5. Положення про громадське спостереження за проведенням зовнішнього незалежного оцінювання : затверджене Наказом Міністерства освіти і науки, молоді та спорту України 25.11.2011 № 1354 (у редакції наказу Міністерства освіти і науки України 15.01.2016 № 20). [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/z1481-11

6. Галунько В.В. Адміністративне право України в сучасних умовах (виклики початку XXI століття) : [монографія] / [В.В. Галунько, В.І. Олефір, М.П. Пихтін та ін.]. – Херсон : Херсонська міська друкарня, 2010. – 378 с.

7. Коломоєць Т. Адміністративна правосуб'єктність юридичних осіб як основа їх адміністративно-правового статусу: теоретико-правовий аналіз / Т. Коломоєць, П. Лютіков // Право України. № 3-4/2013. – С. 385-395.

8. Статут Всеукраїнської громадської організації «Відкрита освіта». [Електронний ресурс]. – Режим доступу: http://openosvita.org/about/statut.php

9. Статут ГО «Київський освітній центр «Простір толерантності». [Електронний ресурс]. – Режим доступу: https://www.prostir.ua/about/

10. Статут громадської організації сприяння розвитку освіти «Діалог». [Електронний ресурс]. – Режим доступу: http://uovmr.net.ua/

11. Хариш М.С. Недержавні громадські організації як складова частина суб'єктів адміністративного права України / М.С. Хариш // Наукові записки Львівського університету бізнесу та права. – 2013. – Вип. 11. – С. 29-31.

УДК 342.9:347.121.1

РІЗАК М.В.

ПРАКТИКА ЄВРОПЕЙСЬКОГО СУДУ З ПРАВ ЛЮДИНИ ЩОДО ГАРАНТУВАННЯ НЕДОТОРКАННОСТІ ПРИВАТНОГО ЖИТТЯ ПІД ЧАС ОБІГУ ТА ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Розглянуто передумови розвитку європейського законодавства у сфері обігу та обробки персональних даних; досліджено практику Європейського Суду з прав людини у цій сфері; охарактеризовано особливості обігу та обробки персональних даних у соціальних мережах та користувачів гаджетів на підставі судової практики; розроблено пропозиції щодо удосконалення національного законодавства у досліджуваній сфері.

Ключові слова: *персональні дані, безпека, обіг, обробка, Європейський Союз.*

В статье рассмотрены предпосылки развития европейского законодательства в сфере обращения и обработки персональных данных; исследована практика Европейского Суда по правам человека в этой сфере; охарактеризованы особенности обращения и обработки персональных данных в социальных сетях и пользователей гаджетов на основании судебной практики; разработаны предложения по совершенствованию национального законодательства в указанной сфере.

Ключевые слова: *персональные данные, безопасность, обращение, обработка, Европейский Союз.*

In article preconditions of European legislation on the treatment and processing of personal data; studied law of the European Court of Human Rights in this area; The features and treatment of personal data in social networks and users of gadgets based on jurisprudence; suggestions for improvement of national legislation in this area.

Key words: *personal data security, circulation processing, European Union.*

© РІЗАК М.В. – кандидат юридичних наук, помічник-консультант народного депутата України (Верховна Рада України)

Вступ. Забезпечення прав людини нерозривно пов'язане з гарантуванням безпеки обігу та обробки персональних даних, які становлять приватні відомості про конкретну особу. Новітні високотехнологічні розробки дозволяють збирати та поширювати інформацію у необмеженій кількості, спілкування вже позбавлено кордонів, на перший план виходять комп'ютери, мобільні телефони, планшети, безліч аксесуарів до них, що працюють на відповідному програмному забезпеченні та платформах, які використовують відомості про особу для її ідентифікації та зберігають ці відомості за допомогою хмарних технологій у різних країнах світу під різною юрисдикцією.

Постановка завдання. За таких умов класичне нормативно-правове регулювання обігу та обробки інформації виявилося неефективним, оскільки технологічний стрибок привів до зміни основоположних принципів поводження у цій сфері. Відтепер законодавство встановлює загальні правила, а судова практика, ґрунтуючись на основоположних принципах захисту прав людини, випереджає законодавство, оскільки на конкретних прикладах показує, як має застосовуватися та чи інша норма права.

Окремі питання у сфері безпеки обігу та обробки персональних даних досліджували такі вчені, як: Л.В. Борисова, В.М. Брижко, І.О. Вельдер, В.Д. Гавловський, В.С. Гербут, Р. Кірін, О.В. Кохановська, А.В. Кучеренко, А.М. Чернобай та інші. Проте, практика Європейського Суду з прав людини (далі – ЄСПЛ) щодо недоторканності приватного життя під час обігу та обробки персональних даних у соціальних мережах та з використанням сучасних гаджетів є малодослідженою, що обумовлює актуальність порушеної проблематики. Оскільки більшість громадян України так чи інакше застосовують у повсякденній діяльності гаджети та є користувачами соціальних мереж, це дослідження також є доволі своєчасним.

Метою статті є дослідження практики Європейського Суду з прав людини щодо гарантування недоторканності приватного життя у контексті безпеки обігу та обробки персональних даних. Для досягнення поставленої мети передбачалося вирішити такі завдання: розглянути передумови розвитку європейського законодавства у сфері обігу та обробки персональних даних; дослідити практику Європейського Суду з прав людини у цій сфері; охарактеризувати особливості обігу та обробки персональних даних у соціальних мережах та користувачів гаджетів на підставі судової практики; розробити пропозиції щодо удосконалення національного законодавства у зазначеній сфері.

Результати дослідження. Правила безпеки персональних даних, які застосовуються в Європі, встановлені двома міжнародними інструментами. Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних датується 1981 роком і була першим міжнародним документом, який запровадив юридично обов'язкові правила щодо безпеки персональних даних. Більшість європейських країн, включаючи Україну, є сторонами цього документа. Конвенція була доповнена у 2001 році Додатковим протоколом, який встановлює правила щодо органів нагляду і транскордонних потоків даних. Держави-члени Європейського Союзу також мають зобов'язання відповідно до Директиви ЄС «Про захист прав приватних осіб стосовно обробки персональних даних та про вільний рух таких даних» 1995 року, яка містить у цілому схожі, але більш деталізовані положення у порівнянні з Конвенцією. Тим самим відбувся швидкий розвиток інформаційних та комунікаційних технологій з часу прийняття цих інструментів, і відповідно сьогодні ведеться робота і Радою Європи, і Європейським Союзом з метою зробити інструменти з питань безпеки персональних даних більш придатними до реагування на виклики XXI століття [2, с. 167].

З часом законодавче регулювання забезпечення безпеки обігу та обробки персональних даних зіткнулося з проблемою правопорушень у цій сфері, що потребувало напрацювання відповідної юридичної практики, зокрема судової. Оскільки персональні дані безпосередньо стосуються приватного життя людини, то найбільшу цінність має практика Європейського Суду з прав людини.

В Узагальнюючій практиці ЄСПЛ підкреслює, що Інтернет, зважаючи на його здатність зберігати і передавати величезну кількість інформації, відіграє важливу роль у розширенні доступу суспільства до новин і поширенні інформації загалом. Підтримка інтернет-архівів є ключовим аспектом цієї ролі, і тому ЄСПЛ вважає, що такі архіви потрапляють під захист ст. 10 Конвенції [3, с. 14–15].

Існують різні види порушень європейського законодавства у сфері безпеки обігу та обробки персональних даних. Серед них можна виокремити незаконні збирання, обробку та поширення персональних даних, торгівлю базами зазначених даних, втручання у приватне життя шля-

хом заволодіння персональними даними людини тощо. Ці та інші негативні явища потребують протидії з боку держави та громадян. Кожна окремо взята форма правопорушення у цій сфері вимагає адекватної реакції суспільства, що тягне за собою удосконалення нормативно-правового регулювання відповідних відносин. Проте, оскільки розмежування приватного життя та потреб держави і суспільства чітко не здійснено у законодавстві, судова практика подекуди спирається на основоположні принципи правового регулювання зазначених відносин. Тому застосуванню підлягають такі принципи, як справедливість, співмірність, доцільність та інші.

Наприклад, у деяких випадках ЄСПЛ не визнає порушенням прав людини перевірку її сторінки у соціальній мережі. Так, позов румунського інженера щодо його звільнення за розміщення особистих повідомлень на сторінці у соціальній мережі Facebook у робочий час був відхилений ЄСПЛ. Судді його Малої палати зазначають, що роботодавець має право перевіряти, чи виконували працівники на робочому місці свої службові обов'язки і чи не використовували комп'ютер з особистою метою. Перевірка сторінки у соціальній мережі може вважатися втручанням в особисте життя, але судді ЄСПЛ вважають, що у цьому випадку перевірка виправдана. Наголошується, що румунського інженера звільнили у 2007 році, коли роботодавець перевірив його сторінку у Facebook і дізнався, що той використовував комп'ютер, аби листуватися зі своїм братом і дівчиною [4].

Як бачимо, у цьому разі, хоча і відбувалося порушення прав працівника щодо безпеки його персональних даних з боку роботодавця, сам працівник порушив трудові відносини першим. Крім того, позивач не зазнав шкоди через порушення безпеки обігу та обробки його персональних даних (негативні наслідки настали через невиконання ним трудових обов'язків та порушення трудової дисципліни).

Інше рішення ЄСПЛ у цій сфері стосується ситуації, коли 15 березня 1999 року невідома особа чи особи розмістили рекламне оголошення на сайті знайомств в Інтернеті від імені заявника, якому тоді було 12 років, без його відома. В оголошені згадувалися його вік та рік народження, давався детальний опис його фізичних характеристик, наводилося посилання на веб-сторінку, яку він мав на той час, де розміщувалися його фото, а також телефонний номер, який був правильний за винятком однієї цифри. У повідомленні стверджувалося, що заявник прагнув інтимних відносин з хлопцем його віку чи старшим, який би «показав йому, як це робиться». Заявник дізнався про оголошення в Інтернеті, коли отримав лист електронною поштою від чоловіка, який запропонував зустрітися і «тоді дізнатися, чого ти хочеш». Батько заявника звернувся до поліції з проханням ідентифікувати особу, яка розмістила оголошення, з тим, щоб пред'явити їй обвинувачення. Однак, постачальник послуг Інтернет відмовився розкрити особу володільця так званої динамічної IP-адреси, про яку йшлося, вважаючи себе зобов'язаним додержуватися вимог конфіденційності телекомунікацій, як це було визначено законом. Національні суди відмовили поліції зобов'язати інтернет-провайдера розкрити зазначену інформацію відповідно до ст. 28 Закону про кримінальні розслідування (Закон № 449/1987 зі змінами, внесеними Законом № 692/1997).

Особу, яка відповіла на оголошення на сайті знайомств та сконтактувала із заявником, було ідентифіковано через адресу її електронної пошти. Виконавчий директор компанії, яка надавала інтернет-послуги, не міг бути притягнений до відповідальності, оскільки у своєму рішенні від 2 квітня 2001 року прокурор установив, що строк давності для відповідного порушення сплив. Відповідним порушенням було порушення Закону про персональні дані (Закон № 523/99, який набув чинності 1 червня 1999 року). Якщо точніше, то постачальник послуг оприлюднив наклепницьке повідомлення на своєму веб-сайті, не перевіривши особу відправника [5, с. 78-79].

Як зазначає ЄСПЛ, порівняльний аналіз законодавства держав-членів Ради Європи показує, що у більшості країн існує спеціальний обов'язок постачальників телекомунікаційних послуг надавати комп'ютерні дані, у тому числі інформацію про абонента, у відповідь на запит слідчих або судових органів незалежно від природи злочину. Деякі країни мають лише загальні положення щодо надання документів та інших даних, які на практиці можуть розширюватися і містити також обов'язок подавати конкретні комп'ютерні та абонентські дані. Кілька країн ще не впровадили положення ст. 18 Конвенції Ради Європи про кіберзлочинність [5, с. 84].

З цього приводу Гельсінська фундація за права людини зауважила, що справа, яка розглядається, піднімає питання знаходження балансу між захистом приватності, честі та репутації (недоторканності приватного життя), з одного боку, і здійсненням свободи вираження поглядів, з іншого боку. Справа дає Суду можливість визначити позитивні обов'язки держави у цій сфері та у такий спосіб сприяти спільним стандартам щодо використання інтернету у країнах-членах. Інтернет є дуже особливим способом спілкування, і одним з основоположних принципів його вико-

ристання є анонімність. Високий рівень анонімності заохочує свободу слова та вираження різних ідей. З іншого боку, інтернет є потужним засобом для можливості наклепу чи образи людей або порушення їхнього права на приватність (недоторканність приватного життя). Через анонімність інтернету жертва порушення знаходиться у вразливому становищі. На відміну від традиційних засобів масової інформації, жертва не може легко ідентифікувати особу, яка зводить наклеп, через той факт, що можна заховатися за псевдонімом або навіть використати чуже ім'я [6, с. 10].

За рішенням ЄСПЛ, заявник був об'єктом оголошення сексуального характеру на інтернет-сайті знайомств. Інформацію про особу того, хто розмістив оголошення, неможливо було отримати від постачальника інтернет-послуг через законодавство, яке діяло на той час. Застосовність ст. 8 не заперечується: факти, які лежать в основі заяви, стосуються «приватного життя» – поняття, що охоплює фізичну та душевну недоторканність особи, з огляду на потенційну загрозу фізичному та душевному спокою заявника, до якої призвела оскаржувана ситуація, та на його вразливість через ранній вік. Хоча метою ст. 8 є насамперед захист особи проти свавільного втручання з боку державних органів, вона не лише зобов'язує державу утриматися від такого втручання: на додаток до цього первинного негативного зобов'язання можуть існувати позитивні обов'язки, які становлять ефективний захист приватного або сімейного життя. Ці обов'язки можуть містити вжиття заходів, спрямованих на забезпечення поваги до приватного життя навіть у сфері відносин осіб між собою. Існують різні способи забезпечення поваги до приватного життя, і суть обов'язку держави залежатиме від конкретного аспекту приватного життя, про який ідеться [5, с. 87].

ЄСПЛ частково задовольнив вимоги заявника, констатувавши факт порушення з боку держави та присудивши компенсацію у розмірі 3000 євро.

Слід звернути увагу, що надмірне регулювання та перевіряння інформації, розміщеної у мережі Інтернет взагалі та соціальних мережах зокрема, також створюють численні перепони на шляху до гарантування безпеки обігу та обробки персональних даних.

Наприклад, моніторинг соціальних мереж, як і моніторинг телефонних дзвінків, а також сервісів електронної пошти, вівся з 2010 р. Агенцією національної безпеки США (далі – АНБ) по так званих метаданих – тобто зводу найбільш загальних відомостей про людину; однак якщо такі дані поєднувалися з даними про телефонні дзвінки і трафік електронної пошти, то можна було отримати достатньо цілісну картинку про людину – де вона перебувала у той чи інший момент часу, чим займалася, куди збиралася їхати тощо. Активним моніторингом соціальних мереж та електронної пошти АНБ зайнялась з 2010 р., створюючи «гігантські колекції даних, щоб побудувати найскладніші системи соціальних зв'язків американців, виявляти їх контакти, місцеперебування на конкретний період часу, плани на майбутнє та інші персональні відомості». Тоді ж прийнято пакет законів, який формально дозволив АНБ вести моніторинг у значних обсягах, отримувати великі бази метаданих без будь-якої формальної звітності. Спочатку програма моніторингу соцмереж була спрямована саме на іноземних громадян, оскільки у США, якщо б програму було викрито, АНБ гарантовано отримала б тисячі позовів. Тим не менш, у відомстві знайшли спосіб шпигувати за місцевими громадянами – розвідка почала брати дані тільки з публічних джерел, а також дані, які були доступні службам економічної розвідки. Закон про діяльність АНБ було розроблено достатньо ефективно – саме відомство не втручалося у діяльність операторів соцмереж для одержання закритих даних, однак інші американські відомства, включаючи податкову службу, банки, постачальників телекомунікаційних сервісів та багатьох інших, без формальних запитів повинні були передавати в АНБ свої відомості, аби Агенція могла створювати цілісну картину щодо осіб, стосовно яких здійснюється спостереження [7].

У сучасному світі спостерігається тенденція щодо намагання різних спецслужб, організованої злочинності, хакерських груп встановити контроль над соціальними мережами, створити постійний безперешкодний та повний доступ до гаджетів користувачів з метою заволодіння інформацією. З цією метою розробляються нові технології, програмне забезпечення, безкоштовні додатки до мобільних операційних систем тощо. Уряди деяких країн фінансують такі проекти власних спецслужб, інші виділяють кошти на блокування певних інтернет-ресурсів.

Наприклад, згідно з Указом Президента України №133/2017 обмежувальні санкції відповідно до рішення РНБО передбачають заборону інтернет-провайдерам надання послуг з доступу користувачам мережі Інтернет до ресурсів сервісів "Mail.ru" (www.mail.ru) та соціально-орієнтованих ресурсів «Вконтакте» (www.vk.com) та «Одноклассники» (www.ok.ru). Також санкції введені проти ТОВ «Яндекс» (Москва) і «Яндекс.Україна», російських компаній розробників-антивірусів «Лабораторія Касперського» і «Доктор Веб» [8].

Одразу ж після цього національні оператори мобільного зв'язку, зокрема ТОВ «Лайфселл» [9] та Київстар [10], запропонували своїм абонентам нові послуги щодо підключення до інших соціальних мереж, пристосувавши тарифи до нових умов. Однак в умовах підключення та замовлення послуги «Соціальні мережі» від ТОВ «Лайфселл» та «Соціальні мережі без обмежень» від Київстар, що розміщені на сайтах зазначених компаній, відсутні будь-які зобов'язання щодо поводження з персональними даними абонентів. Отже, персональні дані громадян фактично залишаються незахищеними.

Заради справедливості варто зазначити, що у розділі «Важлива інформація» сайту ТОВ «Лайфселл» розміщено загальні умови обігу та обробки персональних даних користувачів. Зокрема зазначено, що персональні дані, які надавалися на підставі вільного волевиявлення у процесі укладення договорів або здійснення інших операцій з ТОВ «Лайфселл» з 01.01.2011 р., будуть включені у відповідні бази персональних даних ТОВ «Лайфселл», які формуються і підлягають реєстрації відповідно до Закону України «Про захист персональних даних». Розголошення персональних даних суб'єктів цих даних при реєстрації баз даних не відбувається. ТОВ «Лайфселл» буде вважати, що згода на обробку персональних даних на законних підставах, відповідно до сформульованої у таких угодах мети, предмета угоди і зобов'язань сторін, є підтвердженою, якщо протягом 20-денного строку не буде отримано письмову вмотивовану вимогу щодо знищення персональних даних, наданих під час укладення угоди [11].

Натомість найголовніша проблема в інформаційній безпеці будь-якого девайса – це шпигунство і стеження за особистими даними користувача. А почалося все досить невинно. У 1962 році інженери компанії Bell Laboratories створили гру «Дарвін». Дві програми змагалися між собою, досліджуючи дисковий простір комп'ютера і намагалися знищити одна одну. Згодом принцип саморозмноження структур став використовуватися хакерами для створення шкідливих програм. З'явилися перші віруси і троянці. Троянці, на відміну від вірусів, шукають уразливості пристроїв і використовуються для крадіжки паролів і отримання конфіденційної інформації. Існують безліч троянців, про які користувач і не здогадується:

1) віддалене адміністрування (троянці допомагають хакеру тримати девайс під своїм повним контролем);

2) рекламні модулі (при встановленні зламаної програми або запуску torrent-файлу на комп'ютер завантажуються додаткові спеціальні модулі (рекламні банери і спливаючі вікна));

3) розсилка спаму (цей тип шкідливих програм збирає адреси пошти і згодом організовує масову розсилку рекламного характеру);

4) шпигунські програми (троянці ведуть шпигунство за «жертвою», відслідковують відвідувані сайти, натиснення клавіш і роблять скріншоти екрану);

5) proxy-сервери (непомітно встановлюючи проксі-сервер, хакер підставляє IP користувача, роблячи незаконні дії в інтернет мережі);

6) програми обчислень («інтелігентний» вид троянців, який використовує ресурси вашого комп'ютера для групових обчислень певних завдань) [12].

Це ж стосується і власників мобільних пристроїв, які використовують Android. Наприклад, вірус Simplocker шифрує дані SD-карти, після чого вимагає гроші для розблокування. Потім з'явилися «знамениті» троянці Geinimi і DroidDream, які збирали конфіденційну інформацію у смартфоні і відсилали інформацію на віддалені сервери. Саме після цих випадків Google почав активну боротьбу за «чистоту» служби play market. З початку 2015 року кількість вірусів для Android обчислюється кількома сотнями тисяч [12].

Відомо, що у країнах Європейського Союзу, США, Російській Федерації для придбання SIM-картки необхідно пред'явити паспорт (або інший документ), що містить персональні дані про особу. Продавці SIM-карт, посередники та оператори мобільного зв'язку здійснюють обіг та обробку персональних даних. Ця ситуація відбувається за «мовчазної згоди» абонента. Однак необхідно встановити вимогу у відповідному законодавстві, що обробка персональних даних абонентів здійснюватиметься винятково на підставі письмової згоди абонента (або прирівняної до письмової), тоді як обіг може здійснюватися за принципом «мовчазної згоди». Згода на обіг та/або обробку повинна включати ознайомлення абонента з його правами та правовими наслідками обігу та/або обробки його персональних даних.

Соціальні мережі збирають біографічні дані, щоб дозволити користувачам легко знаходити один одного. Така інформація також приваблює мисливців за персональними даними. Дівоче прізвище матері, рік закінчення школи, кличка домашнього вихованця часто служать контрольними питаннями для зміни паролю. Існує чимало спеціальних програм стеження і зламу. Деякі з

них можна безкоштовно скачати в Інтернеті, а більш складні – купити. Наприклад, одна з найпопулярніших програм Spy Recon не тільки фіксує все, що було введено з клавіатури, у тому числі паролі, але і записує чати, які велися з використанням комп'ютера (ICQ, Skype, MSN). До того ж, щоб дізнатися про користувача соціальної мережі, можна скористатися тільки досягненнями науки, не застосовуючи незаконні засоби. Вчені Кембриджського університету виявили, що навіть те, як користувач ставить «лайки» у Facebook, може багато розповісти про його політичні та релігійні погляди, сексуальну орієнтацію, сімейний стан, шкідливі звички й інші аспекти особистої інформації, які він не хоче розкривати у своєму профілеві. А сучасні комп'ютерні програми дозволяють «витягти» усю цю інформацію з соцмереж і проаналізувати її. Вченим, які аналізували «лайки», вдалося з вірогідністю 88% визначити сексуальну орієнтацію чоловіків, які брали участь у дослідженні, 95% – расову приналежність, 80% – політичні і релігійні погляди, які не були відображені у профілях [13].

Враховуючи досвід провідних країн Європейського Союзу, зокрема Німеччини, у сфері забезпечення безпеки обігу та обробки персональних даних, доцільно закріпити у Законі України «Про захист персональних даних» [14] положення, згідно з яким власники, оператори та інші особи, що надають послуги з доступу до соціальних мереж в Україні, а також їх персонал зобов'язані зберігати та обробляти персональні дані користувачів на підставі згоди останніх як на обіг даних, так і на їх обробку.

Висновки. Залишається невирішеним питання юрисдикції баз персональних даних, коли органи влади України (спеціальні служби, правоохоронні органи тощо) для отримання доступу до персональних даних користувачів, які проживають на території України, зобов'язані здійснювати запит на персональну інформацію в іноземних суб'єктів господарювання, які в 99% не дають згоди на розкриття інформації через відсутність доказової бази про належність акаунту конкретній ідентифікованій особі. Наведене свідчить про необхідність запровадження реєстрації сім-карток щодо ідентифікованої особи з подальшою прив'язкою інтернет-акаунтів до сім-карток для збільшення розкриття правопорушень. Крім цього, з метою чіткої правової оцінки правових ризиків варто на законодавчому рівні встановити вимогу щодо зберігання баз персональних даних осіб на території країни, в якій вони проживають, або країни, з якою існує двосторонній або багатосторонній договір, про забезпечення безпеки обігу та обробки персональних даних.

Список використаних джерел:

1. Регламент Європейського Суду з прав людини від 01.06.2010 року // [Електронний ресурс]. – Режим доступу : www.minjust.gov.ua.

2. Захист персональних даних: правове регулювання та практичні аспекти : [науково-практичний посібник] / М.В. Бем, І.М. Городиський, Г. Саттон, О.М. Родіоненко. – К. : К.І.С., 2015. – 220 с.

3. Интернет: прецедентная практика Европейского Суда по правам человека // Совет Европы. Европейский Суд по правам человека, 2012. – 41 с. [Електронний ресурс]. – Режим доступу: http://echr.coe.int.

4. Перевірка сторінки у соціальній мережі може вважатися втручанням в особисте життя [Електронний ресурс]. – Режим доступу: https://tsn.ua/svit/yespl-dozvoliv-zvilnyati-z-roboti-cherez-perepisku-v-facebook-570259.html

5. Рішення Європейського Суду з прав людини по справі «K.U. проти Фінляндії» від 02.03.2009 р. // Рішення Європейського Суду з прав людини щодо захисту персональних даних [Електронний ресурс]. – Режим доступу: https://www.google.com.ua/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact= 8&ved=0ahUKEwi46t6y-rPUAhWK2BoKHbOICu4QFggvMAI&url=http%3A%2F%2Frm. coe.int%2F168059920d&usg=AFQjCNGJbn8SJzRQjzAJiwmry8m7ftUqbQ&sig2=bBIuhgBjHRpFpnzo1RIyEg

6. Рішення Європейського Суду з прав людини по справі «K.U. проти Фінляндії» від 02.03.2009 р. [Електронний ресурс]. – Режим доступу: https://www.google.com.ua/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uac t=8&ved=0ahUKEwj1w5qqgbTUAhVElxoKHdG_AFUQFgguMAE&url=http%3A%2F%2Fhudoc.echr.coe.int%2Fapp%2Fconversion%2Fpdf%2F%3Flibrary%3DECHR%26id%3D001-117605%26filename%3D001-117605.pdf%26TID%3Dihgdqbxnfi&usg=AFQjCNF_1JkP8mBj DEEia N4tQ_oyYU8zvQ&sig2=bGWVGspLsHJ9zKMzEvwb_A

7. Агентство национальной безопасности США активно создает «социальные карты» на пользователей социальных сетей [Электронный документ] – Режим доступа: http://zadereyko.info/sbor_informacii_o_polzovatele/anb_sobiraet_informaciy_o_polzovarelah_sostsetey.htm

8. Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» : Указ Президента України №133/2017. [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/documents/1332017-21850

9. Офіційний сайт ТОВ «Лайфселл». [Електронний ресурс]. – Режим доступу: https://www.lifecell.ua/ru/mobilnyi-internet/dopolnitelni-uslugi/usluga-vkontakte-bez-ogranicheniy/#change-tariff-block-anchor

10. Офіційний сайт Київстар. [Електронний ресурс]. – Режим доступу: https://kyivstar.ua/ru/mm/social

11. Офіційний сайт ТОВ «Лайфселл». [Електронний ресурс]. – Режим доступу: https://www.lifecell.ua/uk/pro_lifecell/kompaniia-sogodni/vazhliva-informatsiia/

12. Шпигуни усюди: сучасні можливості слідкувати за користувачами. [Електронний ресурс]. – Режим доступу: http://zillya.ua/shpiguni-usyudi-suchasni-mozhlivosti-slidkuvati-za-koristuvachami

13. Яцишин А.О. Шпигунство в соціальних мережах / Я.О. Яцишин. [Електронний ресурс]. – Режим доступу: http://conf.inf.od.ua/doklady-konferentsii/spisok-materialov-konferentsii/56-yatsishin-a-o-student-2-go-kursu-institutu-prokuraturi-ta-slidstva-nu-oyua-naukovij-kerivnik-k-t-n-dotsent-zaderejko-o-v-shpigunstvo-v-sotsialnikh-merezhakh

14. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – С. 1188. – Ст. 481.