

УДК 339.1:342.721:681.302

**В. БРИЖКО**, кандидат юридичних наук, старший науковий співробітник  
**М. ШВЕЦЬ**, доктор економічних наук, професор  
член-кореспондент АПрН України

## ДО ПИТАННЯ Е-ТОРГІВЛІ ТА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

*Анотація.* Щодо захисту прав та свобод за умов розвитку е-торгівлі.

У 1886 році шовкоторговець Л'юїс Тепен із Нью-Йорка створив агентство збору та аналізу інформації про кредитоспроможність підприємців, які зверталися до нього за позицією. Накопичивши декілька томів кредитних звітів, він став продавати інформацію. Клієнти платили від 100 до 200 дол. на рік [1]. Так з'явилися перша паперова картотека персональних даних та комерційне поширення відомостей із неї.

Завдяки появі електронно-інформаційного середовища виникла так звана “електронна економіка” або скорочено – “е-економіка”, частинами якої є е-торгівля та е-бізнес [2]. Торговельна діяльність використовує різні бази даних інформаційних ресурсів та все активніше застосовує сучасні телекомунікації для збору персональних даних за допомогою, зокрема, інтерфейсу під назвою Інтернет. Це надає значні переваги у вирішенні особистих чи корпоративних економічних та соціальних проблем і, одночасно, створює нові загрози приватності.

В Україні до теми “економіка – персональні дані” ставлення поблажливо-легковажне, навіть з точки зору інтересів її фіскальної політики та поповнювання бюджету. З 1992 р., незважаючи на наявність у Законі України “Про інформацію” правової норми про обов'язкову реєстрацію баз персональних даних, ця норма на практиці не реалізована взагалі. Частиною п'ятою статті 31 Закону України “Про інформацію” встановлено: “Всі організації, які збирають інформацію про громадян, повинні до початку роботи з нею здійснити у встановленому Кабінетом Міністрів України порядку державну реєстрацію відповідних баз даних”. Головне полягає у тому, що аналогічна норма є важливою складовою національних законодавств країн світу та європейських стандартів у сфері захисту даних [3], а реєстрація в Україні баз персональних даних понад 14 років не має заповнення. Пам'ятаючи зазначене, почнемо із сучасних уявлень про е-торгівлю.

### Щодо сучасних уявлень про е-економіку

Звичайно *е-торгівлю* можна розглядати як створення *е-магазинів* (Інтернет-магазинів) для здійснення продажу/купівлі товарів, надання послуг і проведення розрахунків за допомогою засобів інформаційних технологій та мереж. Якщо е-торгівля здійснюється одночасно з маркетингом (дослідження кон'юнктури, вибір ринків, розробка та просування товарів або послуг від виробника до споживача, зокрема, методами реклами й інших видів формування потреби в товарі, вироблення цінової політики тощо), то це вже називається е-бізнесом. Іншими словами, *е-бізнес* – це організація ведення традиційного бізнесу, що здійснюється з використанням сучасних інформаційних технологій і електронних засобів комунікаційного забезпечення (укладення угод, проведення платежів, участь в управлінні доставкою товару, штрихове кодування товарів, облік покупців, застосування дисконтних карток та е-карток розрахунку).

Звернемо увагу на два важливих і загальних аспекти е-економіки.

*Перший.* Світовий досвід свідчить, е-бізнес – це не стільки е-магазин (або веб-магазин), а, скоріше, спосіб мислення менеджера нового покоління, втілений у інформаційній інфраструктурі, що динамічно розвивається і призначена, у принципі, для економії часу і ресурсів.

*Другий.* Забезпечення захисту персональних даних користувачів Інтернет, і непомітний, але інтенсивний збір даних, що ідентифікуються з конкретною особою, дві серйозно конфліктуючі одна з одною проблеми. Конфлікт цей швидко стає однією з найбільш “гарячих” тем як у

зв'язку з розвитком е-бізнесу, так і в більш специфічній області, делікатно іменованій “забезпечення належної роботи правоохоронних органів”. Правозахисники вбачають у цих прагненнях замах на фундаментальні права людини, оскільки в переважній більшості випадків персональні дані збираються без їх згоди.

Сьогодні мережа Інтернет надає можливість застосовувати різні моделі (модулі) ведення е-бізнесу. Найбільше поширення зараз мають бізнес з клієнтом (business-to-consumers, або – B2C) і бізнес на базі між фірмових угод (business-to-business або – B2B).

1. **Бізнес-модуль B2C** (“бізнес-клієнт”; *Інтернет-торгівля*). Передбачає здійснення он-лайнного продажу товарів і надання послуг приватним особам (клієнтам) через мережу Інтернет. По суті, це схема діяльності звичайного роздрібного торговельного підприємства і надання банківських послуг із застосуванням новітніх інформаційних технологій і телекомунікаційних мереж.

Принципова схема роботи модуля B2C така: через мережу Інтернет покупець за допомогою браузера заходить на веб-сайт е-магазину. Веб-сайт містить е-вітрину, на якій розміщений каталог товарів і послуг (з можливістю пошуку) та необхідні інтерфейсні елементи для введення реєстраційної інформації, формування замовлення, проведення платежів через Інтернет, оформлення доставки, одержання інформації про компанії та он-лайнної консультації. Після закінчення формування замовлення і реєстрації вся зібрана інформація про покупця надходить з е-вітрини до торговельної системи е-магазину. У торговельній системі здійснюється перевірка наявності вибраного товару на складі, ініціюється запит до платіжної системи. Після повідомлення про проведення платежу торговельною системою формується замовлення для служби доставки.

Головна перевага B2C – веб-сайт фірми (е-магазину) може одночасно відвідати значна кількість покупців. Жоден реальний магазин не може витримувати одночасного напливу тисяч людей. Плюс до цього – потенційна можливість скорочення витрат на оренду приміщення, кількість персоналу, можливість представлення великої номенклатури товарів і послуг.

У бізнес-моделі B2C розрізняють два напрями: “виробник-клієнт” і “магазин-клієнт”.

Поки що у світі існує незначне число бізнесів щодо схеми “виробник-клієнт”. Основні труднощі в реалізації подібного підходу полягають у можливості прямої взаємодії підприємств. Зараз на цьому сегменті ринку B2C головним чином представлені компанії, що використовують ручну працю. Товари, що пропонуються, досить дорогі, а кількість обчислюється десятками (наприклад, автомобілі ручної зборки, штучні ювелірні вироби і т. п.). Однак останні тенденції в сучасній економіці передвіщають найбільшу перспективу розвитку саме цій формі B2C.

Сьогодні на Заході нема віртуальних, приміром, продовольчих магазинів, не прив'язаних до реальних магазинів. Звичайно е-магазин пропонує собою додатковий сервіс. За допомогою Інтернет добре торгувати не їжею, а скажімо, автомобілями, коли вартість угоди виправдовується вартістю однієї транзакції. Є і проблема психологічна – звичка людей витратити гроші в реальних, а не віртуальних магазинах, а також інші труднощі становлення е-бізнесу, про які йтиметься далі.

2. **Бізнес-модуль B2B** (“бізнес-бізнес”). Це сектор ринку міжфірмового е-бізнесу який на думку закордонних фахівців, вважається привабливим і перспективним. Саме на цей сектор й орієнтована робота щодо розробки нових програмних продуктів. Його головною тенденцією стає розробка багатофункціональних бізнес-додатків з єдиним веб-інтерфейсом. Справжня революція у використанні веб-технологій наступить тільки тоді, коли мережа буде тісно інтегрована з бізнес-процесами, невід'ємною частиною яких є маркетинг.

Відомо, що комп'ютери складаються з апаратури і програмного забезпечення. Їх поєднують мережі. Однак часто при створенні і розвитку інформаційної системи в організаціях, фірмах не звертають уваги на ще одну складову – людей, які усією цією технікою і технологією будуть користуватися. Так званий людський фактор – це програми, що закладені не в комп'ютери, а в голови людей, які користуються комп'ютерами. В інформаційних системах використовується лише малий відсоток їх можливостей, оскільки в організаціях нерідко зберігається старий, звичний обіг інформації. Багато операцій, що могли б виконуватися автоматично, продовжують робити вручну, у роботі з'являються дублювання, помилки, затримки.

Причина недоліків проста. Інформаційною системою є не комп'ютерна підсистема організації, а вся організація в цілому. І тому програмуватися, настроюватися і налагоджуватися вона повинна у всіх своїх частинах. Відомо, що для організації, де є десяток комп'ютерів, потрібний системний адміністратор, відповідальний за їх інформаційну взаємодію. Але поки ще доводиться констатувати недостатню увагу до пропозиції про введення в штат фахівця, який відповідає за інформаційну взаємодію користувачів між собою. Менеджери нерідко вважають, що підлеглим досить вказівок про те, що треба зробити. Тим часом, у високотехнологічному інформаційному середовищі такі вказівки часом виконуються за допомогою процедур, на які витрачається купа часу і нервів. Адже виконавці далеко не завжди можуть самі розробити, а тим більше впровадити правильну систему інформаційної взаємодії – вони просто не фахівці в цьому, та й повноважень відповідних у них нема. Зазначене, що одержало назву *реінжиніринг* організацій, відносно нова інформаційна технологія на стику техніки і менеджменту. З усіх наявних технологій вона є найменш відомою.

3. **Бізнес-модулі G2B** (“уряд-бізнес”) і **G2C** (“уряд-громадяни”). Ці моделі тісно пов'язані з е-бізнесом та знаходяться в стадії апробації.

**Модуль G2B** охоплює зв'язки між приватними компаніями й урядовими організаціями. Це стосується так званих *електронних тендерів* (е-тендерів), призначених для більш дешевого та прозорого адміністрування державних закупівель, тобто зменшення корупції у стосунках бізнесу та влади. Ідея е-тендерів була розроблена у травні 1994 р. комісією ЄС під керівництвом Комісара із захисту даних М.Бангемана. Державам-членам Євросоюзу пропонувалося прийняти загальні стандарти із обробки даних при проведенні е-торгів та відзначалася необхідність створення умов безпеки щодо перетворення е-тендерів у сховану форму протекціонізму.

Сьогодні у США плани урядових закупівель не є секретами й анонсуються засобами Інтернет. Компанії можуть відповісти на пропозиції знову-таки через Інтернет. Вільне поширення інформації про обсяги і хід тендерних закупівель за допомогою Інтернет розглядається не тільки як метод підвищення конкурентоспроможності, але й як засіб боротьби з корупцією при проведенні державних тендерів. Проте контури модуля “уряд-бізнес” остаточно так і не окреслені.

**Модуль G2C** (“уряд-громадяни”) розглядається як засіб інформування та відповіді на запитання населення. Крім цього, активно досліджуються питання е-голосування за допомогою телекомунікаційних засобів та засобів зв'язку.

4. **Бізнес-модуль E2E** (е-біржа). Черговим етапом розвитку е-бізнесу очікується інтеграція он-лайнних бірж. Ця модель ще тільки має відбутися, тому що багато підприємств не можуть вирішити для себе, зокрема, брати їм участь у роботі однієї біржі або одержати єдиний доступ до багатьох бірж відразу. Вже випускається відповідний програмний продукт компанії Ironside Technologies. З його допомогою на восьми е-біржах одночасно розміщено каталоги пропозицій. Незважаючи на щомісячну плату в 1000 дол. за кожну біржу (плюс комісії за транзакції), вважається можливим знизити витрати на бізнес шляхом виходу на нові ринки збуту.

5. **Використання засобів мобільного зв'язку**. Існує багато засобів мобільного зв'язку для забезпечення бізнесу. От деякі з них.

*Мобільна комерція (м-комерція)* – це використання мініатюрних (кишенькових) переносних пристроїв для комунікаційного мобільного зв'язку з приватними і державними мережами. Є й інше визначення – використання персоніфікованих пристроїв бездротової стільникової комунікації й одержання послуг за допомогою високошвидкісного доступу до Інтернет.

В економічній діяльності поняття “м-комерція” відносять до будь-якої фінансової транзакції, що здійснюється через мобільні телекомунікаційні мережі. Під *транзакцією* розуміють сукупність операцій над даними, що, з огляду на їх обробку, є елементарною і характеризується логічною завершеністю, тобто виконуються повністю або не виконуються зовсім.

У поняття мобільного зв'язку входить також пейджинговий і транковий зв'язок.

*Пейджинг* (мініатюрний радіоприймальний пристрій) забезпечує однібічний мобільний зв'язок шляхом прийому власником пейджерів буквено-цифрових або цифрових повідомлень від абонента телефонної мережі загального користування.

*Транковий зв'язок* – це система багатоканального радіозв'язку для використання різними суб'єктами, яким необхідний надійний двосторонній зв'язок між мобільними абонентами, наприклад, міліції, швидкій допомозі, пожежній охороні, великим приватним організаціям. Основна задача транкового зв'язку – забезпечення надійним зв'язком на території міста і прилеглих районів. У транкових радіотелефонів значно більше можливостей, ніж м-телефонів і пейджерів. Він працює на відстані до 50 км від бази, а між собою їх власники можуть спілкуватися на відстані 100 км одне від одного.

Найскладнішими для реалізації ідеї м-зв'язку були визначення поточного місця перебування абонента, що рухається, і підтримка безперервності зв'язку при його переміщенні з одного “стільника” до іншого. *Забезпечення зв'язку з абонентом, що рухається і знаходиться за межами своєї зони обслуговування, називають роумінгом.* Роумінг забезпечується завдяки наявності двох спеціальних реєстрів. Перший – це довідкова база даних, що містить відомості про зареєстрованих абонентів і мобільні станції. Іншим пристроєм, що допомагає відслідковувати переміщення мобільних станцій, є реєстр переміщення. Він реєструє мобільні станції в чужих зонах і вказує їх місцезнаходження при здійсненні виклику. Роумінг дозволяє з'єднувати абонентів між собою в межах однієї мережі і може бути регіональним, національним або міжнародним.

У даний час з'явився конгломерат телефону і комп'ютера, тобто мобільний комунікатор.

*Мобільний комунікатор* – це персональний багатофункціональний засіб телекомунікації, що має функціональні можливості комп'ютера, завантаження програм із традиційного персонального комп'ютера, а також може здійснювати е-документообіг у разі підключення за інших пристроїв за допомогою будь-якого роду радіо, провідних, оптичних або інших електромагнітних технологій і систем. До подібних можна віднести поки дорогі в ціновому відношенні мініатюрні засоби, що мають сучасний дизайн, наприклад, фірми Siemens, Nokia, Motorola. Такий м-телефон має те, що є у звичайного персонального комп'ютера – процесор, постійну й оперативну пам'ять, вбудовані в один чіп, а також текстовий редактор.

Оскільки смарт-карта в стільниковому телефоні вже є, а бездротові технології в ньому закладені, для виконання функції е-гаманця або е-портмоне з документами необхідно розв'язати проблеми щодо запровадження єдиного стандарту на передачу даних, створення ефективного захисту від підробок, кіберзлочинних атак і несанкціонованого використання персональних даних.

*PDA – особисті цифрові помічники.* Вони з'єднуються з Інтернет через бездротові модеми або синхронізуються з персональним комп'ютером, підключеним до Інтернет. Значна частина сервіс-послуг PDA заснована на технологіях визначення місця розташування та відстеження переміщення товарів від фабрики до споживача.

**Щодо загальних перспектив е-економіки,** то їх пов'язують, насамперед, з апаратною мінімізацією і збільшенням багатофункціональності засобів зв'язку. Оскільки це молода область діяльності, то у її становленні та розвитку існують проблеми. Відповідної уваги потребують:

- *політична сфера* – активність у формуванні політики щодо е-бізнесу за умов узгодженості національного законодавства із відповідними європейськими стандартами;

- *правова сфера:*

- створення єдиних правил ведення е-бізнесу, що передбачає, зокрема, активність у запровадженні е-підпису та е-документообігу;

- однозначність у вирішенні питань власності на інформаційні ресурси, прав провайдерів і виробників інформаційних продуктів та надання послуг за допомогою технологій та мереж;

- створення механізму захисту персональних даних та забезпечення безпеки транзакцій;

- *психологічні проблеми* - важкість для споживача визначитися з покупкою, не потримавши товар в руках, та складнощі, які виникають при поверненні неякісного товару.

## Про захист персональних даних у контексті е-торгівлі

Тема законодавчого захисту персональних даних – нова і, водночас, одна з проблем, що понад 10 років не може одержати в Україні нормативно-правового й організаційного вирішення.

Виходячи з європейських і світових уявлень про права і свободи журналісти борються за свободу слова. Віруючі – відстоюють свободу віросповідання і проти заміни імені людей на ідентифікаційний номер. Мусульмани – заперечують будь-якому втручання в тіло людини (біометрія, чіпи). Іудеї – проти того, щоб рахували євреїв. Підприємці – проти того, щоб інформація про їх і їхню діяльність (угоди, доходи, нерухомість, автомобілі, їхні діти) потрапляли до рук злочинців. Пенсіонери – відстоюють свої соціальні права, зокрема, від бандитів, які внаслідок “наведень” з безліч існуючих баз персональних даних (приклад див. [6]) споюють власників житла та приватизують їхні квартири, майно тощо. Правозахисники – відстоюють права ув'язнених та стурбовані сексуальною ліберальністю.

При всьому цьому усі ми не дуже пам'ятаємо про те, що всі наші бажання, спрямування і дії мають тісний зв'язок із відомостями персонального змісту, тобто – персональними даними. Приміром, навряд чи хто в захваті від розголошення його паспортних даних, бізнес-відносин та звичок, кола знайомих, маршрутів подорожей, а також стану сімейних відносин, особистих медичних відомостей тощо. Інакше кажучи, все і вся пронизано персональними даними конкретних людей. Немає такої області життєдіяльності людини, суспільства і держави, яка не мала б взаємного зв'язку (навіть кореляції) з персональними даними.

Природно, що там, де “пахне” грошима, відразу виникає й активно розвивається відповідна комерція та злочинність. Збір, збереження і продаж персональних даних – звичайно не виняток. Раніше персональні дані накопичувалися в картотеках і державних реєстрах. Тепер вони активно обробляються в комп'ютерах у приватних і комерційних інтересах. Роблячи покупки в е-магазинах або отримуючи дисконтні картки, споживач змушений повідомляти свої персональні дані. Власники зазначених підприємств, з одного боку, зацікавлені у відомостях про стан попиту на ринку, який може бути оцінений завдяки відомостям про покупців та потенційних споживачів їх продукції, а з іншого – не завжди забезпечують захист персональних даних людини, навіть можуть збирати та пропонувати зазначені дані для продажу й отримання іншого виду прибутку, без диверсифікації щодо номенклатури продукції. Останнє в умовах ринку – значний важіль у конкурентній боротьбі, гарант від розорення при змінах кон'юнктури.

Сьогодні ті, хто займається маркетингом, постійно вишукують нові, ефективні шляхи для збору будь-яких відомостей про своїх конкурентів та потенційних покупців: їх діяльність, оточення, стосунки, погляди, інтереси, характер, поведінка та багато ін. Для бізнесу персональні дані – зручне, а тепер і необхідне доповнення із усього того, що надає Інтернет або інші мережі. Уже цілком чітко усвідомлено, що з допомогою засобів е-середовища набагато легше збирати величезні обсяги різної інформації, а аналіз і взаємне ув'язування відомостей забезпечують істотні прибутки і лідерство в бізнесі. Критерії, відповідно до яких відомості про людину включаються до списку, призначеного для маркетингових заходів, очевидні. Так, дані про людину, що має моторний човен, вносять до списку власників моторних човнів саме тому, що вона володіє човном, дані щодо машини – до списку її відповідної моделі... В основу прямого маркетингу покладене створення списків людей, поєднаних загальними демографічними даними. І для цих цілей зовсім не потрібна конфіденційна інформація. Головне, щоб її було якомога більше.

Більш того, процес отримання персональних даних перетворюється на окремий бізнес, метою якого є тільки збір, обробка та поширення персональних даних на комерційних засадах. Відомості про людину, її матеріальний стан, особисте життя “відбираються” з БД та реалізуються на дисках або розміщуються у Інтернет. Коштує така БД від 10 (дрібний продаж) – до 1500 (продаж через Інтернет) дол. Інформація мобільного зв'язку потрапляє на чорний ринок (номер коштує 50 дол., прослуховування – 150 дол. на год.), і ніхто за це не відповідає. Кримінал продовжує “напрацьовувати” досвід отримання прибутку та політичних дивідендів від втручання в особисте життя. За оцінками експертів, світовий ринок персональних даних досягає 3 млрд. дол. [7], у Росії – 20 - 24 млн. дол., а деякі з них вважають, що він становить 100 млн.

дол. на рік [8, 9]. Як повідомляється у [10], збиток, завданий британській економіці розкраданнями ідентифікаційних даних у 2006 р., склав 1,8 млрд. ф.ст., а у 2010 року ця цифра може досягти 3,8 млрд. ф.ст. завдяки суттєвому зросту структури злочинності у е-середовищі.

З іншого боку, конституційні норми фактично не діють, так як немає правових засад – юридично власника бази персональних даних не існує, закону про службову таємницю немає, а державної таємниці персональні дані звичайно не містять. Наявність у Конституції гарантії недоторканності особистого життя та принцип прямої дії норм Конституції правоохоронні органи вважають недостатніми для заведення справи – немає предмета справи. Механізмів захисту персональних даних, вироблених світовою історією і практикою, у країні немає. Фіскальна політика держави, по суті, ігнорує податкову діяльність у сфері персональних даних. Хоча ясно, що засобами податкової і соціальної політики держава зобов'язана протистояти розшаруванню членів суспільства за рівнем доходів, впроваджуючи в життя фундаментальні права людини і свободи.

Реальність така, що за відсутності відповідного механізму системи, що обробляють персональні дані, працюють і заробляють, як і скільки хочуть, як їм потрібно, а не так, як краще для тих, чий дані обробляються. Від такої комерції бюджет держави взагалі нічого не одержує. І все це на тлі ілюзорності правового захисту персональної даних, неподобства якого покривають заяви типу: *Порядній людині нема чого скривати. Щоб боротися з тероризмом, треба відмовитися від захисту приватного життя.*

Після подій у Нью-Йорку 11.09.2001 р. спостерігається наступна ситуація:

- у рамках антитерористичної кампанії Європейський парламент 30.05.2002 р. скасував положення Директиви 97/66/ЄС від 15.12.1997 р. “Про обробку персональних даних і захист прав осіб у телекомунікаційному секторі”, що обмежують збереження персональних даних користувачів Інтернет. У листопаді 2003 р. Європейський суд постановив: *“згадування конкретних людей у розташованих на Інтернет-сайтах матеріалах, публікація їхніх імен чи будь-якої іншої конкретної інформації про них є операцією з персональними даними. Стосовно подібних дій повинна застосовуватися Директива 95/46/ЄС із захисту персональних даних”;*

- вводяться е-паспорти, у яких (завдяки чипам та антен) стає можливим відслідковувати (із супутника) будь-кого і будь-де;

- упроваджуються системи RFID-міток у вигляді підшкірних імплантатів – персональних ідентифікаторів (людей, товарів). Випускається новий вид гвинтівки, що вистрілює RFID-мітки і непомітно мітить людей. Правової регуляції щодо цього нема;

- обмежуються (у багатьох країнах) можливості самозахисту за допомогою криптографії. Вводиться обов'язковість надання “ключів” дешифрування відповідним службам;

- обмежується можливість анонімності при використанні засобів комунікації (якщо не можна ідентифікувати суб'єкта відправленої транзакції);

- активно використовуються системи відеоспостереження (розпізнавання осіб) в умовах відсутності зацікавленості урядів у прийнятті конкретних законів. Системи щодо порядку оповіщення громадян про спостереження, збереження записів і доступ до них нема.

Сучасні технології застосовуються для перегляду та аналізу змісту е-пошти під час відсутності будь-яких законодавчих обмежень. При цьому е-пошта і дані, що містяться у комп'ютері, така ж особиста недоторкана сфера, як і житло. Але міжнародні стандарти (приклад: Директива ЄС по телекомунікаціях) упроваджуються з великими зусиллями;

- активно ведуться генетичні дослідження. Тестування і створення поліцейських БД ДНК вже є реалією. Небезпека – можливість робити генні висновки про риси особи і складання характеристики. При цьому медичні дані дуже дорого коштують (щодо діагнозів захворювань, відомості про аналізи, запропоновані рецепти тощо, навіть про лікарів, що обслуговують);

- має місце широка практика об'єднання БД на основі ідентифікаційних номерів. Об'єднання податкової, медичної, соціальної інформації, відомостей про майно, родинний стан, особисті таємниці тощо дозволяє створити вичерпне дос'є (навіть негативне), доступне необмеженому колу осіб;

• практично боротьба зі “спамом”, “сокетом” (рекламні розсилання) і “троянським конем” (викачуванням інформації) має номінальний зміст. Продаж персональних даних за допомогою “спаму” – звичайна практика. За допомогою програм-шпигунів запитуються анкетні дані та створюються досє користувачів Інтернет.

### ***Щодо сучасного стану справ в Україні***

Фундаментальне право щодо захисту відомостей про осіб продовжує залишатися нереалізованим, не зважаючи на наявність у законодавстві низки відповідних норм. Їх сукупність має істотні недоліки, а саме:

- відсутня визначеність і погодженість понять у сфері захисту персональних даних;
- відсутня відповідність вітчизняного законодавства принципам європейських стандартів;
- немає організаційно-правової системи (механізму) захисту персональних даних.

Головний недолік сучасного стану захисту персональних даних в Україні полягає у відсутності базового закону України та чіткого і зрозумілого для усіх правового механізму забезпечення регуляції дій з персональними даними (див. [11 – 14]). Без цього немає правового захисту, тому що правове регулювання відносин – це регулювання дій з обробки даних.

### ***Щодо законопроекту у сфері захисту персональних даних***

*Призначення законопроекту:*

- забезпечення ратифікації Конвенції Ради Європи № 108 від 28.01.1981 р.;
- упорядкування інформаційних відносин у сфері захисту персональних даних згідно з принципами і нормами європейських стандартів на базі рамкового закону;
- створення механізму захисту персональних даних, в основі якого повинен бути пріоритет прав людини стосовно інтересів держави – тобто запровадження юридичної категорії “право власності людини на свої персональні дані” (усім відомо, що робота всіх організацій, установ, фірм тощо будується на використанні персональних даних громадян, порядок збору і використання яких не визначено).

*Основні організаційні складові механізму:* уповноважений орган із захисту даних і державний реєстр інформаційних систем обробки персональних даних. Державний реєстр зберігає основні дані про особу (ПІБ, стать, дата та місце народження). Всі інші дані повинні зберігатися в розподілених галузевих БД. Обробка даних і доступ до них мають бути обмежені згідно з базовим законом, норми якого повинні бути деталізовані у галузевих законах та підзаконних актах.

*Проект Закону України “Про захист персональних даних”.* Упродовж понад 10 років проект Закону України “Про захист персональних даних” (№ 2618) пройшов правову експертизу значної кількості юристів міністерств, комітетів (був офіційно узгоджений керівниками), народних депутатів України, громадських організацій. Безпосередньо його підтримали 18 докторів та 19 кандидатів наук. Враховано понад 600 зауважень та пропозицій. Головне науково-експертне управління Апарату Верховної Ради України надало щодо нього позитивний висновок. 16.03.2006 р. проект був прийнятий Верховною Радою України в цілому як Закон (“за” – 287, “проти” – немає, “утримались” – 1, “не голосувало” – 108 депутатів).

*Зауваження до проекту.* Має місце різне розуміння змісту категорій, зокрема, “конфіденційність”. На наш погляд, її слід розуміти як – *обмеження поширення особистої таємниці*. Проте статтею 30 Закону України “Про інформацію” встановлено: “*Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов*”. Тобто з точки зору “букви закону” відповідна правова формула чинного законодавства України однозначно визначає “конфіденційну інформацію” як *тріаду повноважень права власності*. Це передбачає наявність права власності людини на свої персональні дані.

Але заперечення у можливості запровадження в законодавстві України категорії “право власності людини на свої персональні дані” продовжує мати місце. Стверджується, що “*персональні дані – це особисті немайнові права*”, тобто вони не мають економічного змісту.

“Право”, “закон”, “кодекс” – різні за гносеологією поняття. “Право” існує об’єктивно, не зникає та не передається (за депутатом англійського парламенту 1688 р. І.Ньютоном – воно від Бога; за сучасними науковими уявленнями – воно від енергоінформаційної субстанції Всесвіту, тобто – від Природи). Згідно із соціально-економічною формацією держава визначає види “права” та запроваджує їх у Конституцію у вигляді норм права. Виникає суб’єктивне право. На його базі створюються закони, які правовими нормами визначають сферу (головна мета закону – обмеження) суспільних відносин.

Цивільний кодекс України (та будь-якій іншій збірник норм) визначає однорідну сферу суспільних відносин. Кодекс спирається та визначає **“право”**, що передбачає формулювання відповідних декларацій та загальну правову регламентацію. **“Особисті немайнові права”** [15] (до речі, у Конституції це поняття, як й поняття “персональні дані”, не вживаються) – це **“права”**, а не **“норми”** правового регулювання. Норми правового регулювання (правові формули) визначаються законом, у якому є завжди **об’єкт права**. Згідно зі статтею 8 Закону України “Про інформацію” таким об’єктом є “інформація”. А згідно зі статтею 38 того ж закону “інформація” може бути об’єктом права власності. Тобто **не можна ототожнювати** поняття **“право”** (право на життя, на свободу, на власність, на недоторканність, на охорону здоров’я...), яке **не має економічного змісту** (тобто – не має грошової оцінки та можливості включення у господарський обіг), з поняттям **“об’єкт права”** (інформація, відомості, персональні дані, інформаційні ресурси), що **має економічний зміст, може мати грошову оцінку та можливість включення у господарський обіг**. Тому персональні дані людини у визначених законом межах можуть бути об’єктом права власності.

Зауважимо, що система права (суспільних відносин теж) є динамічною, вона постійно змінюється, розвивається. Так з ЦКУ виділились та відокремились у самостійні сфери відносин такі галузі, як господарське, житлове право тощо. Виникло екологічне, атомне, космічне право. На черзі – **Інформаційне право**, яке повинно визначити суспільні відносини щодо “інформації”, “відомостей”, “даних”, “інформаційних ресурсів”, “охорони, захисту, безпеки даних”, ЗМІ, “інтелектуальної власності”, “системної інформатизації” тощо. Перші кроки зроблені. Постановою Президії вищої атестаційної комісії України від 21.05.03 р. № 26-11/5 затверджено паспорт нової спеціальності 12.00.07 – теорія управління; адміністративне право і процес; фінансове право; інформаційне право (юридичні науки). Є спроби здійснити кодифікацію інформаційного законодавства.

Звернемо увагу також на міжнародне та національне законодавство про авторські права. Правове упорядкування відносин у цій сфері передбачає наявність механізму підтримки прав автора на ім’я, на неперекручення тексту тощо та механізму підтримки права на використання об’єкта інтелектуальної власності, що дозволяє юридично вводити його в господарський обіг. Тобто одночасно співіснують та співпрацюють два інститути права – на ім’я та на використання.

Незважаючи на зазначене вище, Президенту України були надані чергові зауваження до закону і 11 квітня 2006 року він повернув його до Верховної Ради України на доопрацювання.

На усі зауваження нами були надані детально аргументовані пояснення та пропонувалося:

1. *Подолати вето Президента України на Закон України “Про захист персональних даних”, який був прийнятий Верховною Радою України в цілому 16 березня 2006 року.*

2. *Зобов’язати Кабінет Міністрів України забезпечити створення умов для запровадження в Україні єдиного правового механізму захисту персональних даних, основною частиною якого є Уповноважений орган із захисту даних в Україні.*

З метою оцінки пояснень та пропозицій було створено робочу групу.

Але ніякої оцінки пояснень не було. Було “програмування” у напрямку – *мови про право власності людини на свої персональні дані не має; персональні дані відносяться до “особистих немайнових прав”*.

У наступному нами було запропоновано (у письмовій формі) внести до тексту закону зміни, які пов’язані із **розмежуванням** поняття **“суб’єкт персональних даних”** на дві категорії



тобто: там, де в законі мова йде про людину (носія природних прав), використовувати поняття “власник персональних даних”, там, де це стосується громадянина (носія конституційних прав), так і зазначати –“громадянин-суб’єкт персональних даних”. З цією метою рекомендувалось текст закону почати з Преамбули, що надається, а також внести зміни до формулювання поняття “суб’єкт персональних даних” у такій редакції:

### Закон України

#### “ПРО ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ”

*Верховна Рада України, керуючись Актом проголошення незалежності України (від 24 серпня 1991 року), виходячи з положень Конституції України (від 28 червня 1996 року), Загальної декларації прав людини (від 10 грудня 1948 року), Європейської Конвенції з прав людини (від 4 грудня 1950 року), Європейської Конвенції про захист осіб у зв’язку з автоматизованою обробкою персональних даних (від 28 січня 1981 року);*

*вважаючи, що слід забезпечити права людини та основоположні свободи громадянина в частині захисту персональних даних в умовах розвитку інформаційно-комп’ютерних технологій та телекомунікаційних мереж згідно з принципами європейського права;*

*прагнучи підсилити рівень захисту природного права людини на свої персональні дані та, одночасно, виконання її конституційних обов’язків як громадянина перед суспільством і державою щодо забезпечення діяльності органів державної влади та органів місцевого самоврядування;*

*визнаючи необхідність поєднання захисту персональних даних зі свободою поширення інформації в суспільстві, за умов забезпечення балансу прав людини, суспільства і держави, утвердження суспільної злагоди і політичної стабільності, забезпечення єдності держави, української нації і зміцнення української державності;*

*прийняла цей Закон.*

.....  
Стаття 2. Визначення термінів  
.....

*суб’єкт персональних даних – людина (фізична особа), яка має право власності на персональні дані про себе (далі – власник персональних даних) та, одночасно є громадянином, або особою без громадянства, зобов’язаною сприяти діяльності органів державної влади та органів місцевого самоврядування щодо надання персональних даних згідно із чинним законодавством (далі за текстом Закону України від 16 травня 2006 р., прийнятого народними депутатами України в цілому).*

#### Деякі висновки

1. Питання щодо е-торгівлі та необхідності забезпечення захисту персональних даних є складовими частинами загальної соціально-політичної та економічної проблеми побудови інформаційного суспільства (див. Додаток). У правовій, соціальній державі ця проблема потребує уваги до двох взаємопов’язаних аспектів стосовно наявності механізму правового регулювання соціальних та економічних суспільних інформаційних відносин. Зазначене регулювання не можна обмежувати тільки нормами Конституції та окремими, не дуже пов’язаними між собою, статтями деяких законів. Необхідним є базовий закон держави у сфері захисту персональних даних. Його принципи повинні бути деталізовані в законодавстві по галузях господарства (зокрема, щодо е-комерції). Складова економічного аспекту має бути спрямована в інтересах розвитку соціальної (духовної) складової суспільства і держави.

2. Узагальнюючи стан захисту персональних даних у контексті е-торгівлі, можна помітити, що між ними існує протиріччя, обумовлене пріоритетністю вирішення питань економіки та вторинною роллю захисту даних та знань. Сучасні інформаційно-комп’ютерні засоби використання інформаційних ресурсів ускладнили це протиріччя, так як правові норми реального простору не завжди здатні врегулювати суспільні відносини в подібному на лабіринт е-середовищі.

Однією з пріоритетних у вирішенні є проблема стягнення податків у зв'язку із створенням та використанням баз персональних даних. Метою цього є забезпечення поповнення бюджету та упорядкування інформаційних відносин згідно з принципами та нормами європейських стандартів.

3. Через те, що законодавство відстає від розвитку інформаційних технологій, а корпоративні засоби захисту персональних даних не завжди відповідають принципам європейських стандартів, захист прав людини у сфері персональних даних вимагає визначення повноважень із нагляду за діяльністю різних суб'єктів Уповноваженим із захисту персональних даних в Україні, незалежним від владних структур (хоча це досить проблематично). Його функціональне призначення має служити головної меті – створенню максимальних умов недоторканності приватного життя з урахуванням державних і суспільних інтересів щодо розвитку економіки.

Додаток

Механізм правового регулювання щодо <b>СОЦІАЛЬНОГО АСПЕКТУ:</b> <i>права людини та захист даних</i>	Механізм правового регулювання щодо <b>ЕКОНОМІЧНОГО АСПЕКТУ:</b> <i>е-бізнес та безпека даних</i>
<p><b>е-демократія G2D</b> (“уряд-демократія”): універсальний портал е-обслуговування громадян.</p> <p><i>Мета</i> – надання громадянам публічної інформації про діяльність органів влади, можливості обговорення питань управління та розвитку суспільства і держави. Портал створюють згідно з тематичною спрямованістю, потім – щодо належності до відомства.</p> <p><b>е-голосування щодо G2D</b>: запровадження он-лайнного голосування. Існують три негативні причини: корупція, кіберзлочинність, слабкість інфраструктури всесвітньої мережі.</p> <p><i>Спеціальне нормативно-правове забезпечення</i> – захист персональних даних, права власності на інформаційні ресурси, технології, авторські та патентні права.</p>	<p><b>е-уряд G2C</b> (“уряд-громадяни”): модуль інформаційних послуг е-обслуговування громадян: відповіді на запитання, скарги, заповнення форм (щодо податків, розрахунків, сплати мита тощо).</p> <p><i>Мета</i> – відкриття для громадян закритих структур шляхом виходу на веб-сторінки через їх портали.</p> <p><i>Спеціальне нормативно-правове забезпечення</i> щодо: е-документообігу; е-підпису.</p> <p><b>е-уряд G2B</b> (“уряд-бізнес”): е-обслуговування бізнесу</p> <p><i>Мета</i> – проведення е-тендерів, прискорення бізнесу шляхом спрощення оформлення ліцензій, кредитів тощо.</p> <p><i>Спеціальне нормативно-правове забезпечення</i> щодо: е-документообігу; е-підпису, е-тендерів.</p> <p><b>е-уряд G2G</b> (“уряд-уряд”): модуль е-обслуговування органів державної влади та органів місцевого самоврядування.</p> <p><i>Мета</i> – оперативне вирішення питань, спрощення діловодства та забезпечення інформаційної безпеки.</p> <p><i>Спеціальне нормативно-правове забезпечення</i> щодо: е-документообігу; е-підпису.</p>
<p><b>Бізнес-модулі інформаційного суспільства:</b>  <b>B2B</b> – сервіс “бізнес-бізнес”; <b>B2C</b> – сервіс “бізнес-клієнт”; <b>C2B</b> – сервіс “клієнт-бізнес”</p>	
<p><b>Загальне нормативно-правове забезпечення щодо:</b></p>	
<ul style="list-style-type: none"> <li>• <b>е-управління;</b></li> <li>• <b>е-медицини;</b></li> <li>• <b>е-освіти;</b></li> <li>• <b>е-бібліотек;</b></li> <li>• <b>е-консалтингу</b></li> </ul>	<ul style="list-style-type: none"> <li>- розвиток інформаційних ресурсів, продуктів, технологій та інформаційних послуг;</li> <li>- розвиток українського сегмента мережі Інтернет;</li> <li>- правове упорядкування діяльності суб'єктів ринку інформаційних ресурсів, продуктів, технологій та інформаційних послуг;</li> <li>- міжнародний інформаційний обмін на базі європейських стандартів.</li> </ul>
<ul style="list-style-type: none"> <li>• <b>моніторингу та контролю</b> стану інформаційної безпеки та захисту персональних даних – щодо мереж передачі даних, обмеження поширення у телекомунікаціях протиправної та аморальної інформації;</li> <li>• <b>моніторингу</b> ринку інформаційних ресурсів, продуктів, технологій та інформаційних послуг у зв'язку із захистом та безпекою даних.</li> </ul>	

4. На виконання європейських принципів захисту персональних даних деякі бізнес-організації роблять спроби вирішити проблеми самостійно, наприклад, застосовують корпоративні кодекси поведінки. Один із важливіших з принципів захисту – персональні дані ні за яких умов не повинні потрапляти (розміщатися) у загальнодоступних інформаційних ресурсах (базах

даних). Тобто не можна поєднувати загальні БД і БД персональних даних. Саме звідси випливають ідея організаційного розмежування діяльності з інформацією і поява окремих посад щодо її кураторства в державах-членах Ради Європи та Європейського Союзу (Комісар РЄ та Європейський наглядач ЄС із захисту даних). Однак практика свідчить, що порушення загальних принципів продовжує мати місце. Правоохоронці стверджують – у зв'язку з поєднанням загальних інформаційних ресурсів та персональних даних в одній базі даних предмета порушення немає, тому й справу відкрити проблематично.

Щодо міжнародного бізнесу, то європейська модель захисту персональних даних встановлює обов'язкові для усіх держав-членів РЄ та ЄС дуже важливі рамкові умови щодо рівня доступу і можливості передачі (експорту) інформації. Експорт забороняється, якщо законодавчо не забезпечений визначений рівень її захисту. За необхідності між партнерами різних країн укладається договір, що передбачає, як треба діяти в тій чи іншій ситуації. Якщо цього не враховувати, то Європейський наглядач ЄС або Комісар РЄ із захисту даних можуть прийняти рішення про заборону передачі інформації з однієї держави до іншої.

5. Мережа Інтернет і захист персональних даних – один із сучасних аспектів протистояння інтересів держави та прав людини.

З одного боку, апарат держави бажає знати про людину якнайбільше. З іншого, Інтернет – це потоки даних, де мають місце розголошення таємниці приватного життя, комерційної таємниці, плагіат, шахрайство тощо. Закордонні компанії, незважаючи на закони про захист даних, активно здійснюють та будуть здійснювати маркетингові дослідження, які передбачають збирання і використання персональних даних споживачів і конкурентів, звичайно, без їх згоди.

Сьогодні немає ефективних методів відстеження діяльності в Інтернет. У разі активного введення е-грошей держава не в змозі надійно контролювати фінансові потоки. Проблематично, як і кому будуть справлятися податки, наприклад, у випадку, якщо громадянин України придбав товар за допомогою Інтернет в українському е-магазині, що працює через сервер, який знаходиться у Польщі, а контора, що відвантажує товар, – в Угорщині. Вважаємо, що це питання потребує вирішення на рівні Світової організації торгівлі (ГАТТ/СОТ), яке має враховувати європейські стандарти щодо принципів захисту прав людини у сфері персональних даних.

6. Про стан “упорядкування” відносин щодо права власності на інформацію у Цивільному Кодексі України [16].

Законодавець у ЦКУ надав визначення поняття інформації – “це документовані або публічно оголошені відомості про події та явища, що мали або мають місце у суспільстві, державі та навколишньому середовищі” (ст. 200). При цьому не визначено в якості якого предмету матеріального світу може бути представлена інформація. Використовуючи норми ЦКУ, неможливо логічно замкнути зв'язок: *інформація – річ – право майнової власності*. Таким чином, на перший погляд, відповідно до ЦКУ, інформація не може бути об'єктом права власності.

Але ЦКУ містить багато норм, які свідчать про протилежне.

У статті 303 ЦКУ зазначається, що “у власності фізичної особи можуть бути особисті папери (документи, фотографії, щоденники, інші записи, особисті архівні матеріали тощо)”, тобто – інформація про особу. Відповідно до статті 178 ЦКУ об'єкти цивільних прав, в тому числі й інформація, можуть вільно відчужуватися або переходити від однієї особи до іншої в порядку правонаступництва чи спадкування або іншим чином, якщо вони не вилучені з цивільного обігу. Законодавець у статті 969 ЦКУ визнає документи, як окрему форму інформації, в якості цінностей, які можуть бути передані до банку на зберігання.

Більш того, у статті 1010 ЦКУ до майна довірителя відносяться його документи. Відповідно до Глави 62 ЦКУ: “До результатів виконання науково-дослідних або дослідно-конструкторських та технологічних робіт, які має право використовувати замовник, відносяться наукові дослідження та конструкторська документація, в якості конкретних організаційних форм інформації”.

Підсумовуючи, можна стверджувати, що українське законодавство є досить суперечливим щодо визначення права власності на інформацію. Це суттєво гальмує процес введення інформації в цивільний обіг, перешкоджає можливості захисту прав суб'єктів інформаційних відносин.

Але ЦКУ надає принципову змогу виправити це негативне становище. Відповідно до статті 200 ЦКУ порядок використання інформації та захисту права на неї встановлюється законом. Тому, на нашу думку, доцільно ввести до інформаційного законодавства такі правові норми, які б надали змогу використовувати всі механізми цивільного права щодо введення інформації в цивільний обіг. Зміст цих правових норм потребує встановити наступне:

- інформація у певних організаційних формах має бути віднесена до об’єктів права власності;
- інформація у вигляді інформаційних продуктів (організаційні форми – документи, книги, бази даних, ілюстрації, фотографії, голограми, кіно-, відеофільми тощо) має бути визнана предметом матеріального світу, тобто віднесена до речей.

Саме нерозривний зв’язок інформації та її носія дозволяє визнати її предметом матеріального світу. Проте така інформація повинна мати назву “дані”.

7. Щодо наполегливості опонентів Закону України “Про захист персональних даних” у запровадженні по відношенню до персональних даних режиму **“особистих немайнових прав”**, замість запропонованої у проекті закону категорії **“право власності людини на свої персональні дані”**.

По-перше. Українці прагнуть відчувати себе європейцями, але ставлення до прав людини та свобод громадянина залишається євразійським. Усе успадковане з минулого. Обговорення та ухвалення законів робиться здебільшого з метою або з урахуванням механізму їх обходу для використання в приватних чи корпоративних інтересах, чи для того, щоб показати юридичну грамотність. У цьому, вважаємо, є одна з головних причин важкості подолання корупції та, зокрема, того що існує на несанкціонованому “ринку” персональних даних.

Раніше джерелом права визначався тільки закон, коли влада наділяла підданих правами, заперечуючи природним невідчужуваним правам та судовому прецеденту. Тобто, держава надавала права, а коли прав держава не надавала, то їх у громадян й не було, панувало свавілля законодавця. Теж саме відбулося із Основним Законом, покликанням якого є оберігання прав людини та основоположних свобод громадянина від посягань держави та від не “чистих на руку”. Конституція із самого початку не була прийнята в результаті конституційного процесу в якому брало участь громадянське суспільство. Вона була політичним договором можновладців, була дарована народу згори і залишається надто декларативною, щоб бути законом прямої дії.

16 років країна знаходиться у процесі трансформації правовій системи та державного управління. Незважаючи на це держава (із судами) продовжує виходити із принципу позитивізму – джерелом права є закони та ін. нормативно-правові акти, зокрема, кодекси, рішення адміністрацій, місцевих рад, навіть рішення “домкомів” (із Швондером; спасибі проф. Преображенському, який вказав де у нас розруха). Різних обґрунтувань та посилок на всілякі норми – досить, для цього існують посади, вища юридична освіта та наукові ступені. Проте все це суперечить духу та принципам ліберальній правовій системі, заснованій на природних невідчужуваних правах людини, та яка визнає Європейські інститути із захисту прав та свобод.

По-друге. Вже зазначалось, що ні в Конституції України, ні в ЦКУ поняття “персональні дані” не вживається. Тому може постати питання – наскільки легітимним є посилання на ЦКУ щодо поняття “персональні дані” (тим більше, у ст. 200 ЦКУ визначено, що це – прерогатива закону)? Адже, з точки зору уявлень юриспруденції, правова експертиза зобов’язана виходити з “букви закону” (хоча ще Марк Тулій Цицерон зауважив: *“Наибольшее бесправие там, где царит буква закона”*), керуватися легітимно визначеними у законодавстві поняттями та підтримувати існуючі межі законодавства, визначеного Конституцією.

Враховуючи наведені нами аргументи, які виходять з реалій та перспектив становлення Інформаційного суспільства, існуючого несанкціонованого збирання та продажу персональних даних у е-середовищі, відсутності державної реєстрації та контролю за базами персональних даних, людина повинна мати можливість захистити сама себе від розповсюдження засобами е-комерції її даних за допомогою потужного інституту права власності. Для будь-якої комерції щодо персональних даних людина виступає як “власник даних на себе”; для держави – людина виступає як “громадянин”, зобов’язаний враховувати інтереси суспільства та держави. Великі мислителі ми-

нулого звертали на це увагу: *“Свобода личности и свобода гражданина не всегда совпадают”* – Ш. Монтескьє; *“Там, где кончается государство, начинается человек”* – казав Ф.Ницше.

*По-третє.* Ніяка інформація так не важлива для людини, як її персональні дані. Вони відображають особистість, приватне життя, стан здоров’я, стосунки тощо людини, яку можна знищити, зокрема, за допомогою створення та поширення так званого “викривленого портрету особи”.

Якщо захист прав людини та свобод є не тільки деклараціями, то ця інформація повинна мати механізм практичної реалізації щодо її унікального та виключного статусу – статусу “майнових та немайнових прав” залежно від відповідних умов її обробки та застосування.

А слово “особистих”, що пристосовано у ЦКУ до “немайнових прав”, взагалі зайве. Зазначене поняття сприймається як “масло - масляне” та сприяє підтримці “системи”, яка в умовах е-середовища може працювати лише формально та адміністративно-суб’єктивно.

*По-четверте.* Історія людства – це нескінченна історія війн: від бійок з дубиною рабовласницької формації з мечами – до ядерних, хімічних, біологічних війн індустріальної цивілізації.

Зараз людство перейшло до епохи інформаційних війн, завдяки яким матеріальних зруйнувань не дуже видно, але мета стара, як світ – економічна експансія. ***Інформаційна війна – це відкриті та закриті цілеспрямовані невідомі інформаційні дії щодо нав’язування супротивнику небажаної інформації для зміни його поведінки через зміну мислення або для самознищення з метою отримання вигашу у матеріальній сфері.***

Для захисту слід передбачити дії противника. Це можливо завдяки інтелекту, яким володіє лише людина. У природі інтелект існує тільки із необхідності захисту. Інтелект людини та наука з’явилися у результаті боротьби за життя проти загроз. Те, що не вдається зрозуміти завдяки логіки, пояснюється вірою та захищається молитвою, магією. Молитва, можна казати, – це програма для особистої підсвідомості. Навіть результати мистецтва є інструментальними засобами захисту суб’єктивних уявлень про світ. Головне у захисті – зрозуміти, з ким маєш справу та знайти відповідні засоби протидії.

Проте, будь-які “розумні” кіберсистеми не в змозі передбачити, яку потенційну загрозу несуть ті чи інші дані, до яких пристосована інформація (мало того, що дані можуть бути небажаними підпрограмами-вірусами-інфекцією, так ще сама інформація невідомо як подіє на свідомість та підсвідомість людини; пригадаємо 25-кадр чи сучасні виборчі технології). Вони просто обробляють вхідні дані та надають висновки чи пропозиції. Це може сприйматися як нові блага (знання), порушуючи такі складні інформаційні системи як людина (суспільство та держава в свою чергу теж), завдяки, насамперед, використання найважливішої для життєдіяльності людини інформації – її персональних даних, та здійснюючи “економічну та духовну інтервенцію”. Тому захист інтелекту, свідомості та підсвідомості людини через засоби максимального захисту її персональних даних є важливою потребою держави у протидії правовому нігілізму, консерватизму та хаосу.

8. У 1600 р. доктор філософії, професор Джордано Бруно (чий ідеї через століття відродили Ж.Кювє та В.Вернадський, якого у 1943 р. знищили завдяки “викривленого портрету”) на допиті трибуналу інквізиції, казав: *“Когда я говорю или пишу, то спорю не из-за любви к победе самой по себе, но из любви к истинной мудрости, и из стремления к ней я страдаю и мучаюсь. ...Я не говорю, что Платон – невежда, Аристотель – осел, а последователи глупцы, дураки и фанатики. Но я не хочу им верить без доказательств и соглашаться с их положениями, недо-стоверность которых доказана ясно и отчетливо”*. Він жив та умер чесно, як вчив жити.

Приклоняючись перед науковим подвигом Д.Бруно, хотілось б помітити наступне.

*“Что есть истина”* – запитав Понтій Пілат. *“Истина есть я”* – відповів Христос. Засновники всіх світових релігій уміли “прислухатися” до природи і створювати стійкі інформаційні системи, функціонуючі століття на фоні виникаючих і зникаючих держав та цивілізацій.

Мислителі старовини вже усвідомлювали, що “істина” – це поняття абсолютне (віра в Бога, Світовий розум і ін.), та, одночасно, відносне (для певного часу). Аристотель був універсальним генієм, головними заслугами якого є створення теорія логіки і спроби наукового підходу до розуміння буття. Він послідовно керувався здоровим глуздом. Любив спостерігати і роздумувати, тому, без сумніву, не схвалив би сліпого поклоніння наступних поколінь до його праць.

Платон – геній мудрості і моральності. Згідно його розуміння блага і оптимальної структури держави (“філософи-стража-народ”) функціонують сучасні демократичні системи (“депутати - виконавча влада-народ”). Він є родоначальником ідеї інформації: *“бесцветная, бесформенная и неосязаемая сущность, в сущности своей существующая, зримая только для кормчего души – разума”*. За Платоном інформація присутня в світі об’єктивно, поза волею і бажанням людей.

У Платона є думка: *“один город – бедных, другой – богатых и в обоих много городов...”*, а тому за демократією походить тиранія. Ця думка заслуговує уваги. Річ у тому, що за допомогою засобів ЗМІ неважко формувати громадську думку, маніпулюючи її за бажанням тих, кому ці засоби належать. При соціалізмі ЗМІ належать державі (точніше, номенклатурі), при капіталізмі – олігархії. Якщо у першому випадку мова може йти про ідеал, про недосягну “державу благоденства” (прямувати до якої є сенс), то у другому – про прагматизм (“город богатых” – за Платоном).

У наш час електронні засоби беруть активну участь в інформаційній експансії (зокрема, у політичній сфері, де ведуться інформаційні війни із поневолення інших держав), пропаганді способу життя, перепрограмуванні світогляду і “зомбування” суспільної свідомості, мета яких – встановлення духовної і економічної влади. Тому, за наявності, здавалося б, загально визначених сучасних прав людини і свобод громадянина, головною проблемою, як вважається, залишається проблема ефективності захисту знань та захисту персональних даних людини.

### Використана література

1. А.Ходорыч. Расколота база // [www.aferizm.ru/bb\\_bd.htm](http://www.aferizm.ru/bb_bd.htm).
2. е-майбутнє та інформаційне право; За ред. члена-кореспондента АПрН України М.Швеця // 2-е вид., доп. – К.: НДЦПІ АПрН України. – 2006. – С. 109-128.
3. Системна інформатизація правоохоронної діяльності: європейські нормативно-правові акти та підходи до упорядкування суспільних інформаційних відносин у зв’язку з автоматизованою обробкою даних у правоохоронній діяльності: Посібник. Кн. 2; За ред. члена-кореспондента АПрН України М.Швеця та к.ю.н. Б.Романюка. – К.: НДЦПІ АПрН України, 2006 р. – 509 с.
4. Типовой закон об электронной торговле Комиссии ООН по правам международной торговли // [www.uncitral.org/uncitral/ru/uncitral\\_texts/electronic\\_commerce.html](http://www.uncitral.org/uncitral/ru/uncitral_texts/electronic_commerce.html).
5. Директива Європейського Парламенту і Ради 2000/31/ЄС “Про деякі правові аспекти інформаційних суспільних послуг, зокрема електронної комерції на внутрішньому ринку” від 8 червня 2000 року // [www.liga.net/zakon/ligazakon.html](http://www.liga.net/zakon/ligazakon.html).
6. Про економічний аспект захисту персональних даних у контексті права власності на інформацію // Правова інформатика. – № 1(9)/2006. – С. 45-48.
7. Цена персональных данных // [www.i2r.ru/article.shtml?id=1384](http://www.i2r.ru/article.shtml?id=1384).
8. Проблема правовой защиты персональных данных // [www.kiev-security.org.ua/box/4/136.shtml](http://www.kiev-security.org.ua/box/4/136.shtml).
9. Законспирированный оборот // [www.privasi.hro.org/risk/data/index](http://www.privasi.hro.org/risk/data/index).
10. Киберпреступность сильнее полиции // Обзор, 2006. – № 103(128). – С. 6.
11. Права человека и защита персональных данных. – Харьков: Фолио-ХПГ, 2000. – 280 с.
12. Правовий механізм захисту персональних даних: Монографія; За ред. д.е.н., професора М.Я. Швеця та д.ю.н., професора Р.А. Калюжного – К.: Парламентське видавництво, 2003. – 120 с.
13. Інформаційне право та правова інформатика у сфері захисту персональних даних; За ред. члена-кореспондента АПрН України Швеця М.Я. – К.: НДЦПІ АПрН України, 2005. – 451 с.
14. Упорядкування суспільних відносин у сфері захисту персональних даних // Правова інформатика. – 1/2003. – С. 43-47; Про зняття з розгляду Верховною Радою України законопроект “Про інформацію персонального характеру” // Правова інформатика. – № 2(6)/2005. – С. 52-64; Про прийняття Верховною Радою України в цілому Закону України “Про захист персональних даних” – № 3(11)/2006. – С. 80-90.
15. Науково-практичний коментар Цивільного кодексу України (Глава 20. Особисті немайнові права. – С. 235-283); За ред. В.М. Косака. – К.: Істина, 2004. – 976 с.

16. Право власності на інформацію: за матеріалами О. Баранова / НДЦП АПрН України, 2006 р.
18. Монтескьє Ш. Избранные произведения: в 2-х т. – М., 1955.
19. Ницше Фридрих. О пользе и вреде истории. – Белая Церковь, 1991.
20. Бруно Джордано. Диалоги. – М., 1949.

~~~~~ \* \* \* ~~~~~