УДК 007:304:004.6:004.7

А. Е. Куля

ГЛОБАЛЬНЕ СТЕЖЕННЯ ЯК СИНДРОМ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

У статті подано системний аналіз фактора глобального стеження в суспільстві. Розглянуто основні характеристики різновидів інформації, що збирається негласними засобами та в електронних мережах. Розкрито питання законності та морально-етичного аспекту втручання в приватне життя людини. Зроблено акцент на смартфоні як головному засобі збору інформації про індивіда. Підкреслено, що діяльність спецслужб нерідко пов'язана з неетичним збором інформації та втручанням у приватне життя як перших осіб держав, так і пересічних громадян.

Ключові слова: *глобальне стеження, АНБ, Сноуден, спецслужби, інформація, метадані, приватність, смарфтон.*

І. Вступ

Стрімкий розвиток інформаційних технологій та розповсюдження соціальних комунікацій відкривають небувалі можливості роботи з інформацію. Продукувати, передавати або збирати дані сьогодні легше, ніж будь-коли, і ключову роль у цьому відіграють технічні засоби. Інформаційне суспільство активно нарощує потреби в споживанні інформації та комунікації, усе більше інтегруючись у медіа. Це дає значні переваги: надзвичайна кількість різноманітних сервісів полегшує повсякденне життя, спрощує робочий процес, створює унікальні можливості для розваг, дає змогу оптимально розподіляти ресурси. Але зворотний бік – масштабний збір особистих даних компаніями-розробниками, який нерідко відбувається без відома користувачів. Причиною називають покращення сервісу продукції та створення цільової реклами – індивідуальне формування переліку пропонованої продукції, враховуючи потреби, смаки та переваги індивіда. Але безневинний, на перший погляд, збір даних має досить розмиті межі з втручанням у приватне життя.

Ще більший резонанс має діяльність спецслужб, які, з одного боку, упроваджують контроль для запобігання тероризму, а з іншого – формують усеохопну мережу глобального стеження, де має місце жорстке порушенням як особистого простору людини, так і міжнародних домовленостей, коли йдеться про електронну розвідку.

Глобальне стеження, коли приватність мертва та всі шпигують за всіма, – це побічне явище розвитку інформаційного суспільства та новітніх соціальних комунікацій, які роблять досяжними будь-яке місце та будь-якого індивіда по всьому світу.

Проблема глобального стеження постала відносно нещодавно, тож на сьогодні існує доволі незначна кількість наукових досліджень відповідної проблематики. Проте тема набула широкого розголосу в ЗМІ. Провідні телеканали всього світу зробили цикли програм, присвячені порушенню конфіденційності та втручанню в приватне життя, зокрема досліджували й аналізували законні, морально-етичні та технічні аспекти. Так, варто відзначити цикл документальних фільмів «Америка контролює всіх» («America's Surveillance State») журналіста Девіда Ньюмена. Чимало статей було опубліковано й у провідних газетах. Зокрема, «The Guardian» та «Washington Post» найпершими почали публікувати розгромні матеріали про незаконну діяльність АНБ. Не можна лишити поза увагою численні інтерв'ю Едварда Сноудена, де він пояснює всі принципи роботи «машини стеження».

ІІ. Постановка завдання

Мета статті – дослідити одну з нагальних проблем суспільства – захисту приватного життя та конфіденційності в умовах стрімкого розвитку електронних програм і заходів, що можуть послужити шпигунським цілям.

ІІІ. Результати

Питання глобального стеження, беззаперечно, набуло небувалого резонансу з приголомшливими викриттями Едварда Сноудена – колишнього співробітника Центрального розвідувального управління та Агентства національної безпеки США. Він відкрив правду про те, що вищезазначені відомства порушують численні правила недоторканності приватного життя людини й ведуть масштабний шпіонаж за першими особами світу, серед яких і союзники Сполучених Штатів Америки. Зокрема, заява Сноудена відкрила те, що АНБ стежило за 122 зарубіжними лідерами, прослуховувалися дзвінки 35 лідерів, у тому числі приватні бесіди канцлера Німеччини Ангели Меркель. «Для Німеччини це неприйнятно, що мобільний телефон нашого федерального канцлера був предметом наглядової діяльності наших американських партнерів. Для нас

шпигунство за близькими партнерами є абсолютно неприйнятним», – відреагували тоді в німецькому уряді [8, timecode 13:43].

Шокуючі статті із засекреченими документами були опубліковані 5 червня 2013 р. у газетах «The Guardian» та «Washington Post», а згодом у мережі з'явилось і резонансне інтерв'ю самого Сноудена, на той час він уже перебував у Гонконзі. «Америка – це принципово хороша країна, – засвідчив він тоді, пояснюючи причини свого вчинку, – у нас є хороші люди, у них правильні цінності, ми хочемо робити правильні речі. Але структури влади працюють на власне винищення, розширюючи свої можливості за рахунок громадських свобод» [11].

Скандал умить розлетівся по всьому світу. Голови держав, передусім, ті, за якими шпигували, заявили про неприпустимість подібної політики, а громадськість вийшла на вулиці з протестами. Так, 26 жовтня 2013 р. у Вашингтоні пройшла масштабна акція, покликана зупинити глобальне стеження. На транспарантах рясніли надписи «Дякуємо, Едварде Сноудену» та «Скажи «Ні» порушенню конфіденційності!». Незабаром такі самі акції пройшли в Європі, Азії, Новій Зеландії. У Берліні зародився радикальний рух під назвою «Camover» («Кінець камерам»), члени якого – здебільшого молоді люди спортивної статури – під гасла «Виколи очі системі» здійснювали численні акти вандалізму, руйнуючи камери спостереження в громадських місцях [7]. Таким способом активісти руху боролись за недоторканність особистого життя.

Тож як глобальне стеження пов'язане із соціальними комунікаціями? Якими є найновіші його прояви і які зв'язки воно має з інформаційними потребами людини?

Для пошуку відповідей на ці питання необхідно розібратись у причинах формування цього явища. Передумови появи глобального стеження формувались ще з 1990-х рр. зі стрімким розвитком телекомунікаційних технологій, але значного поштовху, беззаперечно, дали події 11 вересня 2001 р. Одразу ж після трагічних терактів уряд США створив надсекретне розвідувальне відомство, покликане займатися радіоелектронним перехопленням, простіше кажучи, електронним стеженням. Програма отримала істотне фінансування. Новітні інформаційні технології стали застосовувати як інструменти збору та накопичення колосальних обсягів інформації, причому не тільки державного, ділового, а й конфіденційного характеру. Ці технології забезпечили процесам спостереження, шпигунства, стеження всюдисущість і повсюдність [1]. Борці за свободу почали говорити про відродження «Великого брата», широко описаного у відомому романі-антиутопії Дж. Оруела «1984», але уряд США настійливо переконував, що програма спрямована виключно на боротьбу з тероризмом, і втручання в особисте життя відбувається виключно з дозволу суду.

Таким чином, у США, а згодом за тим самим шаблоном і в інших провідних країнах світу виникла тотальна система спостереження за людиною. Якщо раніше джерела інформації існували окремо, у різних органах і організаціях, то тепер їх можна зібрати разом, аналізуючи та складаючи інформаційний портрет кожної людини. Для формування картини використовують як особисте листування та його історію, так і соціальну активність у соціальних мережах та відеозаписи з камер спостереження. «Я міг бачити все: яку книгу ви шукали на Amazon минулого тижня, з ким ви розмовляєте, хто є вашими друзями у Facebook, ваші SMS та електронні листи. Я міг встановити те, що називається "цифровими відбитками", які дають мені змогу відстежувати, де ви були в Інтернеті, з ким говорили, навіть якщо ви при цьому використовували анонімайзери», – зазначав Едвард Сноуден в ефірі Новозеландського шоу «Момент правди» [9].

Таким чином, здійснилась мрія спецагентів. Віднині немає потреби встановлювати живе стеження за людиною, як це відомо нам із серіалів кримінальної тематики; не потрібно підкидати їй жучки в кращих традиціях шпигунів американського та британського кінематографу; немає необхідності вживлювати чіпи для виявлення дислокації, як описано в науковій фантастиці. Головний шпигун людини – її власний смартфон, на якому вона добровільно розміщує всю інформацію про себе. Можливо, саме на це й була зроблена ставка розвідувальними організаціями ще на початку 1990-х рр., коли мобільний телефон, будучи, по суті, напрацюванням спецслужб, потрапив у широке застосування, як свого часу відбулось і з Інтернетом.

І дійсно, сьогодні складно знайти людину, яка б не брала телефон із собою всюди, де вона працює, розважається або мандрує. З одного боку, це, безумовно, проривний результат розвитку технологій та соціальних комунікацій, адже сьогодні саме смартфон є інструментом соціальної активності людини, але з іншого – він приховує в собі численні ризики. Маючи мультимедійний фіксуючий пристрій у себе в кишені, людина наражає на небезпеку своє приватне життя. Мобільний знає про користувача більше, ніж будь-яка установа на планеті, він збирає всю інформацію про покупки, електронну пошту, місцезнаходження, особисті вподобання, і ці дані вразливі до того, щоб опинитись у руках зловмисників.

Із цього приводу досить доречну думку висуває молодий голландський хакер Ентоні ван дер Меєр, який здебільшого відомий у зацікавлених колах своїм короткометражним документальним фільмом «Знайти мій телефон» («Find My Phone») [10]. У загальних рисах сюжет фільму розповідає про те, як молодик встановив шпигунську програму на свій смартфон і організував його викрадення, щоб дізнатись, який спосіб життя веде типовий крадій смартфонів – він відстежував

всю історію листування крадія, кому той дзвонить, про що говорить, які фотографії робить, та інші персональні характеристики. На думку ван дер Меєра, прогресивне населення планети цілком усвідомлює, що комп'ютери досить уразливі для взламування та викрадення з них інформації, але поки що мало хто замислюється над тим, що так само, як і комп'ютер, хакери можуть взламати і смартфон, на якому значно більше особистої інформації. «Коли мій особистий телефон вкрали, я усвідомив, що хтось має доступ до всієї моєї особистої інформації, – зазначає він. – І ще більше шокує, коли телефон взламують. Тож метою мого експерименту було показати, наскільки легко взламати смартфон і скільки інформації ви можете здобути, зробивши це; показати, наскільки це насправді небезпечно» [10].

Отже, інформація про індивіда збирається відусюди. Найбільше – з його власного смартфона, додатково – з електронних ресурсів та зовнішніх засобів фіксації. Специфіка глобального стеження полягає в тому, що це складна й багаторівнева процедура. Зокрема, крім класичних даних (small data), накопичуються ще й метадані (metadata).

На цьому аспекті варто зупинитися окремо. Класичні, або малі дані (small data), – це власне та базова традиційна інформація, яку заповнюють в анкеті. До неї належить ім'я, вік, стать, конфесійна приналежність, політичні погляди тощо. На сьогодні певна частина цієї інформації міститься мінімум у шести базах даних: паспортна система, бази даних податкових органів, списки органів соціального й медичного забезпечення, освіти, списки виборчих комісій. До цього переліку варто додати дані перепису населення, бази даних військовозобов'язаних громадян і автомобілістів тощо.

Метадані ж відрізняються зовсім іншим значенням та інформаційною цінністю. У більшості літературних джерел метадані визначають як інформацію про дані, або інформацію про інформацію. Тобто, по суті, дані, які характеризують інші дані [3]. Усвідомити, як це працює на практиці, нам допоможе приклад, запропонований вищезгаданим хакером Ентоні ван дер Меєром: «Коли ви комусь дзвоните – метаданими буде не сам дзвінок, не те, що говориться у розмові, а вся інформація навколо нього. Якщо я дзвоню вам, я набираю ваш телефонний номер, тож це телефонний номер. Я дзвоню вам у певний час, я завершую розмову у певний час, тож це тривалість розмови, ви знаєте, з ким була розмова, але не знаєте, про що. Це не тільки телефонні дзвінки, це, і GPS локації, текстові повідомлення – не те, що написано в повідомленні, а кому воно адресоване і коли саме».

Саме збором метаданих тривалий час і виправдовувались найперші спецслужби світу, коли їх звинувачували у втручанні в приватне життя людей. Але, тим не менше, безпосередньо за метаданими можна зробити не менш точні характеристики людини, ніж прослуховуючи зміст її розмов. «Якщо я щотижня дзвоню на певний номер у певний час, і цей номер належить жінці похилого віку з таким самим прізвищем, як у мене, це, вірогідно, моя бабуся», – зазначає ван дер Меєр.

Едвард Сноуден у своїх інтерв'ю теж виокремлював метадані, навіть більше – надав їм більшої переваги, ніж традиційній інформації: «Метадані дуже корисні. Як аналітик я волію переглядати метадані, а не контент, тому що вони швидші, вони легкі в управлінні, вони не брешуть. Якщо ми прослухаємо ваш телефонний дзвінок, ви можете говорити не за темою, говорити, використовуючи кодові слова, але, якщо я дивлюсь на метадані, я можу побачити, який номер дзвонив на який номер, який комп'ютер спілкувався з яким комп'ютером» [9].

Ще одним аргументом на користь істотного значення метаданих є той факт, що у травні 2014 р. засновник АНБ Майкл Хейден шокував аудиторію Вашингтона, коли сказав, що АНБ використовує метадані, щоб вбивати людей [8].

Отже, світові спецслужби, зокрема АНБ, збирають неймовірно великі обсяги інформації різних форм. Таку можливість їм забезпечує технологічний процес. Як вважає Дж. Ульмен, колишній керівник групи дослідників Стенфордського університету, створення цифрового досьє на всіх американців вимагатиме не більше пари терабайт (терабайт = 1024 гігабайти) добре організованої інформації. Із цим завданням цілком можуть упоратися сучасні комп'ютери й телекомунікаційні лінії [4]. Але насправді обсяг детальної інформації, що збирається, не піддається людській уяві. Сервери зберігання інформації Агентства національної безпеки США займають десятки гектарів території і являють собою по суті величезні флеш-накопичувачі інформації, що чекає свого часу і може бути використана в будь-який момент.

АНБ – це найбільша, найдорожча й найкраще обладнана шпигунська організація в світі. Вона фільтрує мільйони телефонних дзвінків на годину. Комп'ютери, які коштують десятки мільйонів доларів і скеровані програмами з дивними назвами на зразок «Призма» або «Чорна вдова», запрограмовані стежити за сотнями тисяч імен. Вони працюють на спеціальних швидкостях, про які більшість людей і не чула, а саме сотні терафлопів, які можуть проводити сотні трильйонів операцій за секунду.

Значний обсяг даних збирають і провідні інтернет-компанії, такі як Google, Facebook, Apple, Microsoft, і, за словами Едварда Сноудена, усі вони працюють з АНБ та надають прямий доступ до змісту всіх систем, які люди використовують для соціальної комунікації, до сховищ даних, до

інформації, що зберігається в «хмарі», і навіть до особистих привітань з Днем народження. Користувач дає згоду на це, підписуючись під угодою використання програми, не вчитуючись у численні пункти, адже це може зайняти цілі тижні. Таким чином, відбувається формально законний, але, по суті, негласний збір інформації через соціальні комунікації.

Із цього приводу в Інтернеті активно поширюється констатація того, що приватність мертва. І справді, треба визнати, що сьогодні практично неможливо повністю захистити свою конфіденційність. Технічний прогрес досяг такого рівня, що за людиною можуть стежити навіть через вебкамеру її персонального комп'ютера, телевізора, керуючи її технікою абсолютно дистанційно. Більше того, звичайні звукові динаміки можна налаштувати на запис звуку, а не тільки на його відтворення. У XXI ст. на заміну агентам-шпигунам прийшли хакери, головна зброя яких – не жучки та технічні пристрої, а програмний вірус, який можна підхопити в мережі в один клік – достатньо перейти за зараженим посиланням, і через секунду кібер-шахрай, або системний адміністратор компанії, не тільки бачить користувача, а й чує.

Частина суспільства має позицію «не робіть нічого поганого, і вам нічого боятися», а інша частина, до якої, зокрема, належить і Едвард Сноуден, категорично із цим не погоджується. «Я не хочу жити у світі, де все, що я говорю, все, що я роблю, кожен вираз творчості, кохання, дружби – все записується. І це не те, що я хотів би підтримувати, будувати, жити в цьому», – зазначив Сноуден у своєму першому інтерв'ю [11]. Право громадян на таємницю власного життя – норма, закріплена в конституції будь-якої розвиненої країни світу, зокрема в Україні.

З одного боку, ми не знаємо, скільком злочинам чи терористичним актам запобігли завдяки використанню сучасних технологій та алгоритмів, а з іншого – підтримання глобальної машини стеження має великі ризики, адже технологія, якою шпигують за злодіями й терористами, може бути використана для шпигування за звичайними громадянами. Зрештою, враховуючи сучасні реалії, визначення злочинця може залежати від того, на якого політика чи олігарха працюють нібито державні організації, які підозрюють у злочині. У майбутньому будь-хто може бути навмисно або випадково стати тими зловмисниками, яких підозрюють у підготовці терористичного акту.

Цілком логічно постає питання: як же захиститись від тотального переслідування та спроб втрутитись у приватне життя? По-перше, доведеться прийняти це як особливість сучасності: щодня приватності буде все менше, і життя індивіда стає дедалі доступнішим як для розвідувальних організацій, так і для віртуальних зловмисників. По-друге, найбільш оптимальним, на нашу думку, буде помірне вирішення питання, і скерування його в нейтральне поле. Суспільство має працювати над технологіями, які допоможуть захистити конфіденційність, має голосувати за політиків, які поважають приватне життя, має підтримувати тих громадських діячів, які популяризують політику збереження приватності. Чималу роль у цьому мають відіграти й соціальні комунікації, адже завдяки їм досить легко надати розголосу будь-яким порушенням у сфері захисту інформації, привести до відома відповідні органи. Більшість теоретиків та журналістів, що досліджують проблему глобального стеження, підкреслюють, що тільки підзвітність, прозорість і демократичний контроль громадськості над установами, які контролюють технічні алгоритми, дадуть змогу бути впевненими, що ніщо не робиться в обхід закону та етики. Радикальні ж дії, на зразок руйнування камер спостереження, не є ґрунтовним вирішенням проблеми, а є лише засобом привертання уваги, який має занадто високу ціну.

IV. Висновки

Інформаційне суспільство дійшло тієї точки свого розвитку, коли прогрес починає приносити забагато ризиків. Соціальна потреба людини ділитися із суспільством своїми досягненнями, способом життя та талантами за допомогою соціальних комунікацій грає проти збереження приватності. Кожний індивід стає абсолютно прозорим для зловмисників та розвідувальних організацій. І якщо збір даних та формування характеристик індивіда відбувається неетичним шляхом, тобто без відома людини, то це приховує в собі багато ризиків, таких як компромат, шантаж, вербування до терористично орієнтованих угруповань. Проаналізовані джерела дають змогу припустити, що тероризм – це лише прикриття, яким виправдовуються спецслужби. Насправді ж глобальне стеження може бути боротьбою за економічний і соціальний контроль. Експансія розвідувальних систем відбувається настільки швидко й активно, що суспільство не встигає до них пристосуватися. Звідси – відсутність будь-якого морально-правового регламенту навіть у разі застосування екстремальних форм. Фактор тероризму спрацьовує як шлагбаум, що відкриває дорогу тотальним розвідувальним діям. Процес «стежити за всім, всюди і весь час» став знаковою подією сучасної епохи. При цьому важливо мати на увазі, що інформація, що отримується таким чином у необмеженому обсязі й зосереджена в одному місці, – це прямий шлях до тоталітаризму, тож не зайвим буде замислитися над питанням: до якої з описаних у художніх романах антиутопій ми йдемо?

Ця стаття не вичерпує всіх аспектів порушеної проблеми, що потребує подальших досліджень.

Список використаної літератури

1. Акопян Д. Эпоха тотальной электронной слежки [Электронный ресурс] / Д. Акопян, А. Еляков // Скепсис : научно-просветительский журнал. – Режим доступа: http://scepsis.net/library/id_2078.html.
2. Брандман Э. М. Глобализация и информационная безопасность / Э. М. Брандман // Философия и общество. – 2006. – № 1. – С. 34.
3. Метадані [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/%D0%9C%D0%B5%D1%82%D0%B0%D0%B4%D0%B0%D0%BD%D1%96.
4. Роговский Е. А. Распространение INT-технологий в Соединенных Штатах / Е. А. Роговский, Б. Э. Верпаховский // США и Канада. – 2004. – № 4. – С. 105.
5. Роговский Е. А. Геопространственная разведка США / Е. А. Роговский // США и Канада. – 2004. – № 8. – С. 125.
6. Убстер Ф. Теории информационного общества / Ф. Убстер. – Москва, 2004. – С. 204.
7. CAMOVER 2013 [Електронний ресурс]. – Режим доступу: https://www.youtube.com/watch?v=9GCsd2TJKjQ.
8. America's Surveillance State 2 (Inside The NSA: How Do They Spy?) [Електронний ресурс]. – Режим доступу: https://www.youtube.com/watch?v=V5OiXyQdyWU Timecode 13.43; 14.51.
9. Edward Snowden's Latest Interview on New Zealand [Електронний ресурс]. – Режим доступу: https://www.youtube.com/watch?v=7uzz34c3odQ Timecode 11.33.
10. Short Film: Find my Phone – Subtitled [Електронний ресурс]. – Режим доступу: https://www.youtube.com/watch?v=NpN9NzO4Mo8.
11. SNOWDEN INTERVIEW PART II HONG KONG [Електронний ресурс]. – Режим доступу: https://www.youtube.com/watch?v=1jfeqzhe3qk.

Стаття надійшла до редакції 15.02.2017.

Куля А. Э. Глобальная слежка как синдром информационного общества

В статье приводится системный анализ фактора глобального слежения в обществе. Рассматриваются основные характеристики разновидностей информации, собирающейся негласными средствами и в электронных сетях. Раскрывается вопрос законности и морально-этических аспектов вмешательства в частную жизнь человека. Делается акцент на смартфоне как главном средстве сбора информации об индивиде. Подчеркивается мысль, что деятельность спецслужб нередко связана с неэтическим сбором информации и вмешательством в частную жизнь как первых лиц государств, так и рядовых граждан.

Ключевые слова: *глобальная слежка, АНБ, Сноуден, спецслужбы, информация, метаданные, приватность, смартфтон.*

Kulia A. Mass Surveillance as a Syndrome of the Information Society

Research methodology. *In order to determine mass surveillance factor the main features of collecting of personal information were implied. Moral and legal sides of surveillance were under consideration during the process of analysis.*

Results. *The information society has reached a point of development where progress is beginning to bear too much risk. Social need of humanity to share with the public its achievements, talents and lifestyle through social communication plays to preserve privacy. Each individual is completely transparent to the intruders and intelligence organizations. If data collection and formation characteristics of the individual is going on unethical way, without the knowledge of the person, it can have many risks, such as dirt, blackmail, recruitment to terrorist-oriented groups. Analyzed sources suggest that terrorism – is just a cover, which justified the special services. In fact, the global surveillance – may be a struggle for economic and social control.*

Expansion of intelligence system is so quick and active that society has no time for them to adapt. Hence – the lack of any moral and legal regulations even in case of extreme forms. Terrorism factor works as a gate that opens the way for pervasive intelligence actions. The process «to follow everything, everywhere and all the time» has become a landmark event of the modern era. It is important to bear in mind that the information obtained in this way in unlimited quantities and is concentrated in one place – a direct path to totalitarianism, so it is useful to ask: «to which of described in fiction novels dystopias do we go?".

Novelty. *The article studies one of the most important problems of society – the protection of privacy and confidentiality with the rapid development of electronic programs and activities that can serve as espionage targets.*

The practical significance. *The results of the investigation can be used for further study of saving privacy and development of electronic techonologies.*

Key words: *global tracking, NSA, Snowden, special services, information, meta-data, privacy, smartphone.*