхідне для повноцінного розгортання обмінів, контактів та співробітництва у політичній, бізнесово-фінансовій і багатьох інших сферах.

З 2010 року Україною була здійснена значна законотворча і адміністративно-організаційна робота зі створення національної системи захисту ПД. Подальшій імплементації європейських положень та норм багато в чому сприяло прийняття Закону України *«Про захист персональних даних», який був прийнятий Верховною Радою України 1 червня 2010-го і вступив в силу 1 січня 2011 року*. Закон базувався на основних принципах Директиви 95/46/ЄС. Деякі з пропозицій Єврокомісії вже тоді знайшли своє відображення в українському законодавстві. Зокрема: вимоги до згоди володільця на обробку даних; зобов'язання призначити окрему особу або інститут, відповідальний за захист персональних даних; право особи вимагати знищення даних.

Однією з вимог ЄС до у України відповідно до Плану дій є прийняття відповідного законодавства про захист персональних даних та створення політично та фінансово незалежного наглядового органу у сфері захисту персональних даних, а також імплементація Закону України «Про захист персональних даних» та забезпечення ефективного функціонування незалежного наглядового органу з питань захисту персональних даних, у тому числі шляхом передбачення необхідних фінансових і людських ресурсів.

9 грудня 2010 року Указом Президента України №1085/2010 *«Про оптимізацію системи центральних органів виконавчої влади»* утворено Державну службу України з питань захисту персональних даних як центрального органу виконавчої влади України, діяльність якого спрямовується і координується Кабінетом Міністрів України через Міністра юстиції України. 6 квітня 2011 року Указом Президента України №390 затверджене Положення про Державну службу України з питань захисту персональних даних.

У жовтні-листопаді 2011 року в рамках імплементації Плану дій щодо лібералізації ЄС візового режиму для громадян України відбулись експертні місії в Україну Європейської Комісії та Європейського агентства з питань юстиції (Євроюст) з метою обстеження поточного функціонування уповноваженого органу України з питань захисту персональних даних (ДСЗПД) на предмет відповідності встановленим для Європейського співтовариства стандартам незалежності (див. розділ 1, параграф 1). За результатами експертних місій було надано звіти, в яких зокрема рекомендовано звернути увагу на:

- внесення змін до Закону України «Про захист персональних даних» на основі рекомендацій європейських експертів;
- забезпечення незалежності уповноваженого органу України з питань захисту персональних даних.[58]

Треба підкреслити, що саме інституційна організація системи захисту ПД в Україні стала предметом найбільш інтенсивних консультацій з ЄК та Євроюстом. Експертами місії було зазначено, що перебування Державної служби України з питань захисту персональних даних у системі органів виконавчої влади **не надає достатніх гарантій інституційної незалежності** цього органу, оскільки за такої моделі зберігається високий ризик зовнішнього тиску і політичного впливу. [59] За результатами зазначеної експертної місії було запропоновано такі **вимоги щодо незалежності державного органу України із захисту персональних даних**: *«законодавство повинно забезпечувати інституційну, організаційну та повну функціональну незалежність органу із захисту персональних даних. Це означає, що при виконанні своїх функцій зазначений наглядовий орган повинен бути захищений від будь-якого зовнішнього впливу та мати необхідні повноваження та ресурси»*.[60]

Цікаво, що обґрунтовуючи ці положення, місія послалася на нещодавній власний досвід. Так, у жовтні 2012 року в Суді ЄС розглядалася ситуація з наглядовим органом із захисту ПД Австрії, подібна до української. Суд визнав дану інституцію такою, що не відповідає вимогам Директиви ЄС, мотивуючи це відсутністю достатньої функціональної незалежності цього органу від Уряду, оскільки він знаходився у структурі відомства федерального канцлера Австрії, його працівники були службовцями канцелярії і так далі.[61] Подібній же судовий розгляд мав місце 2010 року (рішення Суду ЄС від 9 березня 2010 року у справі С-518/07 «Європейська Комісія проти Федеральної Республіки Німеччини» (п.36 та 37 рішення)).[62]

За більшу ефективність моделі, при якій контролюючий орган з захисту ПД підзвітний саме парламенту, але при цьому зберігає особливий статус і повноваження, говорить також досвід Бельгії, Сполученого Королівства, Угорщини.[63]

І хоча *організаційна* незалежність Державної служби України з питань захисту персональних даних і була визнана експертами адекватною,

---

[58] Представництво України при Європейському Союзі. Щодо актуальних питань захисту персональних даних. Лист від 11 червня 2013 р. №3111/16-600-1513

[59] Там само.

[60] Там само.

[61] Справа С-614/10, European Commission v Republic of Austria, 16 жовтня 2012 р. [Електронний ресурс]. - Режим доступу : http://curia.europa.eu/juris/document/document.jsf?text=&docid=128563&pageIndex=0&doclang=EN

[62] Представництво України при Європейському Союзі. Щодо актуальних питань захисту персональних даних. Лист від 11 червня 2013 р. №3111/16-600-1513.

[63] Різак М. Правовий статус уповноваженого органу з питань захисту персональних даних в Україні: сучасний стан та перспективи розвитку / Наукові записки Інституту законодавства Верховної Ради України. - № 2/2013. – С.48. [Електронний ресурс]. - Режим доступу : http://instzak.rada.gov.ua/instzak/doccatalog/document?id=62276

експертною місією все ж було запропоновано передати ДСЗПД до юрисдикції Верховної Ради України.[64]

З огляду на зазначені висновки сторони ЄС, а також враховуючи відповідні положення Конституції України, *Міністерством юстиції як головним розробником законодавства України у сфері захисту персональних даних було внесено пропозиції щодо передачі функцій із захисту персональних даних до Уповноваженого Верховної Ради України з прав людини*.[65]

Черговим кроком у модернізації вітчизняного профільного законодавства став Проект Закону України від 28.05.2012 р. N 10472-1 «Про внесення змін до Закону України "Про захист персональних даних" (щодо удосконалення правового регулювання у цій сфері)», який було прийнято Верховною Радою України 2 жовтня того ж року. За багатьма формальними ознаками цей нормативний акт був зорієнтований на європейські норми, у тому числі – на розглянуті вище Стандарти ЄС. Так, Законом змінено сферу дію Закону України «Про захист персональних даних», в тому числі визначивши, що його дія поширюється на всі дії з обробки персональних даних, а не тільки в базах персональних даних. Закон розширив права суб'єктів персональних даних, зокрема на заперечення обробки своїх персональних даних, внесення застережень стосовно обробки своїх персональних даних, оскарження обробки персональних даних та відкликання згоди на обробку персональних даних.

При цьому дана редакція Закону неодноразово критикувалася вітчизняними експертами, спеціалістами Ради Європи, громадськими організаціями та деякими українськими посадовцями. [66] 8 листопада Президент України застосував до закону право вето. У його пропозиціях, офіційно направлених до Верховної Ради України, зокрема, відзначається, що введення в дію цього акту «призведе до дублювання повноважень органів виконавчої влади, не відповідає засадам утворення, ліквідації та реорганізації центральних органів влади, визначеним статтею 5 Закону України "Про центральні органи виконавчої влади"».[67]

На інституційну неврегульованість української системи захисту ПД в черговий раз вказали і європейські експерти: «істотним недоліком» Закону, прийнятого 2.10.2012 року вони знову назвали «відсутність чіткої норми про

---

[64] Представництво України при Європейському Союзі. Щодо актуальних питань захисту персональних даних. Лист від 11 червня 2013 р. №3111/16-600-1513.

[65] Там само.

[66] Див., наприклад: Эксперты просят Януковича ветировать закон о защите персональных данных [Електронний ресурс]. - Режим доступу : http://www.unian.net/news/529743-ekspertyi-prosyat-yanukovicha-vetirovat-zakon-o-zaschite-personalnyih-dannyih.html; Лутковская призывает Януковича ветировать закон о защите персональных данных [Електронний ресурс]. - Режим доступу : http://www.unian.net/news/530011-lutkovskaya-prizyivaet-yanukovicha-vetirovat-zakon-o-zaschite-personalnyih-dannyih.html

[67] Пропозиції Президента України до Закону «Про внесення змін до Закону України "Про захист персональних даних» [Електронний ресурс]. - Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=43550

організаційну та функціональну незалежність уповноваженого державного органа з питань захисту персональних даних».[68]

12 лютого 2013 року відбулись чергові багатосторонні консультації за участю експертів генеральних директоратів Європейської Комісії «Юстиція», «Внутрішні справи», Європейської служби зовнішньої діяльності, Представництва ЄС в Україні, Ради Європи, а також Національної комісії Франції з питань інформаційних технологій та свобод. У ході консультацій експерти погодились, що запропоноване українською стороною вирішення відповідатиме європейським стандартам незалежності органів захисту персональних даних.[69]

14 травня поточного року Верховною Радою України було прийнято «*Проект Закону про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних*» № 2836 від 17.04.2013, яким передбачений цілий ряд змін у законодавстві в контексті модернізації галузевої нормативно-правової бази.[70]

Так, цим актом внесено зміни до Кодексу України про адміністративні правопорушення, Закону України «Про захист персональних даних» та Закону України «Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних» **з метою визначення Уповноваженого Верховної Ради України з прав людини уповноваженим органом у сфері захисту персональних даних**. 6 червня 2013 року Президент України повернув Закон до Верховної Ради України зі своїми пропозиціями, а 3 липня того ж року український парламент прийняв його з урахуванням пропозицій Президента.[71] Зокрема: виключити з розділу II «Прикінцеві та перехідні положення» підпункт 3 пункту 3 та доповнити його приписом щодо передачі Державного реєстру баз персональних даних та заяв про реєстрацію баз персональних даних, поданих у встановленому порядку до набрання чинності цим законом.

З дня набрання чинності цим законом (01.01.2014 р.) Кабінету Міністрів України протягом трьох місяців доручено забезпечити у встановленому законодавством порядку передачу Уповноваженому Верховної Ради з прав людини Державного реєстру баз персональних даних і заяв про реєстрацію баз персональних даних, представлених до набрання чинності цим законом. Відповідно, до настання зазначеного терміну, спеціально уповноваженим державним органом у сфері захисту

[68] Коментарі експертів Ради Європи до змін до Закону України про захист персональних даних [Електронний ресурс]. – С. 24, 35 - Режим доступу : http://zpd.gov.ua/dszpd/doccatalog/document?id=51483.
[69] Представництво України при Європейському Союзі. Щодо актуальних питань захисту персональних даних. Лист від 11 червня 2013 р. №3111/16-600-1513.
[70] Див.: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=46647
[71] Там само.

персональних даних є Державна служба України з питань захисту персональних даних (ДСЗПД України).[72]

Таку реструктуризацію повноважень підтримали всі дотичні до реформування системи захисту ПД державні відомства та інститути (включаючи, відповідно, Президента України і Верховну Раду України), крім ДСЗПД України. Жодним чином не заперечуючи доцільність розформування ДСЗПД і подальшого вдосконалення механізмів захисту ПД в Україні, експерти Служби разом з цим вважають запропонований в Законі шлях хибним. На їхню думку, «*запропоновані зміни не повною мірою узгоджуються з природою конституційно-правового статусу Уповноваженого Верховної Ради України з прав людини*, який відповідно до статті 101 Конституції України здійснює парламентський контроль за додержанням конституційних прав і свобод людини і громадянина», у той час як «*…переважна більшість повноважень з питань здійснення державного контролю за додержанням законодавства про захист персональних даних,… за своєю природою є повноваженнями саме органів виконавчої влади*» (*курсив наш.* – С. Г.).[73] Відтак, вони вважають цю зміну «концептуально вразливою і такою, що не повною мірою узгоджується з відповідними положеннями Конституції та Закону України «Про Уповноваженого Верховної Ради України з прав людини.»[74]

ДСЗПД запропонувала власну модель модернізації: «…Серед існуючих моделей побудови органів державної влади в Україні *найбільш оптимальним варіантом є створення уповноваженого органу як державного органу зі спеціальним статусом* (*курсив наш.* – С. Г.). Державні органи зі спеціальним статусом мають визначені законодавством України особливі завдання й повноваження, щодо них може встановлюватися спеціальний порядок утворення, реорганізації, підконтрольності, підзвітності, а також призначення і звільнення керівників та вирішення інших питань.» В якості модельного приклада такого органу згадується Антимонопольний комітет України.[75]

Загалом, експерти ДСЗПД України, посилаючись на власні висновки та оцінки європейських спеціалістів, констатують, що вимоги поточної редакції Закону України «Про захист персональних даних» та застосування його положень при обробці персональних даних з використанням веб-ресурсів «повністю кореспондуються з рекомендаціями Комітету Міністрів Ради Європи щодо захисту недоторканості приватного життя в Інтернеті, рекомендаціями Робочої групи, що функціонує відповідно до статті Директиви 95/46/ЄС та рекомендаціями Міжнародної робочої групи (Берлінська група) з питань захисту персональних даних в

[72] Верховна Рада України 14 травня 2013 року ухвалила Закон «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних» [Електронний ресурс]. - Режим доступу : http://zpd.gov.ua/dszpd/uk/publish/article/56523

[73] Державна служба України з питань захисту персональних даних. Щодо актуальних питань захисту персональних даних. Лист від 20.06.2013 №09/1675-13.

[74] Там само.

[75] Там само.

телекомунікація».[76] Тут можна додати, що **з чинної редакції Закону були вилучені деякі архаїчні норми**, які не лише не регулювали обробку ПД у кіберпросторі, але у низці положень, по суті, унеможливлювали її. Серед іншого, переглянуто сферу застосування процедури реєстрації баз даних, яка є практично неможливою в онлайн, а тим більше – у «хмарах». Якщо раніше передбачалась безумовна та обов'язкова реєстрація таких баз, то тепер необхідно буде лише попереджати Уповноваженого про факт збору/обробки персональних даних, і лише в тому випадку, якщо вони несуть «особливий ризик для прав і свобод суб'єктів персональних даних» (відповідний перелік встановлюється Уповноваженим).[77]

Підсумовуючи, треба відзначити, що з 2010 року, коли фактично розпочалася робота зі створення української системи державного нагляду за обробкою і захистом персональних даних, Україні в цілому вдалося сформувати сучасну, адекватну європейським стандартам нормативно-правову базу для подальшого формування вітчизняної системи захисту ПД, що є значним досягненням, враховуючи безпрецедентні виклики, пов'язані з глобалізацією, революційними змінами в ІКТ, комунікаціях тощо.

Показником успішності і фахового рівня роботи українського регулятора захисту персональних даних ДСЗПД, є її широка міжнародна співпраця по лініям Євроюста, Європола (Європейський поліцейський офіс), OLAF (Європейське Бюро по боротьбі з шахрайством, англ. - *European Anti-Fraud Office*, зазвичай вживається скорочення від фр. - *Office de Lutte Anti-Fraude*), Групи керівників уповноважених органів з питань захисту персональних даних країн Центральної та Східної Європи, членство в Глобальній мережі усунення порушень в сфері приватності (GPEN – Global Privacy Enforcement Network), регулярний експертний обмін з Радою Європи, участь у Міжнародній робочій групі з питань захисту персональних даних в сфері телекомунікацій (IWGDPT – International Working Group on Data Protection in Telecommunications).[78]

Проте, якщо на рівні державних органів та експертних кіл ситуація у сфері захисту ПД є досить задовільною, **пересічні українці поки що демонструють** байдужість до цих нових для них правових практик і **недостатній рівень розуміння сутності персональних даних і значення їх захисту в сучасному світі, надто ж – в мережі Інтернет**.

Наприкінці 2012 року Всеукраїнською громадською організацією «Українська асоціація захисту персональних даних» було ініційоване та проведене перше **дослідження в рамках громадського моніторингу**

---

[76] Практика застосування законодавства з питань захисту персональних даних при обробці персональних даних з використанням веб-ресурсів. / Матеріали до відкритого засідання колегії Державної служби України з питань захисту персональних даних [Електронний ресурс]. - Режим доступу : http://zpd.gov.ua/dszpd/doccatalog/document?id=53900

[77] Див.: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=46647

[78] Див.: Козак В. Захист персональних даних: право, практика, нагляд [Електронний ресурс]. - Режим доступу : http://zpd.gov.ua/dszpd/doccatalog/document?id=51760

відкритості та прозорості обробки персональних даних в Інтернеті.[79] За результатами дослідження зокрема виявилося, що лише близько третини веб-ресурсів національного сегменту Інтернет надають суспільству та користувачам мінімальні відомості про розпорядника персональних даних – найменування юридичної чи ім'я фізичної особи, яка і є, відповідно до законодавства, відповідальною за обробку персональних даних відвідувачів та за дотримання їх прав на невтручання в сімейне та приватне життя. Так само, приблизно третина веб-ресурсів повідомляють відвідувачів про їх права.

Автори моніторингу також констатують: «Можна впевнено зробити висновок, що **переважна частина національних веб-ресурсів, можливо більше трьох четвертей, не забезпечують відкритості і прозорості обробки персональних даних**, ігнорують вимоги ратифікованої Україною Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних, положень Закону України «Про захист персональних даних», рекомендацій Комітету міністрів Ради Європи № R (99) 5 від 23.02.1999 р. державам-членам Ради Європи «Про захист недоторканості приватного життя в Інтернеті».[80]

Така ситуація є тим парадоксальнішою і тривожнішою, що **Україна належить до найперспективніших держав світу за показниками/прогнозами імплементації ІТ і проникненню Інтернет**. За офіційними даними НРКЗІ, при тенденції до стабільного зростання Інтернет-аудиторія України у 2012 році склала 43,5 % жителів, причому 35 % домогосподарств мали широкосмуговий доступ до Всесвітньої мережі (одне з перших місць в Європі). Уже в 2011 році Україна увійшла в першу десятку країн світу з найшвидшим доступом в Інтернет, і тоді ж, уперше – до рейтингу абонентів галузевої організації FTTH Council Europe. Згідно з останніми показниками цієї організації, оголошеними на Всесвітньому форумі з широкосмугових технологій (Париж, вересень 2012) Україна посідає 16 місце у світі за розвитком мереж FTTH.[81*]

Більше того, висока динаміка росту спостерігається і у тих секторах українського кіберпростору, які входять до групи особливого ризику з точки зору безпеки персональної інформації. Так, 56 % вітчизняних Інтернет-користувачів виходять в онлайн для спілкування в соціальних мережах,

---

[79] Див.: Проведено перший громадський моніторинг інтернет ресурсів / Всеукраїнська громадська організація «Українська асоціація захисту персональних даних» [Електронний ресурс]. - Режим доступу : http://uapdp.org/index.php/podiji/khronika-podij/144-pershiy-monitoring; http://uapdp.org/images/news/doslidzhennya/Research-results-v.2.2.pdf; http://uapdp.org/images/news/doslidzhennya/Check-list-v.0.4.pdf

[80] Там само. [Електронний ресурс]. - Режим доступу : http://uapdp.org/images/news/doslidzhennya/Research-results-v.2.2.pdf

[81] Звіт про роботу Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, за 2012 рік. – С. 14. [Електронний ресурс]. - Режим доступу : http://www.nkrz.gov.ua/uk/activities_nkrzi/1324727592/1364229681/

[*] FTTH (Fiber To The Home - волокно до будинку користувача) – архітектура побудови мережі, за якої волоконно-оптичний кабель використовується для з'єднання центру надання послуг і певного приміщення (квартири) або приватного будинку.

52 % – для користування електронною поштою.[82] Але **найкритичнішим обіцяє стати один з новітніх і найбільш неоднозначних в плані безпеки даних онлайн-секторів – ринок хмарних послуг**.

16 квітня ц.р. один з провідних українських операторів хмарних сервісів De Novo і GfK Ukraine презентували результати дослідження українського ринку хмарних обчислень.[83] Дослідження було сфокусоване на середніх і великих підприємствах фінансової, телекомунікаційної, роздрібної, логістичної і виробничої галузей, оскільки саме ці галузі є основними споживачами ІТ-послуг в Україні.

Згідно з зібраною статистикою споживання, **хмарний ринок України,** подібно до сусідніх (Російська Федерація, Угорщина, більшість країн СНД) **знаходиться на етапі формування попиту і акумулювання первинного досвіду споживання хмарних рішень**. Про це говорять мінімальний рівень знання кінцевих користувачів про хмарні обчислення і невисокий рівень проникнення технології. Так, 47 % опитаних ІТ-служб вважають свою обізнаність про хмарні рішення поверхневою, а 88 % опитаних керівників зовсім не знайомі з хмарними сервісами.[84]

Разом з цим, більше третини опитаних ІТ-служб планують користуватися хмарними рішеннями, а 75 % з них збираються почати використання вже в 2014 році. «Підігрівають» ринок і ІТ-компанії, що активно освоюють технологію та відповідні бізнес-рішення. За результатами дослідження, цю сферу вивчають близько половини опитаних керівників ІТ-компаній, 15 % вже мають експертизу в цій сфері, а 94 % планують працювати на хмарному ринку України. Швидкому проникненню хмарних обчислень на український ринок в 2014-2016 рр. сприятиме як цей чинник сам по собі, так і здебільшого позитивний досвід первинного споживання. Користування хмарними сервісами повністю, або майже повністю виправдало очікування 84 % опитаних українських організацій.[85]

Плани використання хмарних рішень українськими підприємствами, а також інтенсивне освоєння технології ІТ-компаніями створюють потенціал ринку, який «**до 2015-2016 рр. демонструватиме експоненціальне зростання, характерне для хмарних ринків розвинених країн**».[86]

Показово, що практично таких самих оцінок та висновків щодо України дійшли також експерти компанії Parallels, дослідивши наприкінці 2012 року динаміку хмарних ринків у країнах СНД.[87]

*Зрозуміло, що **швидкий розвиток українського онлайн-середовища**, при всій оптимістичності пов'язаних з цим перспектив, додатково **загострює і актуалізує весь комплекс проблем захисту ПД «у віртуалі».***

---

[82] Там само.
[83] GfK Ukraine. De Novo и GfK Ukraine измерили облачный потенциал Украины. [Електронний ресурс]. - Режим доступу : http://www.gfk.ua/public_relations/partners_news/materials/010936/index.ua.html
[84] Там само.
[85] Там само.
[86] Там само.
[87] Колеров Ю. Облачный рынок в цифрах и фактах: взгляд Parallels. Доклад на CLOUD Computing Summit 2013 (1 марта, Киев) [Електронний ресурс]. - Режим доступу : http://www.ex.ua/view_storage/271113003934

Для успішного протистояння викликам у цій сфері Україна потребує щонайменше: *а) адекватного правового забезпечення та ефективної національної системи регулювання та нагляду; б) розвиненого й диверсифікованого ринку юридичних послуг; в) грамотних і відповідальних контрагентів – провайдерів онлайн-послуг та їх споживачів, володільців персональних даних та їх розпорядників. З цих трьох мінімально необхідних складових – впевнено поки що можна говорити лише про досить успішне формування першої.*

Утім, певна робота ведеться й на рівні громадських та експертних організацій. Третій український форум з управління Інтернетом, що відбувся в Києві 28 вересня 2012 року, в своїй Резолюції ухвалив адресувати постачальникам послуг Інтернет звернення щодо доцільності дотримання рекомендацій Комітету міністрів Ради Європи № R(99)5 від 23.02.1999 р. державам-членам Ради Європи «Про захист недоторканості приватного життя в Інтернеті».[88]

За ініціативи вищезгаданої Української асоціації захисту персональних даних 25 жовтня 2012 року було прийнято Декларацію «За недоторканість приватного життя в Інтернеті», до якої приєдналися низка провідних національних телекомунікаційних компаній.

У вересні 2013 р. було опубліковано посібник «Кібертероризм і захист персональних даних», який став результатом дослідницької роботи колективу експертів ТОВ «Консалтингова компанія «СІДКОН», виконаної в інтересах ВГО «Українська асоціація захисту персональних даних». Автори посібника акцентують на залученні підвищеної уваги державних органів, а також керівників комерційних компаній до проблеми, пов'язаної з кібертероризмом і захистом державних і корпоративних інформаційних ресурсів, персональних даних громадян, а також демонстрації масштабу поширення і необхідності першочергового вирішення зазначеної проблеми.[89]

Подібні акції свідчать про усвідомлення експертною та професійною спільнотою необхідності розгортання в Україні системної роботи довкола підвищення правової культури, поширення адекватного сприйняття «прайвесі» в суспільстві, бізнесі та політиці, встановлення певних єдиних «правил гри» щодо обробки і захисту персональних даних як у фізичному, так і в віртуальному середовищі. Водночас, дані вищезгаданого моніторингу обробки персональних даних в національному сегменті Інтернет переконують у тому, що на сьогодні всі ці поняття і практики тільки починають засвоюватись українським суспільством.

[88] Третій український Форум з управління Інтернетом. м. Київ, 28 вересня 2012 р. Резолюція Форуму. [Електронний ресурс]. - Режим доступу : http://igf-ua.org/docs/Resolution_IGF-UA_2012.pdf

[89] Див. сайт Української асоціації захисту персональних даних - www.uapdp.org.

ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

І

1. Захист персональних даних трактується в європейській правовій традиції як одна з неодмінних підстав забезпечення фундаментального права людини на недоторканість її особистого життя, яке в свою чергу, є основоположним для сучасної демократії з її приматом поваги до прав та гідності людини. Нині ця точка зору є загальновизнаною у світі: недоторканість приватного життя, в тому числі особистої інформації людини, як одне з її основних прав закріплене в найважливіших міжнародних актах сучасності, а також в абсолютній більшості національних законодавств світу.

2. Разом з цим, нині не лише в ЄС, а й практично в усіх країнах та міждержавних об'єднаннях **найбільш проблемною сферою захисту ПД стали ІТ і кіберпростір** як нове специфічне інформаційно-комунікаційне середовище, яке стрімко розвивається і збільшується. **У цій галузі нормативно-правове регулювання хронічно відстає від якісного (технології) та кількісного (продуктивність і поширеність інфраструктур) розвитку**. Це відставання намітилося ще в 90-ті роки минулого століття, але воно **стало справді системною проблемою протягом 2000-х років** разом із революційними винаходами та змінами в інформаційно-комунікаційних технологіях (ІКТ), лавиноподібним поширенням всесвітньої мережі і міграцією цілих галузей людської діяльності в онлайн-сектор.

3. Основним протиріччям тут є **чимдалі ширша прірва між безпрецедентними можливостями сучасного Інтернет-середовища** та асоційованих з ним електронних пристроїв щодо неконтрольованого збору, обробки, зберігання і оприлюднення гігантських обсягів різних ПД, – **і традиційними, «доцифровими» юридичними нормами та практиками**, базованими на традиційному ж уявленні про межі й засоби забезпечення приватного життя людини.

4. Поряд з цим, **тотальна комп'ютерізація** телекомунікацій, систем транспортування, фінансів, обліку населення, медичного обслуговування, численних баз даних **постійно збільшує кількість та якість інформації, що опрацьовується відносно кожної особи**, причому зазвичай без її відома. Існує і постійно вдосконалюється ціле сімейство технологій для датамайнінга й створення індивідуальних «онлайн-портретів» на основі збору та аналізу всіх відомостей, що мають будь-який (хай і непрямий) стосунок до користувачів. **Рівень «деанонімізації» користувачів в сучасному онлайн-середовищі стає**

практично стовідсотковим, навіть якщо вони дотримуються вимог безпеки.

5. **Додаткові і дуже серйозні ступені ризику щодо безпеки даних несуть у собі елементи новітньої третьої IT-платформи**, яка нині активно впроваджується у світі і принципово орієнтована на: а) зберігання основної частини інформації користувачів не на особистих фізичних носіях, а у віртуальному середовищі (хмарні сервіси); б) повсюдний швидкісний безпровідний доступ до Інтернету. Практика свідчить, що на даний момент така **модель зберігання та обробки інформації не може гарантувати володільцеві (а) постійний і стабільний доступ до його даних, (б) недоторканість цих даних, (в) контроль за їх обробкою, (г) точні відомості про їх місцезнаходження**, – іншими словами, проблематично гарантувати його фундаментальне право на «прайвесі».

6. Загалом, на даний момент **суть проблеми захисту персональних даних у кіберпросторі визначається двома процесами**, що є тісно пов'язаними і доповнюють один одного:
   з одного боку – **перманентне і швидке збільшення кількості персональних даних громадян у публічному та/чи несанкціонованому ними доступі**;
   з іншого боку – **перманентне ж зменшення для пересічного громадянина реальних можливостей контролю цього процесу** (а саме – збору й обробки власних ПД).

   Поки що **ці дві тенденції є прогресуючими і стабільними рівно настільки ж, наскільки сталим є розвиток самого кіберпростору**, незважаючи на численні скандали, судові позови, суспільні та законодавчі ініціативи, вимоги права і вдосконалення систем безпеки.

7. У суто соціальному вимірі основний вектор цього розвитку резюмується в **швидкому перетворенні глобального Інтернет-середовища на справді всюдисущу, загальнодоступну і абсолютно необхідну для нормальної життєдіяльності людства структуру**.

8. Відтак, **практично вся зафіксована людиною інформація, включаючи персональні дані, надалі обертатиметься та зберігатиметься у Всесвітній Павутині.**

9. Таким чином, **якщо найближчим часом не буде знайдено ефективного і при цьому демократичного рішення проблеми** захисту персональних даних у веб-середовищі – у перспективі **це може призвести до непередбачуваних і небезпечних переосмислень загальноприйнятих уявлень про приватність, її сенс та межі, а відтак – до перегляду правового змісту самого поняття «персональні дані»**.

II

10. Нині саме керівництво ЄС визнає, що в частині регулювання захисту персональних даних у віртуальному середовищі **класичне законодавство Євросоюзу є застарілим і малоефективним**. З 2011 року в Європейської Комісії триває робота над глибокою реформою нормативно-правового поля Співтовариства в сфері захисту персональних даних.

11. **Єврокомісія здійснює спроби правового врегулювання питань захисту ПД з урахуванням нових викликів та загроз у кіберпросторі, виходячи при цьому з позиції безумовного пріоритету невід'ємного права особи на недоторканість і вільне розпорядження власними персональними даними**. В цьому ж напрямі формуються і стандарти в сфері розширення прав осіб-володільців персональних даних при одночасному посиленні контрольованості та відповідальності операторів ПД.

Варто враховувати, що нові правила ЄС повинні прийматися також і нерезидентами ЄС, якщо вони активно працюють на ринку ЄС і надають свої послуги громадянам ЄС.

12. Попри те, що Стандарти ще не прийняті, вони є чітким індикатором сучасних настроїв в Єврокомісії (а, вірогідно, і загалом у керівництві ЄС) які спрямовані на **наданні громадянам більших можливостей контролю використання їхніх персональних даних за рахунок вдосконалення адміністративних процедур, розширення їх прав і збільшення контрольованості та відповідальності компаній-операторів** в питаннях захисту і обробки персональних даних.

13. У вересні 2012 року Європейська Комісія виступила зі стратегією **«Вивільнення потенціалу хмарних обчислень в Європі»** ("Unleashing the potential of cloud computing in Europe"), що спрямована на прискорення імплементації та значне розширення використання хмар в економіці ЄС. Спеціальну увагу у Стратегії приділено питанням безпеки користувачів і, зокрема захисту персональних даних.

14. На даний момент означені законодавчі пропозиції Єврокомісії оцінюються як найбільш складні проекти, які коли-небудь розроблялись та опрацьовувались в рамках ЄС Водночас, немає сумніву, що **ці дискусії і робота в євроінституціях визначать передові світові стандарти захисту персональних даних**.

III

15. Маємо розуміти, що створення дієвої, гармонізованої з європейським законодавством вітчизняної системи захисту персональних даних є одним з факторів подальшої успішності інтеграції України в ЄС.

16. Системна робота над створенням національних наглядових інституцій та законодавства у сфері захисту ПД триває в Україні лише з 2010 року.[*] **Україна взяла на себе зобов'язання адаптувати національне законодавство та систему захисту персональних даних до** положень відповідних правових актів та стандартів ЄС, наблизивши його таким чином до європейських стандартів. Загалом за цей час **Україні в цілому вдалося сформувати сучасну, адекватну європейським стандартам нормативно-правову базу для подальшого формування вітчизняної системи захисту ПД, а профільні державні структури проводять масштабну міжнародну співпрацю з цих питань.**

17. 14 травня поточного року Верховною Радою України було прийнято *«Проект Закону про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних»* № 2836 від 17.04.2013, яким передбачений цілий ряд змін у законодавстві в контексті модернізації галузевої нормативно-правової бази і серед іншого **Уповноваженого Верховної Ради України з прав людини визначено уповноваженим органом у сфері захисту персональних даних**.

18. Разом з цим, на сьогодні закладені лише основи вітчизняного профільного законодавства. Потрібна подальша робота з його **систематизації, розробки підзаконних актів, відповідних національних стандартів, чіткого визначення термінів, понять та категорій**. Безумовно, Україні також належить уважно слідкувати за відповідним законотворчим процесом в ЄС, проте, **питання остаточної транспозиції нових європейських підходів у національне законодавство України доцільно було б опрацювати після його результативного завершення**.

19. Разом з цим, треба пам’ятати, що як саме поняття «персональні дані», так і правові практики, пов’язані з їх захистом та обробкою, є відносно новими, а отже, малознайомими для українського суспільства.

[*] Насправді, першу редакцію Закону України «Про захист персональних даних» було прийнято 9 січня 2007 року, однак уже 30 січня 2007 року Президент України наклав вето на цей акт. 22 лютого 2007 року була прийнята Постанова Верховної Ради України про доопрацювання Закону України «Про захист персональних даних». Редакція Закону, що згодом стала основою українського профільного законодавства за № 2297-VI була вперше подана на розгляд ВР України 1 червня 2010 року (див.: http://zakon4.rada.gov.ua/laws/card/2297-17).

Пересічні українці демонструють байдужість до них і **недостатній рівень розуміння значення захисту персональних даних в сучасному світі, надто ж – в мережі Інтернет**.

20. З огляду на те, що в Україні високими темпами впроваджуються сучасні ІТ технології та проникає мережа Інтернет, то відповідно актуалізуються і весь комплекс *проблем захисту ПД «у віртуалі»*. ***Для успішного протистояння викликам у цій сфері Україна потребує щонайменше: а) адекватного правового забезпечення та ефективної національної системи регулювання та нагляду; б) розвиненого й диверсифікованого ринку юридичних послуг; в) грамотних і відповідальних контрагентів – провайдерів онлайн-послуг та їх споживачів, володільців персональних даних та їх розпорядників. З цих трьох мінімально необхідних складових – впевнено поки що можна говорити лише про досить успішне формування першої.***