

РОЗДІЛ 3

ПОЛІТИЧНА, СОЦІАЛЬНО-ЕКОНОМІЧНА, ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА ТА ЕКОЛОГІЧНА БЕЗПЕКА НА ПОЧАТКУ XXI ст.

УДК 316.774 : 004.738.5+342.7

Зернецька О.В.,
*доктор політичних наук, професор,
в. о. завідувача відділу глобальних і
цивілізаційних процесів
ДУ «Інститут всесвітньої історії НАН України»*

СОЦІАЛЬНІ МЕРЕЖІ І КІБЕРБЕЗПЕКА ОСОБИСТОСТІ

Досліджуються глобальні соціальні мережі (Facebook, LinkedIn, etc.) як нова віртуальна реальність XXI ст., яка може зашкодити кібербезпеці особистості. Аналізується ситуація, коли громадянин не може висловлювати приватні думки без спостереження з боку держави. Порушуються права на приватність та людську гідність. Вивчаються порушення фундаментальних прав людини на думку, на точку зору, на висловлювання. Пропонуються правила безпеки у соціальних мережах.

Ключові слова: глобальні соціальні мережі, кібербезпека особистості, Інтернет, фундаментальні права людини.

Зернецкая О.В. Социальные сети и кибербезопасность личности. Исследуются глобальные социальные сети (Facebook, LinkedIn, etc.) как новая виртуальная реальность XXI ст., которая может помешать кибербезопасности индивидуума. Анализируется ситуация, когда гражданин не может высказывать личные мысли без слежения со стороны государства. Изучаются нарушения фундаментальных прав человека на мнение, на точку зрения, на выражения. Предлагаются правила безопасности в социальных сетях.

Ключевые слова: глобальные социальные сети, кибербезопасность индивидуума, Интернет, фундаментальные права человека.

Zernetska O. V. Social networks and cybersecurity of an individual. Global social networks (Facebook, LinkedIn, etc.) as a new virtual reality of the XXI st century that may harm cybersecurity of any individual is investigated. The situation of a citizen unable to communicate private thoughts without surveillance of a state is analyzed. The rights to privacy and human dignity are violated. The fundamental rights of freedom of thought, opinion and expression that are at the center of any democratic practice are detected. Some rules of behavior in social networks are recommended.

Keywords: global social networks, cybersecurity of an individual, Internet, the fundamental rights.

На початку XXI ст. соціальні сайти та мережі стали дуже популярними. Люди використовують їх, щоб підтримувати зв'язки із своїми родичами та друзями. Це такі глобальні соціальні мережі, як MySpace,

FriendWise, FriendFinder, Yahoo! 360, Facebook, Orkut, Classmates та багато інших. У кожній країні є також свої соціальні мережі. У Сполучених Штатах, наприклад, багато «юзерів» користуються LinkedIn, щоб мати різні бізнесові контакти та відстежувати можливості у зростанні своїх кар'єр.

Але не всі підозрюють, що користування Інтернетом в добу соціальних медіа, або, як її ще називають, «web 2.0» (blogs, wikis, file sharing, social networking sites, microblogs), несе в собі багато загроз для користувачів Інтернету. «В останні роки він перетворився із системи, орієнтованої передовсім на постачання інформації, на медіум для комунікації та розбудови комунікації» [5]. Поняття «web 2.0», соціальний софтвер, сайти соціального мережування, такі як Facebook, Twitter, MySpace, з'явилися у цьому контексті. Разом із цими платформами сформувалася і зберігається величезна кількість персональних даних, які систематично оцінюються та використовуються рекламодавцями для пошуку своїх таргетингових користувачів.

У світі глобальної економічної конкуренції, кризи та побоювання тероризму після 9/11 і корпорації, і державні установи мають усе зростаючий інтерес до цих персональних даних. Тому особливо важливими стають такі питання:

- як змінюється ландшафт у цій сфері;
- як відбувається збирання комерційних персональних даних для реклами;
- як співвідносяться сайти для споживачів та інтерактивні медіа;
- як відбувається саморозкриття у соціальних сайтах;
- як йде спостереження за тими, хто обмінюється файлами;
- як трактується прайвеси в добу Інтернету;
- що таке громадянське самоспостереження за сайтами соціальних мереж та мережеве спостереження у транснаціональному просторі.

Сайт «Що таке соціальне мережування?» [6] в доступній формі ознайомлює користувачів з тим, які небезпеки чекають необачних «юзерів» у соціальних мережах. Відчувається, що він спрямований на молодіжну групу. Розмова на ньому йде від першої особи: «Я впевнений, що ви свідомі того, що існують небезпеки, пов'язані із соціальними мережами, включаючи крадіжку даних та віруси. Найбільша небезпека часто криється в онлайн-хижачах або індивідуумах, які видають себе за когось, ким вони насправді не є. Хоча небезпека існує в онлайн-мережуванні, вона існує і в реальному житті. Так само, як вам радять, що робити, коли ви зустрічаєте незнайомця у клубах і барах, в школі чи на роботі, – такі саме поради стануть вам у пригоді, аби бути обережними онлайн...». Далі подаються конкретні настанови, як треба поводитися у кіберпросторі:

- Створи свій особистий медіа-прайвесі простір, аби дозволяти тільки твоїм друзям бачити твій профіль та контент.

Не приймай дружніх запрошень від незнайомців.

Не відкривай нікому твій щоденний розклад справ.

- Не дозволяй людям знати, коли тебе немає вдома.
- Не використовуй локально базовані сервіси типу Facebook Places та Foursquare, які автоматично підказують, де ти зараз знаходишся.
- Не надсилай фотографії членів своєї родини (особливо малят) чи фото дорогих речей, що є в твоїй домовіці.
- Запропонуй Google Maps зробити розпливчастими фото твого будинку, твоєї машини або будь-чого, що для тебе є приватним, аби бути висвітленим публічно».

Ясна річ, що ці поради написані для молодого покоління, але вони стосуються кожного. Натомість поради американської впливової газети Washington Post скеровані передовсім на солідну публіку. Це сталося після скандалу 2014 р., коли хакери оприлюднили інтимні фотографії голлівудських зірок, які ті зберігали в сервісі iCloud. ФБР почало розслідування. На сайті Washington Post виклали декілька порад, як захищати свої дані:

1. Слід пересвідчитися, що деякі з ваших фото не потрапили в iCloud без вашого відома.

Деякі компанії на кшталт Apple, Microsoft, Dropbox пропонують автоматично зберігати в «хмарі» фотографії з ваших телефонів або планшетів.

2. Користуйтеся двохетапною ідентифікацією.

Ця процедура допоможе вам підвищити захищеність аккаунтів за допомогою додаткового короткого коду, крім паролю при вході.

3. Уникайте пасток хакерів.

Хакерні атаки часто-густо стають успішними не завдяки високим технологіям, а завдяки введенню в оману потерпілих, які в кінцевому підсумку самі видають зловмисникам потрібні їм дані.

Але не тільки хакери прокладають собі шлях до розкриття даних американців. Це роблять і федеральні інститути США. Вони змусили відомий Інтернет-пошуковик Yahoo відкрити доступ до конфіденційних даних користувачів, погрожуючи щоденно штрафувати компанію на 250 тис. дол. Про це сповіщає адміністрація Yahoo в Інтернет-блозі своєї компанії.

Компанія, отримавши дозвіл суду, опублікувала 1,5 тис. сторінок документів, пов'язаних із судовим позовом проти Агентства національної безпеки (АНБ). Юрисконсульт Yahoo Рон Белл додав до цієї публікації відповідні коментарі. З документів стає зрозумілим, що спроба АНБ отримати доступ до персональних даних стала можливою тільки 2007 р. після того, як законодавство США були внесені зміни, які дозволяли владі вимагати від Інтернет-компаній інформацію щодо користувачів.

Спочатку Yahoo, як стверджує Белл, відмовлялася виконувати накази АНБ, вважаючи їх антиконституційними. Компанія подала судовий позов на АНБ в суд, що займається наглядовою діяльністю над розвідками, вимагаючи відмінити таку антиконституційну вимогу. Але цей суд

здебільшого стає на бік влади, тому компанія після півторарічної боротьби зазнала поразки.

Вимогою АНБ було отримання від компанії метаданих про користувачів її електронної пошти. Такі дані дають змогу відстежити, між ким і коли відбувається обмін посланнями. При цьому дозволу на доступ до листів, як стверджують в Yahoo, спецслужби ніколи не мали. Влітку 2013 р. найбільші Інтернет-компанії США, які брали участь у передачі даних АНБ, звернулися до суду з вимогою дозволити публікацію статистичних даних щодо запитів спецслужб. Перша публікація таких даних відбулася у лютому 2014 р. Зараз Інтернет-компанії намагаються провести через Конгрес закон, який би захищав конфіденційність приватного листування [3].

Влітку 2013 р. в Інтернеті був опублікований лист організацій громадянського суспільства світу до Конгресу Сполучених Штатів про Інтернет-спостереження та телекомунікаційне спостереження. В ньому йшлося: «Ми пишемо як коаліція організацій громадянського суспільства з усього світу для того, щоб висловити серйозну занепокоєність, виходячи з численних прикладів спостереження за американськими та не американськими громадянами. Також ми дуже занепокоєні тим, що дані, які збираються під час спостереження в Сполучених Штатах, передаються іншим державам, включаючи Велику Британію, Нідерланди, Канаду, Бельгію, Австралію та Нову Зеландію. Багато американських компаній глобального значення роблять те саме».

Як бачимо, група могутніх глобальних Інтернет-компаній співпрацює із спецслужбами, хоча тоді, коли вони тільки виходили на ринок інформаційно-комунікаційних послуг, вони обіцяли повну приватність користувачам. На що це з часом перетворюється, простежимо на прикладі найбільшої в світі соціальної мережі Facebook.

Соціальна мережа Facebook перетнула межі країни, регіону й сягнула глобальних масштабів. У чому ж секрет її успіху в світі? Соціальна мережа Facebook принципово відмінна від усіх інших Інтернет-компаній, які їй передували, хоча б тим, що вона теоретично і практично ґрунтується на справжній інформації про особу. «Тут важливо бути собою. В Інтернеті всі давно вже звикли до анонімності, ролей, псевдонімів, нікнеймів..., тут же все це зайве. Якщо ви вигадаете собі образ чи надто штучно поведіться, у Facebook вам робити нічого. Будьте собою, інакше друзі вас не впізнають чи не зафрендять. Тут швидко дізнаються, хто ви насправді, лиш перевіривши список ваших друзів. Саме вони є вашим посвідченням особи», – відзначає Д.Кірпатрік, який написав книгу про цю компанію [2]. Він замислюється над соціальними і психологічними змінами, спричиненими ефектом Facebook. Він розуміє, що ще замало наукових даних, аби з упевненістю говорити про них, але наголошує, що для багатьох Facebook – джерело оманливого почуття єдності (5000 друзів – максимально дозволена кількість друзів), яка з часом вироджується у глибоку самотність. До того ж він запитує, чи не

втрачають молоді люди, які днями сидять у Facebook, здатність радіти й дивуватися тому, що відбувається в реальному світі і оточує їх повсякденно?

З часом ейфорія від знаходження старих друзів та «придбання» нових пройшла. Викладення у Facebook «прикольних» фотографій з вечірок, де студентські витівки часто-густо були зафіксовані їхніми товаришами без дозволу (тобто, у соціальну мережу попадали кадри з пляжками або келихами в руках друзів, сп'янілі обличчя, моменти, коли молодь бавилася «косячками» з травкою та інші компрометуючі фото), почало не тільки драгувати тих, хто на них опинився, а й стало серйозною перешкодою у кар'єрному зростанні. Адже фірми, державні установи і компанії перед тим, як наймати на роботу претендентів, відстежують їх життя і поведінку в кіберпросторі, зокрема у соціальній мережі Facebook, де вони представлені у різних іпостасях під своїм реальним іменем і прізвищем.

Опитування, проведене серед американських роботодавців 2009 р., показало, що 35% компаній відхилили претендентів на посади через інформацію, знайдену про них у соціальних мережах. Перша причина відмови: «розміщення провокативних фотографій чи недостойної інформації» [2, с. 276]. Те саме ввели у практику й університети, оскільки віковий ценз доступу у Facebook знизився до 13 років. Під час вступних кампаній члени приймальних комісій в університетах та коледжах тепер також перевіряють соцмережі.

М.Цукерберг є переконаним сповідачем «відкритого прозорого світу». Він вважає, що, відкрито визнаючи свою сутність і однаково поводячись із усіма друзями, «ми творимо здорове суспільство». Але з часом зростає кількість людей, якій здається, що оприлюднення приватної інформації на Facebook стає надмірним. Як свідчить Кірпатрік, «Цукерберг теж не вірить у тотальну відкритість. Він не лише про конфіденційні зустрічі у своєму профілі» [2, с. 274]. Але реальна політика його компанії доводить, що вона змушує користувачів ділитися власними даними, хоча наголошує тільки на тому, що їй «вдається створити безпечнішу, надійнішу версію Інтернету, де люди свідомі наслідків своїх вчинків, де вони послуговуються справжніми іменами».

Зовнішні експерти не підтримують ці міркування Цукерберга. Один з них – Марк Ротенберг, виконавчий директор Центру електронної приватності інформації (EPIC) і досвідчений «сторожовий пес Інтернету», який пише, що з кожним роком Facebook створює дедалі більше перешкод на шляху захисту приватності користувачів... Вони позбавлені можливості просто контролювати приватність інформації, а сам Facebook, попри переконання і сповідування прозорості, не надто прозоро показує, що він робить з нашою інформацією.

Порушення конфіденційності з боку Facebook шкодить не тільки абітурієнтам та випускникам університетів. Велику загрозу становить він для політиків та офіційних осіб вищого рангу, оскільки може зруйнувати їх кар'єри. Так, «політичний кандидат з канадського Ванкувера зняв свою

кандидатуру, коли в газеті з'явилася фотографія, де двоє людей натягують його труси. Йона Фавро, спічрайтера Барака Обама, публічно засудили, коли в блогі з'явилася фотографія, на якій він на одній з вечірок має груди картонної Гіларі Клінтон. На Facebook знімок вивісив хтось із друзів...». Можливо, Б. Обама думав саме про інцидент з Фавро, виступаючи перед старшокласниками у Вірджинії навесні 2009-го: «Будьте обережні з тим, що ви розміщуєте на Facebook, – попередив він, – оскільки в еру You Tube все, що ви робите, колись може неочікувано вигулькнути на поверхню. А поки ви молоді, ви робите багато дурниць».

З розвитком соцмережі дедалі гостріше постають проблеми конфіденційності. Від її прозорості постраждали люди, посада яких вимагає таємниці. Так, після того, як у Великій Британії в середині 2009 р. оголосили, що сер Джон Соерс очолить управління контррозвідки, Таємну розвідувальну службу (колись відому, як MI 6), газета Daily Mail знайшла публічні фотографії його з дружиною, розміщені нею на Facebook. Там були знімки зі свят, зображення друзів сім'ї й подробиць про те, де він жив і чим займався.

Як приклад знаменитості світового масштабу, яка порушила модель Facebook, можна назвати Біла Гейтса, який заклав свій особистий профіль на цій соцмережі на початку 2008 р.

Отже, ще одна дилема: люди прагнуть скрізь поширювати особисту інформацію, набувати популярності, але при тому хотіли б бути захищеними від неочікуваного розголошення, яке може їм завдати шкоди. Проблема у тому, що нашкочити небажаним розголошенням може тільки людина, яку користувач додав у «друзі», – таке собі «дружнє порушення приватності». Ось чому останніми роками у Сполучених Штатах, щоб на сайті не з'являлися провокативні фотографії, на університетських вечірках заборонено користуватися фотоапаратом, а в деяких закладах є навіть спеціальні темні кімнати, де ніхто не може зафіксувати розпивання алкоголю чи куріння трави. З іншого боку, такі застережні заходи примушують замислитися: чи насправді Facebook сприяє розвитку «прозорого відкритого суспільства», якщо стають потрібні «темні кімнати» для втаємничення не найкращих людських проявів? Чи не призводить це натомість до вкорінення подвійних стандартів моралі?

Початкове призначення Facebook як місця, де можна знайти своїх друзів з реального світу, постійно відсувалося на узбіччя. Важлива віха у розвитку цього сайту – поява сторінок компаній (а не друзів). Тепер їхнє оновлення з'являється у стрічці новин поряд із новинами від друзів. Як би не намагалися маркетологи з Facebook позитивно схарактеризувати цей крок, очевидним є одне – комерціалізація, монетизація компанії. Вона отримує величезні прибутки саме завдяки рекламі – єдиному шляху стати справжньою бізнес-компанією. Завдяки цьому Facebook перетворилася на одне з найкращих рекламних середовищ сучасності. До того ж інформація, яку вона має про своїх користувачів, – «золота жила» для створення

таргетингової реклами. Саме ці стратегії дали змогу Facebook спокійно пережити глобальну фінансово-економічну кризу 2008 р. і стати публічною компанією.

Могутність Facebook, її потенціал і амбіції щодо контролю над користувачами й платформою зонайменше такі самі, як були колись у Microsoft, але Facebook контролює власну платформу більше, ніж Microsoft. «Facebook може натиснути кнопку і вимкнути вас. Усіх вас. Будь-коли» [2, с. 446]. Якщо дивитися з радикального погляду, Facebook може перебрати на себе ключові функції урядів. Кіппатрік наводить слова Ю.Мільнера, російського інвестора компанії: «Facebook Connect – це загалом ваш паспорт – ваш онлайнвий паспорт. Паспорти видає уряд. Тепер з'явилися ще одна інституція, яка цим займається. Так народжується конкуренція. Але хто сказав, що видавати паспорти конче має уряд? Ми просто перейдемо до глобального громадянства». Питання в тому, чи всі користувачі Facebook прагнуть мати глобальне громадянство? Чи це кінцева мета М.Цукерберга, який з початку створення Facebook був більше зацікавлений у зростанні кількості користувачів, ніж у зростанні прибутків? Чи зацікавлені уряди країн світу делегувати Facebook свої повноваження? Адже, коли одна приватна компанія глобального масштабу володіє інформацією про переважну більшість населення Землі, чи це не ознака її м'якого панування (монополії на владу) в сучасному світі панування, багато з ефектів якого нікому, крім Марка Цукерберга не відомі, а, може, навіть, і йому?

Мабуть-таки, ці глобальні ефекти Марк Цукерберг добре знає. На 2015 р. його статок складав 33,4 млрд. дол. США. Зміни за рік додали йому 3,4 млрд. дол.. За рейтингом Forbes він займає 16 місце серед найбагатших людей планети. Засновник і гендиректор Facebook продовжує вести компанію до ринкових злетів, хоча для частини молодшої аудиторії соціальна мережа поступово стає анахронізмом. Дохід Цукерберга 2014 р. виріс на 58 % завдяки мобільній рекламі. Аудиторія компанії – біля 1,4 млрд. чоловік у всьому світі, які дивляться в день 3 млрд. відеороликів. Ще 300 млн. користувачів акумулюють фотоаплікацію Instagram, а 700 млн. використовують месенджер WhatsApp, який був придбаний 2014 р. за рекордні 19 млрд. дол.

Куди ж подівся юний Марк, який мріяв про прозорий Інтернет та про відсутність реклами у створеній ним соціальній мережі? Безжалюї закони ринкової конкуренції привели його до пулу маленької групи величезних Інтернет-компаній, де він опинився у лідерах.

Ден Гілмор в статті «Нові редактори Інтернету» запитує: «Хто дав їм таку владу? Ми з вами. Якщо ми не заберемо те, що віддали, і що в нас віднімають – ми це заслужили: концентрацію медійної влади, яка завдаватиме шкоду, і може повністю забрати в нас зміст нашої традиційної свободи вираження» [4].

Оже, складна ситуація із збереженням прайвесі у соціальних мережах та при користуванні Інтернет-пошуковиками, а також інтерактивними

мультимедіа-додатками, ставить складні запитання як перед творцями Інтернету, так і перед глобальною Інтернет-спільнотою: як зберегти право на свободу слова, право на комунікацію у глобальній громадській комунікаційній сфері, уособленням якої сьогодні великою мірою є Інтернет, як не перетворитися на матеріал для спостереження, аналізу та використання різними інституціями – від спецслужб до маркетологів та рекламодавців.

Таким чином можна сказати, що введення механізмів спостереження у серцевину глобальних диджитальних комунікацій серйозно загрожує правам людини у диджитальному еру. **Всі нові форми децентралізованої влади відбивають фундаментальні зсуви структури інформаційно-комунікаційних систем у модерних суспільствах.** І кожен крок у цьому напрямі повинен бути розглянутий і широко, і глибоко, і транспарентно.

Використані джерела та література:

1. Как повысить безопасность ваших фотографий в «облаке» («Atlantico», Франция) [Electronic resource] – Mode of access: inosmi.ru, 4 сентября 2014, № 11673300
2. Кірпатрік Д. Ефект Facebook. Внутрішня історія компанії, що об'єднує світ / Д. Кірпатрік. – К.: Темпора, 2013. – 488 с.
3. Федеральные власти и Yahoo [Electronic resource] – Mode of access: Russian-bazar.com, 12 сентября 2014, № 1175498.
4. Gillmor D. New Internet Editors / D.Gillmore // The Atlantic. – 2014. – 24 August.
5. Internet and Surveillance / Ed. By C. Funch, K. Boersma, A. Albrechtslund and M. Sandoval. – New York : Routledge, 2011. – 332 p.
6. What is Social Networking? [Electronic resource] – Mode of access: <http://www.whatissocialnetworking.com>

УДК 316.774 : 32.019.51+316.722(477)

Метельова Т.О.,
*кандидат філософських наук,
доцент, провідний науковий співробітник,
заступник директора з наукової роботи
ДУ «Інститут всесвітньої історії НАН України»*

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В КОНТЕКСТІ ЄВРОПЕЙСЬКИХ ЗДОБУТКІВ: ДОСВІД МИНУЛОГО І ПОТОЧНІ ЗАВДАННЯ

У статті аналізується європейський досвід збереження і посилення національної ідентичності громадян країн-членів ЄС та роль у цьому інформаційно-культурних чинників. Розглянуто конститутивне значення культурно-ціннісного складника інформаційних потоків для формування особистісних ідентифікацій. На матеріалах соціологічних досліджень доведено факт функціонування в Україні двох територіально локалізованих ціннісних систем, показано використання ціннісного розколу держави для