ISSN 2078-6115. Вісник Львівського університету. Серія економічна. 2019. Випуск 56. С. 3-15
Visnyk of the Lviv University. Series Economics. 2019. Issue 56. P. 3-15

УДК 330.101 DOI: http://dx.doi.org/10.30970/ves.2019.56.0.3001
JEL D18,D82,D83,L86,M31

ПОШУК ІНФОРМАЦІЇ ТА ПРИВАТНІСТЬ СПОЖИВАЧІВ В ЕПОХУ ІНФОРМАЦІЙНОЇ ЕКОНОМІКИ І *BIG DATA*

О. Ватаманюк

Львівський національний університет імені Івана Франка
79008 м.Львів, проспект Свободи, 18
E-mail: ostap.vatamaniuk@gmail.com

Проаналізовано основні зміни у поведінці споживачів щодо пошуку інформації, зумовлені розвитком інформаційних і цифрових технологій. Показано, що збереження приватності споживачів різко ускладнюється у зв'язку з прогресом алгоритмів штучного інтелекту. З'ясовано комплекс заходів, спрямованих на поліпшення ситуації з захистом особистих даних.
Ключові слова: *інформаційна економіка, пошук інформації, витрати пошуку, асиметрія інформації, приватність споживачів, витоки даних, захист особистих даних.*

Постановка проблеми. Економічна наука, безумовно, намагається йти в ногу з часом і адекватно описувати реалії сучасної економіки. Стосовно інформаційної економіки це особливо помітно, якщо поглянути на відповідні статті в англомовній Вікіпедії. Тут стаття, присвячена *"information economics"* (тобто економічній науці, яка визнає важливість проблематики інформації в економіці та вивчає її), у декілька разів інформативніша і насиченіша за статтю, присвячену власне *"information economy"* (інформаційній економіці). У цьому сенсі достатньо символічно, що першу Нобелівську премію з економіки нового століття у 2001 році було присуджено Дж. Акерлофу, М. Спенсу та Дж. Стіґліцу саме за дослідження ринків з асиметричною інформацією, що, певним чином, зафіксувало перехід до інформаційної парадигми в економічній науці.

Упродовж багатьох років під час побудови теоретичних моделей економісти припускали досконалість інформації, вважаючи, що певне відхилення від неї принципово не вплине на результати. Натомість, як показав Дж. Стіґліц, навіть незначна недосконалість інформації має глибокий вплив на природу рівноважного стану, оскільки інформація впливає на ухвалення рішень у будь-якому контексті. За Стіґліцем, у реальному світі ключове питання полягає у тому, як і наскільки успішно ринки вирішують фундаментальні проблеми інформації [1].

Стрімкий розвиток інформаційних та цифрових технологій упродовж останніх років різко актуалізував цілу низку проблем, пов'язаних з пошуком та захистом інформації.

Аналіз останніх досліджень та публікацій. Фундаментальні засади інформаційної парадигми в економічній науці сформульовано у працях Дж. Стіґліца [1]. Основи сучасних теорій пошуку інформації заклали Дж. Стіглер та Дж. Маккол [2, 3]. Важливими напрямами досліджень сьогодні є аналіз особливостей пошуку

інформації споживачами в умовах інформаційної економіки [4, 5] та вивчення комплексу проблем, пов'язаних зі збереженням приватності індивідів і захисту особистих даних, які загострюються унаслідок швидкого удосконалення алгоритмів штучного інтелекту [6, 7].

Формулювання цілей статті. Мета пропонованої статті – з'ясувати ключові зміни, що відбулися в поведінці споживачів щодо пошуку інформації в епоху Інтернету, та проаналізувати різноманітні аспекти приватності індивідів за сучасних умов.

Виклад основного матеріалу. Першим, хто запропонував формальну модель пошуку інформації в економіці, був відомий американський економіст Дж. Стіглер [2]. Він виходив з того, що у більшості ситуацій інформація є рідкісним благом, а тому її здобуття передбачає витрати і приносить вигоди. Як наслідок, стан ринкової рівноваги характеризується не єдиною ціною, а певним розподілом цін, дисперсія яких прямо пропорційна витратам пошуку інформації. Оптимальний обсяг цього пошуку визначається рівністю граничних витрат і вигід отриманої інформації. За Стіглером, потенційні покупці зосереджують свою увагу на певній фіксованій кількості продавців (магазинів, веб-сайтів тощо) і купують потрібний їм товар там, де він найдешевший.

Більш поширеним сьогодні є підхід, запропонований незалежно Дж. Макколом та Д. Мортенсеном для аналізу процесу пошуку праці (див. напр. [3]). Результатом його є так звана модель послідовного пошуку, яка легко і логічно видозмінюється для опису поведінки покупців. Згідно з нею, споживачі заздалегідь визначають для себе прийнятну ціну товару і купують його у першого ж продавця, який запропонує цю або нижчу ціну.

В епоху Інтернету витрати пошуку інформації різко знизилися, оскільки значно легше шукати та порівнювати дані щодо потенційних угод чи покупок у режимі онлайн. Це спричинило низку важливих наслідків [5].

Передовсім, нижчі витрати пошуку полегшують споживачам порівняння цін різних продавців, що створює відповідний тиск у напрямку їх зниження. Натомість, всупереч попереднім прогнозам, суттєва дисперсія цін у більшості випадків зберігається. З одного боку, це пов'язано з об'єктивними відмінностями у якості товарів, умовах доставки, досвіді роботи різних роздрібних продавців, впізнаваності брендів тощо.

З іншого боку, самі ж продавці використовують усі доступні можливості, щоб впливати на процес пошуку інформації споживачами. Обираючи товар, потенційні покупці оцінюють різноманітні його аспекти: ціну, якість, репутацію продавця, оплату та час доставки тощо. Зважаючи на це, фірми мають змогу вирішувати, інформацію про які характеристики товару споживач отримає найшвидше і з найменшими зусиллями (тобто за найнижчих витрат пошуку). Інакше кажучи, фірми організовують процес пошуку інформації покупцями у такий спосіб, щоб отримувати вищі ціни. Наприклад, *eBay* за умовчанням показує результати пошуку згідно з алгоритмом рейтингування *best match*: товари показують у порядку, який максимізує очікувані доходи компанії (винагорода за лістинг товарів плюс відсоток ціни кінцевого продажу) [4, С. 7].

Водночас не варто забувати, що до процесу пошуку інформації залучені обидві сторони ринку. Низькі витрати пошуку відчутно поліпшують якість узгодження потреб покупців та продавців, фірм і найманих працівників тощо. Характерною рисою сучасної економіки став розвиток онлайн-платформ, які виконують подвійну

роль – допомагають узгоджувати інтереси покупців і продавців та виступають у ролі посередників, що полегшують пошук контрагентів у найрізноманітніших сферах і підвищують ефективність ринкового обміну.

Обидва попередньо згадані базові підходи до пояснення процесу пошуку інформації споживачами передбачають, що люди точно знають, які товари чи послуги хочуть купити, та містять низку інших, більш чи менш обґрунтованих, припущень стосовно поведінки індивідів у процесі купівлі потрібних їм благ. При цьому оцінки витрат пошуку, базовані на аналізі теоретичних моделей, а не реальних даних, є дуже високими, що веде до висновку про відносно обмежений характер пошуку споживачами інформації про характеристики потрібних їм товарів. Натомість результати нещодавніх досліджень з використанням баз даних, зібраних онлайн-платформами, свідчать, що в реальності поведінка споживачів є значно різноманітнішою.

Використання надзвичайно широкої і деталізованої бази даних *eBay* дало змогу групі американських науковців детально проаналізувати особливості процесу пошуку інформації споживачами [4]. Ці дані дозволяють безпосередньо простежити усі дії індивідів з перебігом часу, упродовж різних сесій пошуку аж до купівлі товару чи відмови від неї і, як наслідок, без жодних додаткових припущень оцінити величину витрат пошуку[1]. Зокрема, у згаданому дослідженні було використано три основні напрями вивчення поведінки покупців [4, С. 3–4]:

1) аналіз дій споживачів упродовж однієї сесії пошуку у деякий конкретний момент часу на основі даних щодо сформульованих запитів для пошуку, відвіданих сторінок, здійснених переходів між ними тощо;

2) виокремлення когорти користувачів (у кількості 500 тисяч осіб!), які здійснювали пошук упродовж певного дня, і фіксація усіх наступних дій кожного з них щодо пошуку та придбання товарів протягом наступного місяця;

3) виокремлення "оберненої когорти" (тобто групи споживачів, які здійснили покупку певного дня) і аналіз їхніх дій протягом певного періоду часу, що передував покупці.

Результати такого масштабного та різнобічного дослідження поведінки споживачів стосовно пошуку інформації про майбутні покупки можна звести до декількох фундаментальних висновків [4].

По-перше, споживачі шукають товар значно довше, ніж вважалося: покупці передують пересічно 36 процедур пошуку, здійснених протягом 3,5 різних, не послідовних, днів за період до декількох тижнів. Оскільки проведений аналіз стосувався лише одного сайту, можна обґрунтовано припускати, що, ймовірно, насправді споживачі шукають ще більше. Альтернативна вартість години пошуку

---

[1] Упродовж багатьох років компанія *eBay* дуже ретельно фіксувала усі дані щодо процесів пошуку та купівлі благ на її сайті. Загалом, ця база даних складається з двох частин. Перша містить повну інформацію щодо кожної здійсненої покупки (цінові пропозиції, сплачена ціна, відомості про продавця і покупця тощо) і охоплює період від 2005 р. Друга зберігає усі дані стосовно того, що робив кожен користувач на сайті (пошукові запити, отримані результати включно з порядком показу товарів та їхніми характеристиками, кліки на посилання і переходи між сторінками) від 2010 р. Вагомою перевагою бази даних *eBay* є можливість відстеження поведінки конкретного користувача упродовж різних сесій пошуку та здійснення різних покупок (цього досягають за допомогою використання *Cookies*) [4, С. 8–9].

оцінюється у межах 15 доларів США у годину (що виглядає значно більш реалістично, ніж попередній діапазон оцінок у межах 81–1800 дол.).

По-друге, можна стверджувати, що поведінка споживачів у процесі пошуку інформації не відповідає жодній зі згаданих моделей, а здійснюється, радше, інтуїтивно (покупці часто оновлюють пошук, середня кількість слів у запиті упродовж сесії зростає, пошук за критерієм *best match* з перебігом часу поступово зменшується, а середня ціна визначених у процесі пошуку потенційних покупок знижується).

По-третє, процес пошуку загалом має лійкоподібний характер: спочатку пошук інформації здійснюється за широкими категоріями, а потім стає все більш сфокусованим на придбання товару за найнижчою ціною за даних витрат пошуку.

Активний пошук потенційними покупцями потрібних їм товарів та послуг онлайн відкриває просто неймовірні можливості щодо нагромадження операторами онлайн-платформ даних про своїх користувачів. Як наслідок, проблеми поваги до приватності індивідів і безпеки особистих даних виходять сьогодні на перший план. Дослідженням цих питань займається економічна теорія приватності (*economics of privacy*) як одна із складових інформаційного напряму економічної науки.

Передовсім, варто з'ясувати наповнення самого терміну "приватність", оскільки в нього нерідко вкладають достатньо різний зміст: захист деякого особистого простору індивіда та його права бути залишеним на самоті; контроль над особистою інформацією та її захист; відчуття гідності, автономії та, зрештою, свободи людини. Пов'язує всі ці, дещо відмінні, аспекти приватності ідея встановлення певних меж між особою та іншими, між приватним та спільним (публічним) [6, С. 443]. Звідси, предметом вивчення економічної теорії приватності є питання вибору, пов'язаного з урівноваженням публічного та приватного між індивідами, організаціями та органами влади [6, С. 443]. При цьому інтерес економістів стосується насамперед інформаційних аспектів приватності, зокрема, аналізу наслідків розкриття та захисту особистих даних[2].

Ще декілька десятиліть тому економічна наука розглядала приватність споживачів лише у контексті асиметрії інформації стосовно конкретної угоди [7, С. 1]. Покупці прагнуть не видавати свою реальну готовність платити за товар зовсім подібно, як продавці не зацікавлені розкривати інформацію про свої граничні витрати та намагаються приховати низьку якість товару. У межах інформаційної парадигми економічної науки і продавці, і покупці мають стимули приховувати або розкривати інформацію, і такі стимули критично важливі для ефективності ринкового обміну[3] [1].

Натомість упродовж останніх років ситуація принципово змінилася. Радикальне зниження витрат збору, зберігання, опрацювання та використання даних спричинило розширення проблематики асиметрії інформації далеко поза межі конкретної угоди.

---

[2] Водночас навіть у межах такого звуженого підходу до визначення приватності вирізняються два очевидно відмінних тлумачення: приватність як *контроль над використанням* особистої інформації та приватність як *захист від доступу* до особистої інформації [6, С. 449].

[3] У реальному житті більша частина інформації отримується зацікавленими сторонами на основі аналізу поведінки економічних агентів. Водночас той факт, що дії передають інформацію, спонукає людей коригувати свою поведінку [1, С. 472].

Зокрема, можна виокремити три ключові її аспекти: невизначеність щодо майбутнього використання даних, негативні екстерналії для покупців та (не)виконання зобов'язань продавців щодо захисту даних споживачів [7, С. 1–3].

У момент часу, коли покупець вирішує, чи надати деяку особисту інформацію у процесі купівлі товару або послуги, можливе використання цих даних залишається невизначеним. Розважливіші споживачі можуть передбачати потенційну небезпеку щодо майбутнього використання даних і вагатися. Проте, у ситуаціях, коли передача особистих даних необхідна для завершення угоди купівлі-продажу, покупці постають перед вибором між негайною вигодою від бажаної покупки та потенційними втратами колись у майбутньому[4].

Суперечливість поведінки споживачів у цьому контексті часом описують терміном "парадокс приватності". З одного боку, люди часто висловлюють серйозне занепокоєння щодо приватності та безпеки особистих даних. З іншого, під час реалізації угод купівлі-продажу значна більшість виявляється готовою надати особисті дані в обмін всього лише на невеликі знижки, безкоштовне обслуговування чи деякі приємні стимули (піца у подарунок тощо)[5].

Ще одна проблема полягає у тому, що очевидні вигоди від майбутнього використання даних – краща класифікація споживачів, ефективніше прогнозування попиту чи поліпшення дизайну продукту – інтерналізуються отримувачем інформації через власне використання або продаж її третім особам. Натомість потенційні шкідливі наслідки, пов'язані з крадіжкою особистих даних, обманом чи шантажем, стосуються, здебільшого, лише покупців. Ця асиметрія між отриманою вигодою і неврахованою ймовірною шкодою означає негативні екстерналії для покупців. Якщо неможливо простежити, хто винен у витоку даних, продавці завжди матимуть стимули збирати якомога більше інформації про покупців.

Складність виявити безпосереднього винуватця завданої споживачам шкоди поряд з невизначеністю щодо майбутнього використання даних та наявною асиметрією інформації про практики збирачів даних також веде до проблеми зобов'язання. Якщо (оскільки) споживачів турбує проблема використання їхніх даних, покупці мають стимули декларувати прихильність кращим практикам, зберігаючи можливість відмовитися від них після збору даних. Водночас виявити реальну практику використання даних зазвичай складно. Ще складніше довести

---

[4] Згідно з результатами численних емпіричних досліджень, людям здебільшого притаманні прагнення до негайного отримання винагороди (задоволення) в короткостроковому періоді і терплячість у довгостроковому. Зворотною стороною нетерплячості щодо задоволення є зволікання з виконанням діяльності, яка потребує часу чи зусиль. У межах поведінкового підходу в економічній науці таку часову структуру уподобань індивідів описують за допомогою так званого гіперболічного дисконтування (див. напр. [8, 9]).

[5] Цікава ідея, запропонована у цьому контексті, полягає у тлумаченні можливостей щодо майбутнього використання даних як нового атрибуту товару, купленого під час угоди. У випадку чіткого визначення цього атрибуту зацікавленими сторонами (скажімо, через детально виписану політику щодо приватності) продавці товарів і послуг на конкурентному ринку поважатимуть побажання своїх покупців щодо обмеженого використання особистих даних. На жаль, сьогодні цей атрибут залишається недостатньо чітко визначеним на момент угоди купівлі-продажу і може змінюватися з перебігом часу – залежно від змін політики щодо особистих даних, здійснюваної продавцями товарів та послуг, проте повністю поза полем зору покупців, їхнім контролем, здатністю спрогнозувати чи оцінити такі потенційні зміни [7, С. 2].

шкоду, завдану споживачам неправильною політикою щодо даних, оскільки суд вимагає чітких доказів причинно-наслідкового зв'язку між цією шкодою та діями збирачів даних.

З огляду на все сказане, стає очевидним, що фактичний стан справ у сфері захисту приватності споживачів спонукає продавців товарів та послуг збирати стільки інформації, скільки готові надати їхні покупці. Отримані дані можуть бути використані як для досягнення власних цілей, так і продані згодом іншим зацікавленим сторонам. При цьому фірми зазвичай не несуть належної відповідальності за ризики, які спричиняють для приватності споживачів та безпеки особистих даних. Така ситуація безпосередньо зумовлена ставленням до неї та діями обох сторін ринку.

З одного боку, покупці, як з'ясовано вище, переважно готові надавати особисту інформацію під час придбання товарів та послуг. При цьому абсолютна більшість (91%) споживачів у США вважають, що вони втратили контроль над процесом збору та використання фірмами їхніх особистих даних; водночас лише 11% припиняють відносини з компанією, яка допустила витік даних, тоді як 77% повністю задоволені її діями після інциденту з втратою даних [7, С. 9–10].

З іншого, фірми, навіть усвідомлюючи потенційні ризики для своїх клієнтів унаслідок нових цифрових технологій, спершу впроваджують ці технології і лише потім задумуються про заходи щодо захисту особистих даних [7, С. 10]. Така легковажність має раціональне підґрунтя: прямі збитки компаній, спричинені втратою даних, є порівняно незначними, що опосередковано підтверджується слабкою і тимчасовою реакцією фондового ринку на масштабні витоки даних [7, С. 11]. Зазвичай саме споживачі змушені витрачати час, зусилля та й гроші для ліквідації наслідків витоків даних.

Масштаби витоків особистих даних достатньо переконливо ілюструє перелік хоча б декількох широко відомих нещодавніх випадків:

- лютий 2015 р., *Anthem* (охорона здоров'я), 80 мільйонів записів, у тому числі імена та дати народження, номери соціального страхування;
- липень 2017 р., *Equifax* (фінансовий сектор), 145,5 млн. записів, у т.ч. номери соціального страхування, посвідчень водіїв, повні кредитні історії;
- березень 2018 р., *Under Armour* (споживчі товари), 150 млн. записів, у т.ч. імена, електронні адреси та паролі користувачів;
- вересень 2019 р., особисті дані щодо усіх 17 мільйонів громадян Еквадору, включно з повними іменами, датами і місцями народження, ідентифікаційними номерами та номерами телефонів і даними щодо освіти [10].

У поточному році вже зафіксовано нові масштабні витоки даних, повніша інформація про які, ймовірно, стане відомою дещо згодом: *Canva* (веб-дизайн), 140 мільйонів записів; *Capital One* (фінансовий сектор), 106 млн. записів; *Facebook* (соціальні мережі), 540 млн. записів; *First American Corporation* (фінансові послуги), 885 млн. записів; *MTS* (телекомунікації), 100 млн. записів; *Truecaller* (телефонна директорія), 299 млн. записів; *Zynga* (соціальні мережі), 218 млн. записів [11].

Загалом, згідно з даними одного з найвідоміших спеціалізованих сайтів (станом на 11 листопада 2019 р.), від 2005 року зафіксовано 9738 витоків даних, які охоплюють понад 11,6 мільярдів записів [12]. Як прогнозують, до 2020 року середні збитки унаслідок витоків даних перевищать 150 мільйонів доларів США, а втрати у глобальному масштабі досягнуть 2,1 трильйона доларів [11]. Лише у першій половині 2018 року витоки даних охопили приблизно 4,5 мільярдів записів, а у поточному році

набір з 2,7 мільярдів записів, що включає 774 мільйони електронних адрес та 21 мільйон паролів було запропоновано до продажу у світовій мережі [11].

Проблема захисту приватності споживачів різко загострилася буквально упродовж декількох останніх років у зв'язку з швидким удосконаленням алгоритмів штучного інтелекту, які опрацьовують величезні масиви даних для того, щоб краще зрозуміти і передбачити поведінку споживачів та вплинути на неї.

Штучний інтелект уможливлює використання зібраних даних для ідентифікації індивідуальних споживачів. Використання його на законних підставах може підвищити ефективність управління компаніями, стимулювати інновації і краще узгоджувати попит та пропозицію. Водночас нові вигоди, зумовлені його застосуванням до аналізу великих обсягів даних – заощадження на витратах і збільшення продажів – можуть спонукати фірми до таємної відмови від обіцянок щодо приватності та безпеки даних. У поганих руках штучний інтелект може стати засобом масштабного обману та шахрайства.

У зв'язку з широким впровадженням алгоритмів штучного інтелекту виокремлюють дві ключові небезпеки стосовно використання особистих даних [7, С. 7]. По-перше, сьогодні доступ до такої інформації отримують не лише великі компанії, які використовують штучний інтелект для масового, індивідуалізованого, проте не персоналізованого маркетингу, але й невеликі неринкові організації, які можуть використати ці дані для персоналізованого таргетування споживачів. Останні значно небезпечніші для таргетованих осіб, оскільки менше зважають на репутацію, невидимі для споживачів і можуть бути зацікавлені у спричиненні більшої шкоди, ніж просто спонукати до придбання непотрібного товару. До того ж, ці "погані хлопці" використовують такі ж ключові алгоритми штучного інтелекту, що й великі компанії.

По-друге, навіть у разі повної безпеки особистих даних і обмеження використання штучного інтелекту тільки для "правильних цілей", немає жодних гарантій, що це не завдасть шкоди споживачам. Прогнозні алгоритми у пошуках правди про споживачів підлягають зовнішньому впливу; як наслідок, алгоритм, спроектований для *розкриття правди*, може трансформуватися в алгоритм для *визначення, що ж є правдою* [7, С. 7]. Це завдаватиме шкоди, оскільки розробники алгоритмів можуть використовувати їх для реалізації своїх інтересів – збільшення прибутків, здобуття політичної влади чи управління культурними змінами, що може розбігатися з інтересами споживачів.

Згадані небезпеки вже сьогодні не можна вважати позірними чи чисто теоретичними. Найвідомішим прикладом, ймовірно, є ситуація довкола президентських виборів у США у 2016 році. Багато фахівців вказують на важливу роль у перемозі Дональда Трампа зусиль фірми *Cambridge Analytica*, яка використала під час президентської компанії підходи, розроблені М. Козинським з Центру психометрії в англійському Кембриджі[6] [13]. Як нещодавно визнав віце-прем'єр з

[6] Побудована М. Козинським модель базується на аналізі уподобань ("лайків") та пересилання повідомлень інших осіб ("репостів") індивіда у соціальних мережах і співставленні їх з його статтю, віком та місцем проживання. При цьому вивчення 68 "лайків" програмі достатньо, щоб визначити колір шкіри особи (з ймовірністю 95%);

питань цифрової трансформації М. Федоров, подібні технології активно використовувалися і під час виборів в Україні[7] [14].

Треба зазначити, що економічна наука упродовж тривалого часу серйозно недооцінювала потенційні загрози, пов'язані з порушенням приватності споживачів. Це особливо помітно під час аналізу основного фокусу досліджень у цій сфері. Скажімо, автори фундаментальної оглядової статті, присвяченої економіці приватності, виокремлюють три хвилі різкого зростання інтересу до цієї тематики – у 1970-х та на початку 1980-х років, у 1990-х роках і сьогодні [6, С. 449]. Перша з цих хвиль зосереджувала увагу на аналізі "загальних економічних аргументів щодо величини шкоди, якої можуть зазнати індивіди та суспільство, коли особиста інформація захищена, унаслідок чого потенційно корисна інформація залишиться недоступною на ринку" [6, С. 450].

Подібним спрямуванням відзначалися, значною мірою, і праці представників другої хвилі. Як приклад, варто навести висновок, що споживачі зазнають втрат, якщо надто *мало* (а не надто багато) особистої інформації про них буде відомо третім сторонам [6, С. 452]. У цьому ж руслі лежить і теза про можливі суспільні втрати, спричинені тим, що приватність споживачів може бути перешкодою на шляху встановлення довіри [6, С. 452]. Спроби використати для вирішення проблеми приватності підхід теореми Коуза виявилися не надто успішними з огляду на супутні неповноту та асиметрію інформації [6, С. 453].

Лише у межах сучасної хвилі досліджень питання власне захисту приватності споживачів стає одним із ключових. Водночас і сьогодні автори згаданого огляду наголошують, що "економічна наука та емпіричний аналіз приватності допускають

після аналізу 150 "лайків" вона знає людину краще, ніж її батьки, а після аналізу 300 "лайків" – краще, ніж її партнер.

Cambridge Analytica використала розробки Козинського для цілеспрямованого впливу на конкретні, чітко визначені групи виборців у США. Скажімо, у день третіх дебатів між кандидатами у президенти Д. Трампом та Г. Клінтон у соціальні мережі було відправлено понад 175 тисяч різних варіацій повідомлень, які відрізнялися лише в дрібних деталях. Ідея полягала у тому, щоб максимально точно психологічно відповідати запитам конкретних отримувачів інформації, для чого використовувалися незначні відмінності у заголовках і підзаголовках, фонових кольорах, особливостях фото- та відеоматеріалів тощо. З огляду на результати виборів, 15 мільйонів доларів, отримані від Д. Трампа за свої послуги, компанія чесно заробила (детальніше див. [13]).

[7] У нещодавньому інтерв'ю "Українській правді" Михайло Федоров так відповів на запитання журналіста про використання досвіду президентської компанії Д. Трампа під час виборів в Україні: "Я можу сказати про той напрям, за який я відповідав. Ми достатньо широко використовували глибоке таргетування – з різними аудиторіями говорили про те, що конкретно цікавить дану цільову аудиторію. Це не було маніпуляцією, це було більше транслювання нашої конкретної програми. Ми говорили студентам – що ми робимо для студентів, пенсіонерам – що ми робимо для пенсіонерів. Це називають глибоким таргетуванням. Нібито всі кажуть, що Трамп переміг завдяки цій технології. Я не вважаю, що Трамп переміг завдяки цьому. Я не вважаю, що ми перемогли завдяки цьому. Але *цю технологію, мені видається, ми допрацювали на рівень глибше, ніж це було в команді Трампа* (виділення моє – О.В.). І при набагато меншому бюджеті змогли більше пропрацювати, сегментувати цільову аудиторію. Не просто жінки, мами, пенсіонери. А, наприклад, чоловіки 30–35 років, які працюють в *Uber*. Ми намагалися максимально глибоко таргетуватися для того, щоб наша комунікація була точковою" [14].

різні сценарії. В одних захист приватності може зменшувати індивідуальний та суспільний добробут, в інших – підвищувати. Тому неможливо однозначно стверджувати, що захист приватності спричинить "позитивні" чи "негативні" зміни в чисто економічному плані: цей вплив залежить від контексту" [6, С. 443–444].

З огляду на складність і багатогранність проблеми захисту приватності споживачів, реально змінити ситуацію можна лише за допомогою системних зусиль усіх зацікавлених сторін за декількома ключовими напрямами.

1) Підвищення поінформованості споживачів щодо наявних проблем. Повніше усвідомлення потенційних загроз несанкціонованого використання особистих даних спонукатиме людей відповідальніше ставитися до поширення чутливої інформації і ретельніше оцінювати пов'язані з цим ризики.

2) Формування правильної системи стимулів для вибору фірмами кращих практик щодо використання та захисту даних. Конкурентне ринкове середовище стосовно цих питань часто посилає суперечливі сигнали. З одного боку, фірми реагують на попит з боку споживачів щодо захисту приватності та особистих даних, що підштовхує їх до відповідних кроків у цьому напрямку. З іншого, згаданий попит конкурує з їх же попитом на зручність використання та нижчі ціни товарів та послуг. У разі протиріччя між цими запитами фірми мають вагомі стимули віддати перевагу тим аспектам, які легше помітити і оцінити споживачам, що, вочевидь, не йде на користь безпеці особистих даних.

Забезпечення реальної відповідальності фірм за збереження приватності та особистих даних споживачів вимагає прозорості аналізу зв'язків між практиками роботи з даними та завданою у результаті цього шкодою, і формування стимулів безпосереднього впливу на вибір фірмами кращих практик.

3) Адекватне законодавче регулювання питань приватності та безпеки даних. Навіть у США відповідне законодавство сьогодні оцінюють як уривчасте і несистемне, присутнє передовсім на рівні окремих штатів та стосовно окремих сфер (фінансовий сектор, сфера охорони здоров'я, захист дітей тощо).

4) Саморегулювання галузі. Логіка цього підходу очевидна: хто, краще ніж самі фірми, може знати тонкощі сучасних технологій та оптимальні практики роботи з особистими даними. З іншого боку, як свідчить історичний досвід, ефективне саморегулювання галузі можливе передовсім у разі реальної загрози запровадження жорсткого регулювання з боку держави. Тобто заходи держави і кроки щодо саморегулювання галузі в ідеалі мали б взаємодоповнюватися.

5) Визначення прав приватності за аналогією з правами власності. Згідно з цим підходом, традиційний законодавчий захист приватності індивідів очевидно застарів, і система, базована на правах власності щодо особистої інформації, краще відповідатиме інтересам як споживачів, так і фірм. Відповідно, мають бути створені ринки інформації, на яких індивіди зможуть передавати права на свої особисті дані зацікавленим сторонам за певну компенсацію [6, С. 453].

6) Використання штучного інтелекту для контролю за доступом до даних. Оптимісти сподіваються, що у цьому випадку джерело проблеми може водночас стати і ключем до її розв'язання. Прикладом такого підходу може бути так звана диференційована приватність, яку використовують, зокрема, *Apple* та *Google*. Базова ідея полягає в тому, що фірма-збирач даних додає трохи випадкового шуму до інформації стосовно особистих даних, що допускає їх повноцінний аналіз без надмірної деталізації стосовно конкретних осіб [7, С. 13–14]. Достатність таких

заходів залишається дискусійним питанням, проте перспективи підвищення ефективності цього підходу очевидні.

Висновки. Підсумовуючи, треба зазначити, що в епоху інформаційної економіки витрати пошуку інформації споживачами радикально знизилися, що, певною мірою, поставило під сумнів усталені теоретичні моделі. Результати нещодавніх досліджень з використанням масивів даних, зібраних онлайн-платформами, засвідчили, що пошук інформації потенційними покупцями здійснюється назагал інтуїтивно, триває значно довше, ніж вважалося досі, і має лійкоподібний характер (поступово фокусується на придбанні товару за найнижчою ціною за даних витрат пошуку).

Нагромаджені онлайн-платформами та соціальними мережами обсяги інформації стосовно особистих даних індивідів, їх доходів, уподобань, бажань, інтересів, резервних цін тощо все більшою мірою сприймаються як цінні активи, що можуть бути використані для таргетування послуг, пропозицій та реклами або перепродані іншим зацікавленим сторонам. Якщо володіння інформацією дає владу, то контроль над особистими даними може мати кардинальний вплив на перерозподіл економічної влади між учасниками ринку.

Проблема захисту приватності споживачів відчутно ускладнюється у зв'язку з швидким розвитком алгоритмів штучного інтелекту, які відкривають небачені можливості для ідентифікації індивідів та впливу на їхню поведінку. Змінити ситуацію на краще можна, доклавши серйозних зусиль за декількома напрямами, такими як підвищення поінформованості споживачів стосовно наявних проблем, формування системи стимулів для вибору фірмами кращих практик роботи з даними та їх захисту, адекватне законодавче регулювання з боку держави та саморегулювання галузі, використання самого ж штучного інтелекту для контролю за доступом до даних.

1. Stiglitz J. Information and the Change in the Paradigm in Economics / J.Stiglitz // American Economic Review. – 2002. – Vol. 93, № 2. – P. 460–501.
2. Stigler G. J. The Economics of Information / G. J. Stigler // Journal of Political Economy. – 1961. – Vol. 69, № 3. – P. 213–225.
3. McCall J. J. Economics of Information and Job Search / J. J. McCall // The Quarterly Journal of Economics. – 1970. – Vol. 84, № 1. – P. 113–126.
4. Blake T., Nosko K., Tadelis S. Returns to Consumer Search: Evidence from eBay / T. Blake, K. Nosko, S. Tadelis // 2016. – 25 p. – [Електронний ресурс] – Режим доступу: http://www.nber.org/papers/w22302
5. Goldfarb A., Tucker C. Digital economics / A. Goldfarb, C. Tucker // 2017. – 89 p. – [Електронний ресурс] – Режим доступу: http://www.nber.org/papers/w23684
6. Acquisti A. The Economics of Privacy / A. Acquisti, C. Taylor, L. Wagman // Journal of Economic Literature. – 2016. – Vol. 54, № 2. – P. 442–492.
7. Jin C. Z. Artificial Intelligence and Consumer Privacy / C. Z. Jin // 2018. – 23 p. – [Електронний ресурс] – Режим доступу: http://www.nber.org/papers/w24253
8. Angeletos G.-M. The Hyperbolic Consumption Model: Calibration, Simulation, and Empirical Evaluation / G.-M. Angeletos, D. Laibson, A. Repetto, J. Tobacman, S. Weinberg // Journal of Economic Perspectives. – 2001. – Vol. 15, № 3. – P. 47–68.
9. Ватаманюк О. Біхевіористський підхід у сучасній економічній теорії / О. Ватаманюк // Економічна теорія. – 2006. – № 1. – С. 40–51.
10. Data breach. – [Електронний ресурс] – Режим доступу: https://en.wikipedia.org/wiki/Data_breach

11. List of data breaches. – [Електронний ресурс] – Режим доступу: https://en.wikipedia.org/wiki/List_of_data_breaches
12. Data breaches. – [Електронний ресурс] – Режим доступу: https://privacyrights.org/data-breaches
13. Крогерус М. Хто насправді привів Трампа до перемоги / М. Крогерус. – [Електронний ресурс] – Режим доступу: https://nv.ua/ukr/opinion/recommends/kto-na-samom-dele-privel-trampa-k-pobede-316617.html
14. Романюк Р., Некрасов В. Віце-прем'єр Михайло Федоров: Деякі технології на виборах ми допрацювали глибше, ніж Трамп. – [Електронний ресурс] – Режим доступу: https://www.pravda.com.ua/articles/2019/09/27/7227431/

References

1. Stiglitz, J. (2002). Information and the Change in the Paradigm in Economics. *American Economic Review, 93*(2), 460–501.
2. Stigler, G. J. (1961). The Economics of Information. *Journal of Political Economy, 69*(3), 213–225.
3. McCall, J. J. (1970). Economics of Information and Job Search. *The Quarterly Journal of Economics, 84*(1), 113–126.
4. Blake, T., Nosko, K., Tadelis, S. (2016). *Returns to Consumer Search: Evidence from eBay*. Retrieved from http://www.nber.org/papers/w22302.
5. Goldfarb, A., Tucker, C. (2017). *Digital economics*. Retrieved from http://www.nber.org/papers/w23684.
6. Acquisti, A., Taylor, C., Wagman, L. (2016). The Economics of Privacy. *Journal of Economic Literature, 54*(2), 442–492.
7. Jin, C. Z. (2018). *Artificial Intelligence and Consumer Privacy*. Retrieved from http://www.nber.org/papers/w24253.
8. Angeletos, G.-M., Laibson, D., Repetto, A., Tobacman, J., Weinberg S. (2001). The Hyperbolic Consumption Model: Calibration, Simulation, and Empirical Evaluation. *Journal of Economic Perspectives, 15*(3), 47–68.
9. Vatamaniuk, O. (2006). Biheviorystskyi pidhid u suchasniy ekonomichniy nauci [The behavioral approach in modern economics]. *Ekonomichna teoriya – Economic theory, 1,* 40–51 [in Ukrainian].
10. Data breach (n.d.). From *Wikipedia, the free encyclopedia.* Retrieved November 11, 2019, from https://en.wikipedia.org/wiki/Data_breach.
11. List of data breaches (n.d.). From *Wikipedia, the free encyclopedia.* Retrieved November 11, 2019, from https://en.wikipedia.org/wiki/List_of_data_breaches.
12. Data breaches. Retrieved November 11, 2019 from https://privacyrights.org/data-breaches .
13. Krogerus, M. (2016, December 9). *Khto naspravdi pryviv Trampa do peremohy [Who actually led Trump to victory]*. Retrieved from https://nv.ua/ukr/opinion/recommends/ kto-na-samom-dele-privel-trampa-k-pobede-316617.html [in Ukrainian].
14. Romaniuk, R., Nekrasov, V. (2019, September 27). *Vice-premyer Mykhaylo Fedorov: deyaki tekhnolohiyi na vyborah my dopraciuvaly hlybshe, niz Tramp [Deputy Prime Minister Mykhaylo Fedorov: Some election technologies we have finalized deeper than Trump*]. Retrieved from https://www.pravda.com.ua/ articles/ 2019/09/27/ 7227431/

ISSN 2078-6115. Вісник Львівського університету. Серія економічна. 2019. Випуск 56

INFORMATION SEARCH AND CONSUMER PRIVACY IN THE AGE OF INFORMATION ECONOMY AND BIG DATA

O. Vatamaniuk

Ivan Franko National University of Lviv
Prospekt Svobody 18, UA – 79008, Ukraine

The main changes in consumer behavior concerning information search, caused by development of informational and digital technologies, are analyzed. It is shown that situation with consumer privacy is substantially deteriorated due to the progress of artificial intelligence algorithms. The set of possible measures, directed on the improvement of personal data security, is outlined.

Problem setting. The increased role of information in the modern economy is recognized within information economics, which represents a fundamental change in the prevailing paradigm within science of economics. The fast development of informational and digital technologies during last decades had opened unprecedented opportunities for consumers to find necessary goods and services online. At the same time, it caused serious problems concerning consumer privacy and personal data security.

Recent research and publications analysis. G. Stigler and J. McCall were the first to develop formal models of information search in economics. Current research in this sphere is focused on the characteristics of online consumer search and analysis of the key problems of consumer privacy protection and data security arising under digital economy. Such problems are strongly exacerbated due to rapid progress of artificial intelligence.

Paper objective. The purpose of the article is to trace basic changes in consumer behavior concerning the search of information in the age of the Internet and consider different facets of consumer privacy under the current conditions.

Paper's main body. The avalanche growth of modern informational and digital technologies resulted in the radical decline of information search costs and questioned standard theoretical models. On the other hand, extremely rich and detailed datasets, collected by some online platforms, provided excellent opportunities for comprehensive empirical analysis. According to recent studies, consumer search usually follows intuitive patterns, lasted considerably longer than earlier suggested, and is of funnel type – initially conducted along broad categories and then becomes more focused to buy a good at the lowest cost under given cost of search.

During the last decade, many online platforms have accumulated huge volumes of data about their customers, including rather sensitive information regarding wants, preferences, interests, incomes, reserve prices, etc. That kind of data today is more and more often considered as a valuable business asset that can be used to target services, offers, and advertising, or be traded with other interested parties. If possession of the information means power, then control over personal data can have crucial effect on the redistribution of economic power between market participants. As data breaches of large scale became almost weekly routines, consumer privacy today is seriously endangered.

The problem of personal data safety is seriously complicated by the progress of artificial intelligence algorithms that reveal unprecedented opportunities to identify individual users. Nowadays, artificial intelligence can be used both for individualized and personalized targeting of consumers. Even in the first of these cases consumers can suffer harm as algorithm developers pursue their interests, which could contradict the best interests of their customers. In the wrong hands artificial intelligence can become a powerful instrument of consumer choice manipulations, mass production of fraud and deception.

Conclusions of the research. Fundamental advances in informational and digital technologies caused essential reduction of information search costs, simultaneously decreasing, even more, the costs of collecting, storing, processing, and using data. As a result, consumer privacy protection and personal data safety became the vital challenges for modern economy. The solution can be found by combining efforts in different directions such as create right incentives to help firms choose

consumer-friendly data practices, approve adequate legislation, introduce industry self-regulation and use artificial intelligence to control data access.

Keywords: information economy, information economics, information search, search cost, information asymmetry, consumer privacy, data breaches, personal data security.