

Київський національний університет імені Тараса Шевченка
Філософський факультет
Кафедра теоретичної і практичної філософії

**АНОНІМНІСТЬ ЯК ОСНОВНИЙ ЕЛЕМЕНТ НОВОЇ КОМУНІКАЦІЇ В
МЕРЕЖЕВОМУ ПРОСТОРИ ТА ЇЇ ПСИХОСОЦІАЛЬНІ І ПРАВОВІ
НАСЛІДКИ**

**ANONYMITY AS THE MAIN ELEMENT OF NEW COMMUNICATION
IN NETWORK SPACE AND ITS PSYCHOSOCIAL AND LAW AFFECTS**

Кваліфікаційна робота за напрямом підготовки 033 «Філософія»
на здобуття кваліфікаційного рівня бакалавра

Студент-виконавець:

Чалова Раїса Олександрівна

(підпис)

IV курс, ОС - Бакалавр

Науковий керівник:

Якубіна Валентина Леонідівна
Кандидат філософських наук, доцент

(підпис)

Допущено до захисту:
на засіданні кафедри теоретичної
і практичної філософії
протокол № ____ від _____ 2020 р.

Зав. кафедри теоретичної і практичної філософії,
доктор філософських наук, професор
Шашкова Людмила Олексіївна _____

Київ-2020

Зміст

Вступ	3
Розділ 1. Нове суспільство як основа нового типу взаємодії	8
1.1. Інформаційне суспільство як основа переоформлення соціальної організації.....	9
1.2. Мережеве суспільство та розповсюдження мережі.....	12
1.3. Віртуальна спільнота та її комунікативна культура свободи.....	17
Розділ 2. Анонімність як елемент сучасної віртуальної комунікації	21
2.1. Визначення анонімності та цифрової ідентифікації.....	22
2.2. Псевдонімність.....	23
2.3 «Континуум анонімності».....	25
Розділ 3. Психологічно-соціальний аспект розгляду анонімності. Анонімність як особливий мотиватор поведінки	28
3.1. Ефект мережевої дезінбації.....	30
3.2. Деіндивідуалізація в кіберпросторі.....	33
3.3. Кіберагресія як прояв негативних наслідків анонімності.....	34
3.4. Формування вільного простору соціальної взаємодії як позитивний наслідок анонімності.....	36
Розділ 4. Правовий аспект розгляду анонімності. Анонімність як елемент здійснення прав людини	39
4.1. Анонімність та право на свободу слова та вираження.....	42
4.2. Анонімність і захист конфіденційних даних. Право на недоторканність приватного життя.....	44
4.3. Анонімність і право на захист честі, гідності та ділової репутації.....	48
4.4. Анонімність і авторське право.....	53
4.5. Держава у протистоянні з простором анонімної мережевої комунікації та діяльності. Кіберзлочинність як стимул заборони анонімної комунікації.....	56
Висновки	62
Список використаних джерел	67

Вступ

Актуальність теми дослідження обумовлена мережевізацією суспільства, суспільних відносин в інформаційну епоху, що призводить до становлення нових форм соціальності — мережевого суспільства, появи нових типів спільнот — віртуальних спільнот, а також змін типів і характеру комунікації та взаємодії. Найбільш яскраві прояви цих змін походять і спостерігаються в мережі Інтернет, основним елементом функціонування і поширення якої є анонімність і псевдонімність.

Можливості анонімної комунікації в її різних проявах змінюють усталені форми соціальної взаємодії, представляючи користувачам Інтернет-простору і соціальних мереж абсолютно новий інструментарій для комунікації, взаємодії з іншими користувачами, для сприйняття своєї ідентифікації та її зміни. Крім того, подібні новації не залишаються тільки в межах віртуальної взаємодії, формуючи перетворення функціонування суспільства в цілому.

Інтернет-простір, соціальні мережі та мережева комунікація стають невіддільною складовою життя більшості населення планети, а Інтернет-технології та елемент анонімізації поширилися на всі сфери людської діяльності: все більше сфер людської діяльності розвиваються в Інтернет-просторі або змінюються під його дією, відбувається трансформація соціальних інститутів, економічних взаємодій, політичного і правового регулювання. Механізми анонімізації та анонімність в цілому є невіддільною частиною цих трансформацій, що веде до появи нових проблем у всіх сферах.

У сфері соціальної взаємодії у віртуальному просторі виникають проблеми зміни поведінки користувачів під впливом ефекту мережевої дезінбації, який спостерігається виключно в умовах мережевої комунікації, основним елементом якої є анонімність. Ця зміна вказує на актуальність досліджень віртуальної комунікації з позицій соціальної психології, психології ідентифікації, регулювання групових відносин. Важливість цього питання можна простежити на прикладі зростання ролі соціальної етики та

етики віртуальної взаємодії, зростання кількості досліджень в галузі психології та соціології щодо питань анонімної комунікації, взаємодії та анонімного сприйняття себе та інших у віртуальному мережевому просторі.

Анонімність як елемент взаємодії різних людей і груп людей в Інтернет-просторі також породжує безліч правових проблем регулювання відносин між користувачами, які пов'язані з можливістю уникнення правової та неправової відповідальності. Актуальною є проблема впливу анонімності та анонімної поведінки на реалізацію основних прав людини та громадянина в Інтернет-просторі. Це підтверджує зростаюча настороженість міжнародних організацій щодо захисту прав людини. Їхня діяльність зачіпає ще одне актуальне питання анонімної комунікації — питання взаємоіснування анонімності та правової відповідальності. Все більша кількість країн і державних структур скептично ставляться до можливості повної анонімності в Інтернеті, що, на їхню думку, породжує неконтрольовану кіберзлочинність і несе небезпеку для суспільного благополуччя.

Анонімність в Інтернет-просторі через поширення кіберагресії та кіберзлочинності часто розглядається виключно в її негативному впливі. У даній роботі я намагалася показати, що важливим є вивчення анонімності в її комплексному розгляді. Недостатня база досліджень позитивних наслідків анонімної комунікації може призвести до того, що анонімізація в Інтернет-просторі стане неможливою через її заборону державними структурами. Для перешкодження такого результату необхідно глибоке розуміння соціального і правового значення анонімності.

Ступінь опрацювання. Філософія Інтернет-простору і віртуальної комунікації є однією з новітніх течій сучасної філософії, соціальної психології, філософії права та інших суміжних дисциплін, в рамках яких проблема анонімності та різні її інтерпретації — проблема фізичної непередставленості, неявного правового суб'єкта — займають одне з центральних місць. Розробка цієї проблеми є логічним продовженням вивчення віртуальних спільнот і соціокультурних особливостей глобального

соціуму і комунікації в інформаційну епоху, якому присвячені роботи Ф.Уебстера, М.Кастельса, Ж.Бодрійяра, Г.Рейнгольда. Найбільш поглиблене обґрунтування поняття мережевої комунікації та мережевої взаємодії отримано в теорії мережевого суспільства М.Кастельса, дослідження якого заклали основи поняттєвого апарату в даній роботі. Їх доповнили роботи сучасних зарубіжних дослідників - Б.Годдіна, Н.Еллісон, Г.Маркса та А.В.Курочкина.

Агеографічність і глобалізованість проблеми анонімності визначають міжнародний, глобальний підхід дослідження, що обумовлює звернення в рамках даної роботи до міжнародних правових документів, міжнародних наукових досліджень ролі анонімної комунікації — документів ЮНЕСКО, Ради Європи, доповідей спеціальних доповідачів ООН Франка ла Рю і Девіда Кайе, а також до незалежних досліджень різних неурядових організацій — Freedom on the Net, Reporters Without Borders, Electronic Frontier Foundation.

Міждисциплінарний підхід відіграє ключову роль в дослідженні проблеми анонімної комунікації та анонімної взаємодії. Ця проблема розглядається з філософських, соціально-психологічних, правових, технічних сторін. Саме тому комплексне всебічне дослідження питання анонімної комунікації та анонімної взаємодії неможливо без звернення до досліджень філософії комунікації, соціальної психології, досліджень з віртуальної ідентифікації та віртуальних спільнот, досліджень правового і неправового регулювання віртуального простору. Проблематиці соціокультурних і соціально-психологічних аспектів мережевої комунікації присвячені роботи зарубіжних дослідників — Дж.Сулера, К.Скотта, Е.Холленбо, Дж.Бішопа, Е.Нагель, а також роботи вітчизняних і російських дослідників — Н.Н.Королевой, Т.А.Фетісовой, А.Е.Жичкіной та інших. Проблематика правового регулювання анонімної комунікації в Інтернет-просторі є актуальною проблемою як на міжнародному, так і на національному рівні, що зумовило розгляд міжнародних документів ЮНЕСКО, ООН, Ради Європи, доповідей спеціальних доповідачів ООН, досліджень неурядових

організацій - Freedom on the Net, Reporters Without Borders, робіт політичних і правових дослідників віртуальної взаємодії та її державного контролювання — Я. ван Дьюка, Чень Ді, Г. Чао.

Новизна проблематики анонімної комунікації та анонімної взаємодії в мережевому просторі обумовлює велику кількість сучасних досліджень з її різних аспектів, а глобальний характер Інтернет-простору і доступність даної платформи спонукає проводити дослідження представникам різних країн.

Об'єктом дослідження виступає сучасна філософія віртуальної комунікації та філософія права в Інтернет-просторі.

Предметом дослідження є сучасна тенденція анонімної комунікації та анонімної взаємодії в мережі Інтернет як базисний аспект нового віртуального суспільства, а також поширення цієї тенденції на правове регулювання віртуальних відносин.

Метою дослідження є визначення способів функціонування анонімної комунікації та визначення ступеня її впливу на психологічно-соціальні та правові сфери віртуальної взаємодії.

Відповідно до поставленої мети її досягнення було здійснено шляхом розв'язання наступних завдань:

— дослідити еволюцію мережевого суспільства як суспільства нового типу комунікації в інформаційну епоху;

— з'ясувати причини посилення ролі анонімності та анонімної комунікації в віртуальному соціальному просторі;

— визначити термінологічний апарат анонімної комунікації та анонімної взаємодії у віртуальному мережевому просторі;

— виділити рівні функціонування анонімної комунікації;

— розглянути специфіку соціально-психологічних змін поведінки особистості в умовах анонімної комунікації та анонімної взаємодії у віртуальному мережевому просторі;

— схарактеризувати наслідки анонімної комунікації для поведінки осіб у віртуальному мережевому просторі;

— дослідити специфіку регулювання взаємовідносин між основними правами людини та анонімним віртуальним мережевим простором на міжнародному та національному рівнях;

— розглянути підходи окремих держав і міжнародних коаліцій щодо обмеження анонімної свободи в мережевому віртуальному просторі.

Методи дослідження. Методологічну основу дослідження склали принципи та концепції вітчизняного та зарубіжного підходів до розгляду комунікації та взаємодії у віртуальному мережевому просторі, що розкривають особливості функціонування анонімності на індивідуальному, груповому рівнях, а також взаємозв'язок анонімності у віртуальних спільнотах з питаннями регулювання реального соціального простору.

В межах дослідження були застосовані:

— аналітичний метод, який спрямований на визначення тенденцій становлення нового типу суспільних відносин і комунікації, простежування тенденцій поширення анонімності на поведінку індивідів і груп, а також тенденцій регулювання анонімних відносин в Інтернет-просторі.

— компаративний метод, який спрямований на порівняння поведінкових моделей у віртуальному мережевому просторі анонімної комунікації та реальному соціальному просторі, а також на порівняння політичних і правових ініціатив щодо регулювання можливостей анонімної дії в віртуальному просторі з боку різних країн.

— Крім цього, в роботі розглядалися статистичні дані Інтернет-взаємодії та комунікації, представлені різними дослідницькими центрами, що вказує на звернення до методу формалізації різних контактів в Інтернет-просторі, негативних і позитивних проявів анонімної комунікації, ставлень щодо анонімної взаємодії з боку користувачів і державних та правових структур.

Сформульовані завдання і загальна логіка дослідження зумовили структуру даної роботи, яка складається зі вступу, чотирьох розділів, висновків та списку використаної літератури.

Розділ 1. Нове суспільство як основа нового типу взаємодії

Середину-кінець ХХ — початок ХХІ століття можна з упевненістю визначити як період широкомасштабних змін фундаментальних основ суспільства, діяльності, комунікації тощо. Представники різних сфер дослідження формують безліч теорій для пояснення тих змін, які відбулися з усіма аспектами суспільного життя в новій епосі, для пояснення нового устрою та стану сучасного суспільства.

Незважаючи на велику кількість підходів та концепцій до пояснення цих явищ з боку різних дослідників можна помітити кілька схожих характеристик. Першою характеристикою служить глобальний характер суспільних змін та його поширення на всі сфери людської діяльності та життя в цілому. Другою характеристикою є збільшення кількості інформації, інтенсифікація обміну інформацією, розширення можливостей отримання та поширення інформації. Ця характеристика визначає нове суспільство в його інформатизації, яка поширюється не тільки на сферу виробництва, економіки, політики, а й на сферу приватного спілкування.

До дослідження інформаційного суспільства підходили представники різних дискурсів та традицій, які по-різному трактували появу та прояви інформаційного суспільства. Деякі з них бачили в інформатизації суспільства продовження встановлених законів розвитку цивілізації, деякі — суспільство абсолютно нового типу. До найбільш відомих дослідників даної теми відносяться Д.Белл з його ідеєю постіндустріалізму, Ж.Бодрійяр та ідея постмодернізму, М.Кастельс, який розглядав інформатизацію як особливий новий шлях розвитку цивілізації (інформаційний спосіб розвитку), Ф.Уебстер, який прагнув класифікувати теорії інформаційного суспільства для виділення основних його рис, З.Бауман та ідея індивідуалізованого суспільства, Ю.Габермас та концепція публічної сфери тощо. Всі ці концепції по-різному розкривають особливості сучасності. У наступних розділах даної частини роботи я буду намагатися виділити основні особливості інформаційного суспільства, які відзначають багато дослідників даної теми, а

також зосередитися на аспектах соціальних та комунікативних змін. Особливу увагу я приділю розгляду особливостей інформаційного суспільства в мережевому аспекті.

1.1. Інформаційне суспільство як основа переоформлення соціальної організації

Отже, який би підхід до інформаційного суспільства ми не розглядали, вони сходяться на тому, що «інформація стає чимось особливим». Саме визначення інформаційного суспільства безпосередньо залежить від того критерію зміни, який визначається як вирішальний. В даному розділі я зосереджусь на розгляді змін в комунікації та взаємодії між людьми з приходом інформаційного періоду.

Більшість початкових теорій інформаційного суспільства ґрунтуються на якісних змінах саме в технологічній сфері. Можна погодитися зі словами М.Кастельса про те, що суспільство не може бути зрозуміле без його технологічних інструментів [5]. Технологічні інновації багато в чому визначили вимірювання соціального, економічного, політичного, залишаючись самодостатнім та самоцінним критерієм. Ф.Уебстер впевнений, що технологічні нововведення є частиною соціального, по-новому перерозподілили та визначили цінності соціуму, створили можливості для перебудови системи комунікації та соціальної взаємодії [9].

Починаючи з 70-х років ХХ століття технологічні інновації та цифрові комунікаційні технології дійсно мали характер глибокого проникнення в усі сфери соціального життя: кабельне та супутникове телебачення, комп'ютерні мережі, персональні комп'ютери, онлайніві інформаційні послуги — все це вплинуло на взаємодію в усіх сферах суспільства. Особливе значення в цьому мали цифрові комунікаційні технології — електронна пошта, інформаційний обмін в режимі он-лайн, Інтернет чати, соціальні мережі, а також прискорення виробництва та розповсюдження персоналізованих технічних пристроїв, які зробили революцію у сфері спілкування та обміну

інформацією. З появою, розвитком та активним поширенням Інтернету та супутніх комунікаційних технологій світове співтовариство стало функціонувати в умовах глобального комунікаційного простору, в умовах технологічної інфраструктури, яка забезпечує миттєву комп'ютерну мережеву комунікацію в будь-який час та в будь-якому місці, де є відповідне обладнання.

Одним з критеріїв інформаційного суспільства, який називає Ф.Уебстер, поряд з економічним та технологічним, є просторовий критерій, який переносить акцент розгляду на «інформаційні мережі, які пов'язують різні місця, а тому можуть надати глибокий вплив на організацію часу та простору, що перетворює соціальну організацію» [9, с.15]. Новий тип соціальної організації утворює певне «провідникове» суспільство — суспільство, що складається з представників різних країн, регіонів, культур, які володіють достатнім обладнанням для доступу до глобальної мережі. Нова соціальна архітектура, яка базується на принципах мережевої комунікації, не має центру та периферії, вона містить в собі безліч автономних агентів — комп'ютерних мереж, персональних пристроїв тощо. Поширення інформаційно комунікативних технологій в напрямку їхнього індивідуального використання та зростання доступності цих технологій для все ширших верств населення, призводять, з одного боку, до «віртуалізації» соціальних контактів за допомогою легкості доступу до мережі Інтернет та доступності індивідуальних комунікаційних пристроїв, а з іншого — до «технологізації» та зростання можливостей маніпулювання поведінкою соціальних суб'єктів, штучного створення соціальних спільнот та управління ними в рамках т.зв. «соціальних технологій» [8].

Нова соціальна організація принесла зміни й в інші сфери суспільства. Наприклад, у сфері культури потоки інформації та обсяги інформаційних джерел дуже зросли. Зросла кількість телекомунікацій, збільшився час телемовлення. Всі міста переповнені рекламними вивісками. Крім того, розширюються обсяги інформації та її споживачів на різних платформах в

Інтернеті. Інтернет-сервіси багато в чому заміщають теле- і радіомовлення, друкарську продукцію. Можливо, незабаром теорія М.Маклюена про придушення попередніх форм культури новими виявиться дієвою в умовах розширення влади мережевих технологій.

Практично повсюдний доступ до інтернет-комунікацій дозволяє отримувати інформацію з будь-якої точки доступу. Все це робить інформацію більш доступною, що призводить до того, що збільшується саме кількість споживачів та постачальників, джерел інформації. Можна зробити висновок, що сучасне суспільство має існувати в умовах, які Ф.Уебстер назвав «медіаперевантаженими» [9]. Ця медіаперевантаженість поширюється по всьому тілу різноманіття соціальних відносин, соціальних структур, внаслідок чого модифікується сам досвід життя, тіла, інших, себе тощо. Наприклад, через доступність до інформаційних потоків про різні групи, субкультури суспільства людина може різнобічно порівнювати себе з іншими, що дає їй більше інформації про неї саму. Однак перетворюється не тільки людина, споживач інформації, а й характер самої інформації, змінюється також сама взаємодія з інформацією. У цьому контексті можна згадати підхід Ж.Бодрійяра, який фіксував за знаками в інформаційних потоках певне «потьмарення» [1]. Людина отримує знаки звідусіль, ці знаки розрізняються, постійно змінюються, дуже часто одні знаки суперечать іншим. В результаті знаки вже не означають, а скоріше імітують. Аудиторія споживачів, яка по-своєму пристосувалася до інформаційної епохи, стала більш критична та рефлексивна, що призводить до того, що знаки-симуляції сприймаються несерйозно, дають свободу переломлювання колишніх смислів та інформації.

Сучасна людина має пристосовуватися до нових умов, як колись за часів індустріальної революції доводилося пристосовуватися до умов машинного виробництва. Базовим моментом взаємодії між людьми стає інформація, а все більшого значення як поле комунікації та взаємодії набувають мережеві ресурси; засоби комунікації та інформації проникають в

усі галузі соціальної дійсності та перетворюють її. Ф.Уебстер робить висновок, що життя «проходить в процесах обміну та отримання повідомлень» [9]. Велика частина цих процесів проходить в мережевому полі та глобальній мережевій структурі. Найбільшу теорію з приводу глобальної соціальної структури як нового мережевого суспільства запропонував М.Кастельс. У суспільстві нового типу панують глобальні мережеві структури, які змінюють тип комунікації, поширюються засоби самокомунікації — персональні мережеві пристрої з доступом до глобальної мережі — через які людина будує власні інформаційні системи.

Мережеві структури стають новою платформою та новою умовою для розвитку всіх сфер суспільного життя, технологічна детермінація проникає в усе різноманіття соціальних, політичних та духовних компонентів суспільства. Це призводить до виникнення нових форм соціальної взаємодії, формує особливості соціальної поведінки. Таким чином, можна зробити висновок, що інформаційне суспільство заклало основи для розвитку та поширення мережевого суспільства, в рамках якого умови, можливості, джерела інформації та комунікації зазнають колосальних змін, відбувається соціальна трансформація та генезис нової соціальної реальності, основними компонентами якої є інформаційні технології, реалізація дійсності через віртуальну реальність та мережевість відносин.

1.2. Мережеве суспільство та розповсюдження мережі

Мережеве суспільство можна визначити як глобальне суспільство, яке побудоване навколо персональних та організаційних мереж, котрі засновані на цифрових мережах та мережі Інтернет. Вивчення структур мережевого суспільства тісно пов'язане зі збільшенням в середині ХХ ст. наукового інтересу до питань мережевих форм комунікації та введення в термінологічний апарат поняття «соціальна мережа». Вперше термін «соціальна мережа» був введений Дж.Барнсом в 1954 році, що послужило поштовхом для розгляду соціальних мережевих взаємин в різних сферах [38].

Мережева соціальна структура як нове явище інформаційної епохи вперше було розглянуто в роботі Б.Веллмана 1973 року «The network city», в якій автор звернувся до питань впливу нового соціального устрою на соціальні, політичні, урбаністичні та інші аспекти діяльності та комунікації. Сам термін «мережеве суспільство» був введений в праці 1991 року голландського дослідника Яна ван Дайка «De Netwerkmatschappij» («Мережеве суспільство»). Автор визначав мережеве суспільство як «таку форму суспільства, яка все частіше організовує соціальні відносини з допомогою медіамереж, поступово заміщуючи або доповнюючи ними соціальні комунікації "віч-на-віч"» [23]. Відповідно до Я. ван Дайку соціальний простір подвоюється, тим самим спільноти всередині суспільства стають менш стабільними, їхні межі розмиваються, вони взаємопроникають один в одного.

Ідею вільного «перетікання» ідей та інформації, координації зусиль та відсутності в нову епоху суворої ієрархічної системи розвиває іспанський соціолог Мануель Кастельс — одна з ключових фігур наукового дослідження питань мережевого суспільства та соціальної комунікації на сучасному етапі. На його думку, архітектура мережевого суспільства має характер «ризому», адже мережа та мережева система, які стають універсальною формою організації суспільства та суспільних процесів, неможлива при ієрархічній системі та відсутності постійної комунікації.

Появу та розвиток мережевого суспільства М.Кастельс пов'язує зі змінами в інформаційно-технічних можливостях людини, з культурними та соціальними змінами другої половини ХХ століття та економічною перебудовою. Ці процеси вплинули на побудову нової соціальної структури — мережевого суспільства, нової економічної системи — глобальної інформаційної економіки, та нової культури — культури «реальної віртуальності». В мережевому суспільстві зникає єдина провідна культура та основним стає процес вільної конкуренції субкультур та культурних кодів. Взаємозв'язок мережевої віртуальності та соціальної реальності породжує

нові типи взаємодії та комунікації, при яких суб'єкти відмовляються від спілкування в соціальному середовищі та віддають перевагу віртуальному спілкуванню. М.Кастельс називає цей феномен «реальною віртуальністю», вказуючи на те, мережевий віртуальний світ сприймаються багатьма куди більш реально, ніж сама дійсність [4]. Таким чином, мережа стає універсальним типом соціальних відносин.

Мережева структура стає універсальною організаційною структурою для всіх видів комунікацій: для індивідуальної та міжнародної комунікацій, для корпорацій, для підприємств, окремих соціальних спільнот, в тому числі, як описує М.Кастельс, для злочинних груп тощо. Інформаційно-комунікативні технології відкривають можливості встановлення миттєвого, постійного зв'язку та передачі майже необмежених обсягів інформації, тим самим створюючи єдину комунікативну мережу, яка зв'язує всі сфери суспільства. Інформаційні технології охоплюють всі галузі людської діяльності, безпосередньо формують як особисте життя індивідів, так і їхню групову діяльність.

Основний елемент поширення мережевого суспільства та взаємопов'язаних з ним мережевих способів комунікації полягає в повсюдному глобальному використанні масових і, особливо, персональних електронних засобів комунікації. М.Кастельс вважає, що, починаючи з 1990-х рр., відбувається світова комунікаційна революція: зростає кількість персональних мобільних пристроїв, пристроїв з доступом до мережі Інтернет, розширюються функції пристроїв, розширюється поле покриття зв'язком. За статистикою, яку наводить М.Кастельс, в 1991 році було близько 16 млн. користувачів мобільних телефонів, але вже у 2008 році це число перевищило 3,4 млрд. — тобто більшість населення [19]. Згідно зі статтею Дослідницького центру П'ю зараз понад 5 мільярдів осіб мають мобільні пристрої, понад 3,5 мільярда з яких — мобільні пристрої з доступом до мережі Інтернет, постійним доступом до соціальних мереж тощо [48].

Доступ до мережі Інтернет поширюється ще більш високими темпами: згідно International Data Corporation, якщо в кінці 1995 року, коли почалася повсюдне залучення до Інтернету, в світі налічувалося близько 16 мільйонів користувачів Інтернету, що становило 0.4% населення, то вже в березні 2001 було 458 мільйонів абонентів, що склало 7.6% населення. У наступні роки зросла не тільки кількість абонентів, але і поле поширення мережі і відсоток світового населення, який мав доступ до мережі Інтернет [57]. Згідно зі статистикою Internet World Stats в березні 2011 року вже 30.2% світового населення були користувачами Інтернету, що склало 2 мільярди 95 мільйонів чоловік [57]. На момент січня 2020 року загальна кількість користувачів мережі перевищила 4,5 мільярда чоловік, що склало більшу частину населення, майже 60 відсотків [57]. Інтернет-простір розширюється не тільки по зовнішньому вектору, поширюючись на країни третього світу, віддалені місцевості та все більший відсоток населення, але й шляхом внутрішнього розширення через створення все більшої кількості веб-сайтів та соціальних мереж.

У ХХІ ст. всередині Інтернет-простору найбільш використовуваними та популярними ресурсами є, як їх визначив М.Кастельс [19], системи масової самокомунікації (mass-self communication), які дозволяють шляхом транслявання різної інформації, текстових, фото-, відео- та аудіофайлів, отримувати зворотний зв'язок від аудиторії та провадити таким чином комунікацію: блоги, відеоблоги, подкасти. У 2007 році YouTube, відеохостинг, який дозволяє будь-якому користувачеві завантажувати, переглядати, коментувати та ділитися відеофайлами, став найпоширенішим засобом масової комунікації у світі. Самокомунікація має характер масової комунікації, тому що поширюється на глобальну аудиторію за допомогою пірінгових мереж та підключення до мережі Інтернет. Крім того, зміст самокомунікації доповнює вся спільнота користувачів, вона не має посередників у процесі передачі інформації — будь-який індивід, що має доступ в мережу Інтернет, може побудувати свою інформаційну систему. У

2019-2020 рр. в рейтингу найбільш відвідуваних веб-сайтів 2 і 3 місця, після пошукової системи Google, займають саме засоби самокомунікації: Youtube та Facebook, що лише підтверджує тенденцію до того, що саме засоби самокомунікації зі змістом різного характеру займають передові позиції.

Починаючи з 2002, а саме — появи Friendster — першої соціальної мережі, найбільш поширеною формою самокомунікації є соціальні мережі - Facebook, YouTube, Twitter, Instagram, які стають незамінним елементом повсякденного життя величезної кількості людей. Соціальну мережу можна визначити як певний сервіс, заснований на веб-інструментах, який дозволяє певній особі створювати загальнодоступний або частково доступний профіль в обмеженій веб-платформі системі, вступати в різні взаємодії з іншими користувачами та переглядати їхні дії, якщо ці дії передбачені платформою [26].

Згідно з даними Global Web Index у 2020 році кількість користувачів соціальних мереж досягла 3,8 млрд. Крім того, користувачам соціальних мереж є люди абсолютно різного віку, статі, класів, ступенів освіти, що дозволяє говорити про те, що процеси, що відбуваються в соціальних мережах, віртуальних спільнотах та мережевому суспільстві впливають на майже половину населення планети [60]. Можна зробити висновок, що більша частина комунікації в мережі Інтернет відбувається саме через соціальні мережі, які стають платформами для всіх видів діяльності, починаючи від особистого спілкування та маркетингу, закінчуючи освітою, культурою, поширенням ЗМІ тощо.

Мережеві спільноти поширюються не тільки як віртуальна реальність, але і як явище, яке інтегровано в повсякденне реальне життя та змінює багато сфер життєдіяльності людей. Наприклад, зміни відбуваються щодо засобів масової інформації, які все частіше переходять в зацифровану форму в мережевому полі. Згідно з дослідженням М.Гільберта, 95% всієї інформації, яка існує на планеті, зацифрована, та більша її частина доступна в Інтернеті [30]. Все більшого поширення отримують сервіси потокового відео та

онлайн-кінотеатри — YouTube, Hulu, Netflix; мережевий компонент стає важливим також й для преси, яка приділяє значну увагу мережній взаємодії, взаємодії з соціальними мережами, блогами.

Інтернет та різноманітні мережі складають технологічну інфраструктуру мережевого суспільства. Мережа Інтернет, соціальні мережі, пристрої з доступом до мережі та інші форми мережевої комунікації є комунікаційним каркасом доступу до інформації, основою життя величезної кількості людей, їхнього робочого та особистого проведення часу, основою формування їхніх знань про світ, політику, економіку, продукти та товари, а крім того вони є технологічним каркасом функціонування багатьох сфер суспільства. Таким чином, в мережевому суспільстві формується та поширюється нова комунікаційна форма і культура.

1.3. Віртуальна спільнота та її комунікативна культура свободи

Соціальна комунікація, яка багато в чому тепер є опосередкованою через мережі та Інтернет, породжує величезну кількість спільнот, а сьогодні ці спільноти отримують характер віртуальних. Термін «віртуальне співтовариство» був введений в 1993 р. Г.Рейнгольдом, який визначив його як «соціальне об'єднання, яке з'являється на основі практики комп'ютерно-опосередкованої комунікації в Інтернеті, коли група людей підтримує відкрите обговорення досить довго та гуманно, для того щоб сформувати мережу особистих відносин у віртуальному просторі» [45]. Єдиною різницею між віртуальними та реальними практиками Г.Рейнгольд називає арсенал мультимедійних засобів, яким володіють віртуальні спільноти, що робить віртуальність простору здійснення комунікацій відмінною рисою віртуальних спільнот. Мені здається, що погодитися про тотожність віртуальних та реальних спільнот буде недостатньо, адже крім перенесення реальних практик у віртуальний простір, віртуальні спільноти можуть також кардинально відрізнятись від реальних. Віртуальні співтовариства не мають географічних, політичних кордонів, містять в собі більше можливостей

для об'єднання людей, вони відрізняються можливістю потенційної взаємодії всіх членів спільноти з усіма та їхнім високим рівнем анонімності.

Особливу увагу віртуальним співтовариствам як особливим комунікативним утворенням приділяє М.Кастельс. М.Кастельс визначає віртуальні спільноти як «мережі міжособистісних зв'язків, які забезпечують соціальну взаємодію, підтримку, передачу інформації, почуття приналежності до групи та соціальну ідентичність» [4].

Віртуальні співтовариства почали формуватися з приходом перших користувачів комп'ютерних мереж, які й заклали основи громадської культури в Інтернеті. Якщо спочатку веб-сайти з можливістю комунікації або навіть соціальні мережі були лише віртуалізацією реальних соціальних зв'язків, то у ході збільшення масштабів та розширення сфери впливу віртуальних спільнот їхні початкові зв'язки з реальною соціальною базою та контркультурою, з потребою перенесення цього в віртуальне поле слабшали. Це дало можливість розвиватися самим різним цінностям та інтересам, поглядам, створити «какофонію віртуальних спільнот» [4]. Незважаючи на різноманіття та різнорідність віртуальних спільнот, М.Кастельс вважає, що можна виділити дві культурні цінності, які є фундаментом віртуальної комунікації всередині віртуальних спільнот [4]. Перша цінність полягає в можливості для кожного знайти його власне місце в Мережі або самостійно створити нову мережу, нове співтовариство. Друга цінність є вирішальною — це цінність вільної комунікації. М.Кастельс вважає, що ця цінність багато в чому визначає саму практику віртуальних спільнот, яка зводиться до втілення на всіх рівнях свободи слова в опозиції до «панування медійних конгломератів та цензур державних бюрократій» [4]. Ця свобода для багатьох висловлювати свою думку та доводити її до відома багатьох інших стала однією з фундаментальних цінностей Інтернету.

В даному питанні цікаво буде згадати "Декларацію незалежності кіберпростору» (A Declaration of the Independence of Cyberspace, 1996) — документ, який закликає до незалежності від будь-якої форми зовнішньої

влади; цей документ проголошує свободу слова та думок. П.Барлоу, автор Декларації, заявляє, що жодна з держав не має право поширювати свою владу та закони на віртуальне середовище, тому що Інтернет та мережа знаходяться за межами будь-якої держави. Інтернет та віртуальні спільноти розробляють свої власні соціальні контракти, норми та здатні самі регулювати всі виникаючі конфлікти. Інтернет проголошується середовищем, в якому «хто завгодно і де завгодно може висловлювати свої думки, не відчуваючи страху, що його або її примусять до мовчання або згоди з думкою більшості» [15]. «Декларація незалежності кіберпростору» стала знаковою для ідеології свободи соціального виміру Інтернету.

Зараз все більша кількість онлайн та офлайн ресурсів та правових організацій привертають увагу до проблеми свободи в рамках віртуальних спільнот та мережі Інтернет в цілому. Наприклад, в статуті ЮНЕСКО закріплена стаття про те, що організація закликає до створення вільного Інтернет-простору як частини забезпечення всеосяжної свободи вираження думок. У 2009 році ЮНЕСКО запустила серію публікацій про свободу в Інтернеті (Series on Internet Freedom), метою якої є привернення уваги до даної проблеми, вивчення правових та політичних проблем Інтернет-простору та надання політичних рекомендацій, які спрямовані на створення сприятливих умов для свободи вираження думок в мережі [61]. Неурядова організація Freedom House, яка займається дослідженнями стану політичних та громадянських свобод, бачить в Інтернет-просторі поле реалізації та гноблення прав особистості, а тому організувала щорічне дослідження Freedom on the Net, метою якого є аналіз свободи інтернету та цифрових медіа по всьому світу [56].

Однак поряд з діяльністю подібних організацій у світі зростає тенденція до регулювання Інтернету з боку урядів, внутрішніх цензорів тощо. Наприклад, найбільш поширеними елементами інтернет-цензури з боку урядових структур є блокування сайтів та фільтрація контенту. Відповідно до недавнього дослідження Freedom on the Net, дві третини всіх

користувачів Інтернету — 67% — живуть у країнах, де критика уряду, влади, правлячої групи піддається цензурі [58]. Дослідження показало, що на момент 2016 року свобода на просторах Інтернету в усьому світі знижується вже шостий рік поспіль. 27% всіх користувачів Інтернету живуть у країнах, де людей заарештовують за публікацію на їхній особистій сторінці або на сторінці загальнодоступного інформаційного ресурсу, за шерінг постів, репост публікацій. За 2016 рік влада в 38 країнах провели арешти на основі повідомлень в соціальних мережах. Ще однією тенденцією, зазначеної в дослідженні, стало збільшення законодавчих змін, що дозволяють урядам контролювати онлайн-спілкування людей [58].

Можна зробити висновок, що регулювання контенту в Інтернеті останнім часом вийшло на перший план громадських дебатів як питання, яке хвилює як уряд, так й користувачів Мережі. Крім того, питання свободи в віртуальних спільнотах та в Інтернет-просторі породжує проблему анонімності. Франк ла Рю, доповідач ООН з питань захисту права на свободу думок, вважає, що «готовність людей брати участь в дискусіях щодо спірних питань в публічній сфері завжди була пов'язана з можливістю зробити це анонімно» [34]. Він також зазначає, що саме анонімність є одним з найбільш важливих досягнень Інтернет-простору, адже цей елемент дозволяє людям вільно висловлювати свою думку, не побоюючись відплати або засудження [34].

Анонімність має основоположне значення для повного здійснення права на свободу та вираження думок, для підтримки нормального функціонування віртуальної комунікації. Якщо ж порушиться обсяг інформаційного потоку, зменшиться кількість користувачів, постраждає найважливіший тип комунікації в мережевому суспільстві, це, ймовірно, може змінити загальну картину сьогоденної громадської, правової, культурної ситуації. Саме тому нам здається важливим вивчити проблему анонімності більш детально.

Розділ 2. Анонімність як елемент сучасної віртуальної комунікації

Анонімність — не нововведення Інтернету, вона існує повсюдно в нашій соціальній реальності. Усна традиція часто не мала авторства, а друкована культура часто вдається до псевдонімів, як до інструментів забезпечення анонімності з тих чи інших бажань. Прагнення деяких авторів можна зіставити з прагненнями членів віртуальних спільнот сьогодні — тролінг, висміювання соціальних порядків, політичної системи чи церковних традицій, а анонімність для них в цьому контексті служить механізмом захисту.

Забезпечення анонімності служить двигуном не тільки літературного збагачення, а й прогресу правової системи, демократичних свобод. Справа Національної асоціації сприяння прогресу кольорового населення проти штату Алабама в 1958 році стало показовим випадком того, що анонімність необхідна для просування суспільно важливих ідей. Штат Алабама вимагав організацію розкрити повний список членів, але суд визнав, що «недоторканність приватного життя в груповому об'єднанні може бути необхідною для збереження свободи об'єднання, особливо коли група підтримує переконання інакомислячих».

Анонімність дозволяє дискусіям на теми важливих суспільних проблем протікати в різних, іноді не можливих для цього контекстах та спільнотах. Почасти тому анонімність була вбудована в ті протоколи, які служать основою для глобальної комп'ютерної мережі зараз. Одним з перших методів анонімного спілкування служив ремейлер — це сервер, який переправляє повідомлення електронної пошти анонімно, щоб одержувач був позбавлений можливості з'ясувати, хто є автором повідомлення. Й.Хельсінгюс, розробник анонімного ремейлер `anon.penet.fi`, стверджує, що саме анонімність є тим елементом віртуальної комунікації, яка робить мережу популярним місцем для спілкування [43].

Однак разом з відкриттям безмежного числа можливостей, мережева анонімність відкриває безліч проблем, адже в мережі відсутня велика

кількість меж та норм. Якщо поширення інформації в соціальній офлайн сфері шляхом нанесення гасел на стіни міського центру обмежено фінансовими ресурсами, кількістю стін, а також законом про вандалізм, то поширення інформації в мережі не обмежено ані фінансовими ресурсами, а ніяким редакторським контролем чи цензурою, ані встановленими законними межами такої діяльності. Крім того, все більше психологів та дослідників поведінки людини бачать в анонімності каталізатор масовізації свідомості, втрати контролю та посилення агресії. Ці питання стають все більш і більш актуальними, тому що все більша кількість людей відкриває для себе мережевий світ та стикається з анонімністю.

2.1. Визначення анонімності та цифрової ідентифікації

Інтернет-комунікація, та анонімізація користувача вводять нову грань ідентифікації — цифрову ідентифікацію, мережеву особистість (digital identity). Цифрова ідентичність являє собою модель особистості, яку формує людина, та яка створюється шляхом збору, зберігання та аналізу цифрових даних про цю особистість. Ця інформація може стосуватися абсолютно різних аспектів цифрової ідентифікації: дата народження, нікнейм, фотографія профілю, а також публікації, на які певна особистість спрямовує свою віртуальну активність.

Основна особливість цифрової особистості полягає в тому, що на деяких мережевих платформах цифрова особистість може бути повністю створена відповідно до бажань користувача, а також неодноразово змінена. Таким чином, цифрова ідентифікація не обов'язково буде співвідноситися з ідентифікацією користувача з реального соціального простору. Поняття цифрової ідентичності тісно пов'язане з поняттям анонімності в тому контексті, що в обох випадках люди прагнуть контролювати інформацію, яку вони передають та отримують.

Визначення анонімності дуже неоднозначно у зв'язку з неоднозначністю самого феномена. Б.Годдін вважає, що анонімність можна

визначити як відсутність справжньої ідентичності, при тому, що ідентичність визначається як певний обсяг унікальних характеристик, які необхідні для відстеження, розпізнавання кого-небудь, а цифрова ідентичність — як обсяг цифрової інформації, яка створює образ індивідуальної ідентифікованої людини [28]. М.Паскуда визначив анонімність в мережевому просторі як «онлайн діяльність від імені, яке не пов'язане з громадянською, "офіційною" ідентичністю, реальною ідентифікацією в соціальному просторі, або діяльність під псевдонімом» [42, с. 8].

В загальному вигляді ми можемо визначити анонімну діяльність в Інтернет-просторі як діяльність на мережевих ресурсах від імені, яке неможливо пов'язати з реальною ідентифікованою людиною через відсутність технічних механізмів для цього. Мережевими ресурсами є всі платформи комунікації — різноманітні сайти, форуми, соціальні мережі, блоги, інтернет-месенджери тощо. Діяльність на мережевих ресурсах охоплює все різноманіття дії в мережевому середовищі: реєстрація профілю в соціальному середовищі, написання коментарів, вступ до групи на веб-платформах, обговорення на форумах тощо.

Співвідношення між бажанням не розкривати свою справжню особистість, особисту інформацію та можливостями зберегти свою анонімність вказує на певний рівень конфіденційності. Конфіденційність (privacy) охоплює безліч методів та технологій, які використовуються для захисту конфіденційних даних. Конфіденційність в інтернет-просторі містить в собі можливість контролювати, яку інформацію людина розкриває про свою особистість через Інтернет, та контролювати, хто може отримати доступ до цієї інформації. У загальних рисах конфіденційність в мережевому просторі може бути визначена як зацікавленість або необхідність людини в нерозголошенні особистої інформації, що може використовувати анонімність як метод для збереження конфіденційності.

2.2. Псевдонімність

Поряд з анонімністю необхідно визначити поняття псевдонімності — це такий тип анонімної діяльності в інтернет-просторі, яка здійснюється з використанням псевдоніма. Б.Годдін визначає псевдонім як фіктивний відмітний знак, який, на відміну від повної анонімності, може привести до певної існуючої реально особи або вказати на деяку інформацію про неї [28]. Анонімність передбачає неможливість зв'язати інтернет-користувача з іншими формами його ідентичності, в той час як псевдонімність може бути пов'язана з певними ідентифікаторами. Дійсно, особистість може не передбачати анонімність та/або не прагнути до неї: ідентифікація через цивільне ім'я безпосередньо відсилає до соціального аспекту певної особистості, до обсягу особистої інформації. Прикладом цього можуть служити профілі в соціальних мережах, які створюються з метою «продовження» соціального життя в віртуальному просторі. Найбільш часто сьогодні користувачі інтернет-платформ звертаються саме до часткової або повної псевдонімності.

М.Фрумкін визначає чотири типи анонімного та псевдонімного: відстежувана анонімність (*traceable anonymity*) не дає іншим користувачам віртуальної спільноти ніякої інформації про анонімного користувача, що дозволяє зберегти конфіденційність всередині певної інтернет-платформи, проте самі інтернет-платформи та інтернет-провайдери зберігають вихідні дані особистості до надання користувачеві анонімного для спільнот нікнейма, профілю; невідстежувана анонімність (*untraceable anonymity*), другий тип, який не передбачає збереження жодного запису або способу доступу до походження анонімного акаунта або анонімного повідомлення; невідстежувана псевдонімність (*untraceable pseudonymity*) передбачає формування якоїсь ідентифікації на певній інтернет-платформі або декількох з них, що дозволяє іншим користувачам ідентифікувати цього користувача всередині віртуальної спільноти, проте не мати зв'язку з реальною ідентичністю цього користувача; відстежувана псевдонімність (*traceable*

pseudonymity) видозмінює невідстежувану псевдонімність за допомогою встановлення зв'язку між псевдонімом та реальною ідентичністю [27].

Таким чином, анонімність, по-перше, може бути повною, "чистою", що передбачає створення анонімного профілю, відсутність постійних акаунтів та постійного спілкування на платформі під одним акаунтом — псевдонім не може бути взагалі пов'язаний з будь-якою формою ідентифікації особистості, або, по-друге, вона може співвідноситися з псевдонімністю, що передбачає використання постійного псевдонімного акаунта, який в різних пропорціях надає конфіденційну інформацію. «Анонімний псевдонімний акаунт» — певна «суміш» анонімності та псевдонімності — є формою цифрової ідентифікації, яка найбільш часто зустрічається, тому що дозволяє поєднувати соціальну реальну діяльність, контакти та комунікацію з їх онлайн формами, а також, при необхідності, здійснити дії та вести спілкування, маючи можливість контролювати обсяг особистої інформації, що надається іншим. Надалі в даній роботі я буду використовувати термін анонімності та анонімного акаунта, маючи на увазі, що в кожному окремому випадку йдеться про якусь суміш анонімної та псевдонімної поведінки, про певний континуум анонімності.

2.3 «Континуум анонімності»

Анонімність та псевдонімність в інтернет-просторі існують не як чітко розділені елементи. Все більше дослідників, розглядаючи складності практики анонімності, звертаються до тези про «континуум анонімності», яка втілює ідею безлічі відтінків ідентифікації, можливих в інтернет-просторі. Дж.Бейер у своєму дослідженні 2012 року прагнула класифікувати різні сайти на анонімні та неанонімні, однак замість чіткої «так/ні» таблиці, вона прийшла до континууму анонімності [16]. Наприклад, сайт, який позиціонує себе як абсолютно анонімний веб-форум — 4chan.org, не є повністю анонімним, бо він відстежує IP-адреси, що потенційно може вказати на місцезнаходження користувача, проте сам сайт є досить анонімним для

більшості користувачів, які не володіють навичками для розпізнавання IP-адреси.

Х.Цянь та К.Скотт розглядають континуум анонімності як складний простір взаємодій, який формується можливостями комунікаційних технологій, а тому розгляд анонімності в контексті дихотомії анонімний/неанонімний не відповідає сьогodнішнім технологічним ресурсам [46]. Сучасні інструменти та технології соціальних мереж, різних віртуальних спільнот дозволяють користувачам самостійно регулювати певний рівень анонімності, виходячи з тієї кількості реальної ідентифікуючої інформації, яку хоче надати користувач. Крім того, автори відзначають, що ступінь анонімності в сучасних умовах формується не тільки користувачем, але й модераторами та власниками мережевих ресурсів, які можуть не поширювати інформацію про політику конфіденційності публічно.

Е.Нагель та Дж.Фріс, посилаючись на дослідження Дж.Донат про соціальні мережі, також розглядають анонімність як континуум, який простягається від повної анонімності до самостійного відкритого називання себе [41]. Вони стверджують, що перебування в континуумі анонімності дозволяє користувачам розширювати уявлення про свою ідентичність, розширюючи та обмежуючи вхід у своє конфіденційне поле за власним вибором. Крім того, користуючись механізмами анонімності та псевдонімності, користувач отримує можливість вивчати різні прояви своєї ідентичності та експериментувати з ними в просторі, який надає більшу безпеку в порівнянні з простором соціального реального світу, в якому деякі форми самопрезентації сприймаються негативно [41].

Континуум анонімності чітко простежується на прикладі соціальних мереж, які дотримуються різної політики конфіденційності. Поведінка людей на сайтах соціальних мереж різниться в залежності від того, чи дозволено користувачам спілкуватися через віртуальну ідентифікацію, тобто від того, чи прагне мережа прив'язати користувача до його однієї особи соціальної реальності чи ні. Соціальна мережа Facebook прописує в угоді про політику

конфіденційності, що очікує від користувачів реєстрацію їх «реальної» особистості, використання цивільного, офіційного імені та власних фотографій. Компанія стверджує, що вона не дозволяє використовувати псевдоніми, щоб запобігти залякуванню, переслідуванню, шахрайству та злочинній поведінці з боку анонімних облікових записів. У 2015 році Facebook позначив як підозрілі профілі транссексуалів та драг-квін, які використовували свої сценічні імена замість своїх офіційних імен, та зажадав від них надати документацію для підтвердження своєї особистості. Але учасники даної ситуації заявили, що для них важливо мати можливість на платформі найбільшої соціальної мережі представитися не юридичним ім'ям [35]. Хоча Facebook наполягає на тому, що з того часу розширив свої угоди, критики стверджують, що політика щодо імен створює проблеми для уразливих користувачів, які не використовують юридичні імена в цілях безпеки та конфіденційності. Інші соціальні мережі також кодують різні методи ідентифікації в структурі сайту. Соціальний новинний сайт Reddit наполягає на тому, щоб користувачі використовували псевдонім, який, однак, буде незмінним та буде ідентифікувати їх для інших користувачів. 4chan та інші анонімні форуми не використовують псевдоніми або фотографії профілю: всі повідомлення повністю анонімні.

Таким чином, розгляд континууму анонімності та різноманітності механізмів анонімності та псевдонімності на різних сайтах дозволяє зробити висновок про те, що користувач стикається з різними можливостями представити свою реальну або нову ідентичність в мережевому просторі. У той час як сувора політика конфіденційності та анонімності/псевдонімності часто обмежує діяльність користувачів мережі, континуум анонімності відкриває доступ до самопрезентації в різних образах та прояву різних сторін особистості, які користувач бажає розкрити тільки в умовах анонімності або псевдонімності. Анонімність в різних своїх проявах впливає на поведінку людини всередині віртуальної спільноти та на інтернет-платформах, і саме ці зміни я б хотіла розглянути в наступному розділі роботи.

Розділ 3. Психологічно-соціальний аспект розгляду анонімності. Анонімність як особливий мотиватор поведінки

Зміна соціальної поведінки під дією певного рівня анонімності розглядалася великою кількістю дослідників та філософів в межах вивчення масових товариств. Г.Ле Бон, Х.Ортега-і-Гассет, С.Московичи приписували анонімним членам натовпу розвиток імпульсивної поведінки, підвищення агресивних настроїв. Ф.Зимбардо вже в 1970-х роках припустив, що анонімність сприяє деіндивідуалізації та антисоціальної поведінки, зменшенню сприйняття заборон та норм, зниженню здатності до саморефлексії. Сьогодні дані висновки про вплив анонімності на особистість в масових спільнотах можуть бути співставлені зі змінами поведінки людини в віртуальних спільнотах. Одними з перших філософів, що звернули увагу до соціальних проблем взаємодії в мережі Інтернет були феноменологічні філософи техніки А.Боргман і Х.Дрейфус. Х.Дрейфус критикував Інтернет-простір за те, що він позбавляє людей повністю втіленої присутності [24]. Він вказує на те, що анонімність, відсутність відчуття наслідків позбавляють взаємодії в Інтернеті ризику, а без ризику в електронному просторі не може бути справжнього змісту або відповідальності. Дослідження, що проводяться соціальною мережею Facebook, підтримують побоювання цих філософів та демонструють, що коментарі, які залишені анонімними користувачами, є менш «якісними» — вони частіше мають ознаки агресії, образи інших користувачів [51].

Можливості багатопланової віртуальної ідентифікації, можливості вийти з жорстких меж бажаної та нормованої соціальної поведінки і, завдяки анонімності, можливості не нести за діяльність або слова поза цими межами відповідальності породжує в кіберпросторі підстави для зміни поведінки користувачів. На думку А.Жичкіной, саме анонімність несе для спілкування, опосередкованого мережею, цілий ряд психологічних наслідків. По-перше, при втраті більшої частини спектра невербальних засобів спілкування, людина отримує можливість приховувати справжні почуття і виражати

почуття, які вона в цей момент не відчуває. Фізичне неподання, псевдонімність і анонімність позбавляють значення цілий ряд бар'єрів спілкування, обумовлених такими характеристиками партнерів комунікації, які виражені їхньою статтю, віком, соціальним статусом, зовнішньою привабливістю, невербальною компетентністю тощо [3]. Другим наслідком є можливість створювати про себе будь-яке враження за своїм вибором, конструювати свою ідентичність за власним бажанням, незалежно від соціальних ролей в реальному світі [3]. Крім того, Н.Н.Королева бачить у віртуальному спілкуванні психологічну особливість сприйняття часу, простору і контактів: користувач не обмежений географічним полем, він може переміщатися між різними віртуальними спільнотами, він може продовжувати сесію віртуального спілкування безмежну кількість часу, він має необмежену доступність користувачів, може здійснювати безліч різноманітних контактів з великою кількістю людей, перепробувати та змінити безліч варіантів спілкування [6]. В даному контексті можна згадати «синдром відеоігри»: він полягає в тому, що гравець, користувач, бачить свої дії у віртуальному просторі в межах закритої системи, наслідки за дії усередині якої не поширюються на інші його активності, і його «смерть» — порушення норм, образи — всередині цієї системи також не впливають на його ідентичність за її межами.

Н.Н.Королева звертає увагу на те, що анонімність знижує рівень психологічного та соціального ризику в спілкуванні, в поведінці проявляється велика розкутість, психологічна безпека [6]. Я вважаю, даний наслідок може бути розглянутий як з негативних, так і з позитивних сторін: анонімність може бути причиною для прояву соціальної ненормативності, яка може проявлятися в агресивній поведінці, безвідповідальності учасників; з іншого боку, анонімність забезпечує простір психологічної безпеки, що дозволяє, наприклад, людям зі стигматизованою соціальною ідентичністю приєднуватися до інтернет-груп, отримувати в них підтримку, шукати однодумців, розширювати свою реальну соціальну ідентичність.

3.1. Ефект мережевої дезінбації

Віртуальна комунікація є сприятливим середовищем для прояву тих властивостей та потенціалів особистості, які можуть бути недоступними в реальному спілкуванні. Це явище має назву «the online disinhibition effect», що я пропоную перекласти як «ефект мережевої дезінбації». Дезінбація — термін когнітивних наук, який означає відсутність стриманості, що впливає на інстинктивні, емоційні, когнітивні та сприйнятливі аспекти; коротко дезінбацію можна описати як відкидання гальмувань у соціальних обставинах. Дж.Сулер використовує термін «the online disinhibition effect» для опису зниження психологічних обмежень, бар'єрів, які часто служать як регулятори поведінки, що призводить до того, що в онлайн-соціальному середовищі люди поводяться так, як вони зазвичай не поводитися в реальному житті, висловлюють себе більш відкрито [50].

Дж.Сулер виділяє два типи даного ефекту: з одного боку, відбувається добродійна дезінбація (benign disinhibition) — можливість анонімності дає користувачам велику свободу в розкритті своїх почуттів, прихованих емоцій, актів підтримки; вона дає можливість досліджувати різні аспекти своєї ідентифікації та її нові емоційні виміри. З іншого боку, існує токсична дезінбація (toxic disinhibition), яка характеризується проявами агресивності, ненависті, булінгу; вона не веде до особистісного зростання і зазвичай є наслідком задоволення негативних потреб, які часто не можуть бути задоволені в соціальному реальному житті без подальшого за цим покарання. Однак ці види дезінбації в багатьох випадках мають розпливчасті межі, залежать від культурної та ситуативної відносності та можуть змінювати один одного в залежності від контексту, субкультури тощо.

Дж.Сулер описує шість чинників, що послаблюють психологічні бар'єри, які блокують вихід прихованих почуттів і потреб [50]. Ці чинники перетинаються і взаємодіють один з одним, що призводить до більш складного посиленого ефекту. Основним фактором, що створює ефект мережевої дезінбації, є фактор дисоціативної анонімності (dissociative

anonymity) — переконаність людини в тому, що інші користувачі її не знають, не володіють особистою інформацією, понад ту, що розкрила сама людина; за бажанням людина може приховати частину або всю свою особистість, змінити її або придумати нову. Можливість частково або повністю відокремити свої дії в онлайн-просторі від своєї реальної особистості породжує те, що онлайн-самість стає самостійною, вона переймає на себе відповідальність за вчинені дії у віртуальному просторі, що наділяє людину відчуттям більшої свободи у висловлюваннях і діях.

Ще одним фактором ефекту мережевої дезінбації, який багато в чому пов'язаний з анонімністю, є фактор невидимості (*invisibility*). Анонімність, фізична неприсутність виступають захисним муром, що приховує дії користувача від очей більшості людей. Фізична неприсутність, невидимість знімає бар'єри вербального і невербального спілкування — користувач відходить від необхідності підтримувати зоровий контакт, він позбавляється невербальних ознак засудження або незгоди, що підвищує його впевненість і розширює межі ефекту мережевої дезінбації. Третім фактором є асинхронність (*asynchronicity*) — люди не взаємодіють один з одним в режимі реального часу, вони не отримують миттєву, часом неусвідомлювану реакцію від свого співрозмовника на свої слова чи вчинки. Дж.Сулер, посилаючись на дослідження психотерапевта мережевої взаємодії К.Мунро, описує ефект «вдар і біжи» ("emotional hit and run"), який також породжується асинхронністю — людина не отримує миттєвої реакції на слова або вчинки, а анонімність і невидимість можуть повністю виключити подальшу відповідальність за них, що дозволяє людині «втекти» від дискусії, відповідної реакції за емоційне або вороже повідомлення [50].

Четвертий фактор — соліпсична інтроекція (*solipsistic introjection*) — зміна сприйняття кордонів себе та інших користувачів у зв'язку з відсутністю візуального та аудіо контакту; користувачі створюють образ «уявного співрозмовника». У міру того, як створений персонаж стає все більш складним і суб'єктивно «реальним», людина може почати вважати, що сама

бесіда відбувається лише в уявному просторі. Свідомо чи несвідомо, люди можуть відчувати, що уявні персонажі, яких вони «створили», існують в іншому просторі, у вигаданому вимірі, який відокремлений від вимог і обов'язків реального світу, що дає відчуття безпеки, свободи та дозволяє, не соромлячись, говорити та робити те, на що не наважуєшся в реальності. Це відчуття уявного простору є п'ятим чинником ефекту мережевої дезінбації, який Дж.Сулер назвав дисоціативною уявою (dissociative imagination). Він посилається на припущення Е.Фінч, яка вивчала феномен крадіжки особистих даних в кіберпросторі та прийшла до висновку, що деякі люди розглядають своє онлайн-життя як свого роду гру з правилами та нормами, які не належать до повсякденного життя; як тільки вони вимикають комп'ютер, вони вважають, що можуть залишити позаду гру, ігрову ідентичність, зняти з себе відповідальність за те, що відбувається в уявному ігровому світі [50]. Шостий фактор сумарно відтворює всі попередні фактори — анонімність, невидимість, дисоціативну уяву, які проявляються в тому, що відбувається мінімізація влади, соціальний статус та його атрибути позбавляються пріоритетного значення, знижується боязнь несхвалення, незгоди чи покарання від "вищої", авторитетної особи.

Взаємозв'язок ефекту мережевої дезінбації та анонімності підтверджують різні дослідження на дану тему. Дослідження Х.Цяня і К.Скотта у 2007 році та Е.Холленбо у 2013, в яких вивчалася ступінь впливу анонімності на емоційне саморозкриття себе в блогах, показали, що блогери були більш відверті в умовах дисоціативної анонімності [46; 31].

Розгляд ефекту мережевої дезінбації та інших змін поведінки у віртуальному просторі допомагає по-новому подивитися на «онлайн-самість» людини, причини зміни її поведінки, спілкування і дії. Анонімність, фізична неприсутність, часові та просторові зміни, а також різні способи віртуальної комунікації та контексти її здійснення сприяють більш широкому розумінню ідентичності — як з негативних, так і з позитивних сторін.

3.2. Деіндивідуалізація в кіберпросторі

Теорія про ефект мережевої дезінбації представляє досить недавні дослідження і новий погляд на проблему впливу анонімності на ідентичність і поведінку. Класичною ж теорією з даного питання є теорія деіндивідуалізації, яка відсилає до філософських напрацювань ХІХ століття щодо впливу мас на особистість. Основна ідея цієї теорії полягає в тому, що індивідуальні норми однієї людини губляться, коли вона входить в досить велику групу. Анонімність і втрата особистої відповідальності змінює поведінку людини, яка стає схильною до масової поведінки, що дозволяє їй брати участь в діях, від яких у звичайних умовах вона утримується. Деіндивідуалізація є важливою частиною деперсоналізації, яка характеризується зниженим почуттям самоідентифікації, самосвідомості та більш низьким рівнем самоконтролю.

Найчастіше деіндивідуалізація в мережі може відбуватися несвідомо: цінності та установки людини формуються в залежності від тієї інтернет-культури, під впливом якої вона знаходиться. Прикладом цього може служити масовізація думок на будь-які теми в інтернеті: дуже часто користувач, не заглиблюючись у проблематику дискусії або суперечки, приймає позицію більшості та загальний настрій інших користувачів соціальної мережі. Анонімність і невидимість в такому випадку знімає з людей моральні обмеження і соціальний етикет, який регулює нашу поведінку в нормальних ситуаціях. Часто це призводить до такого явища як тролінг, яке більш детально я розгляну трохи пізніше.

Дж.Бішоп вважає, що деіндивідуалізація, яку можна спостерігати у тролінгу, призводить до прагнення підірвати впевненість в собі в інших користувачів, щоб отримати почуття задоволення [17]. Можна також припустити, що, якщо анонімність і невидимість позбавляють людину способу її індивідуальності, представлення її в соціумі як самостійного та незалежного дієвця, то людина сама не прагне в масових групах

висловлювати незалежну думку, вважаючи за краще підтримувати стратегію і висловлювання більшості.

Якщо ефект мережевої дезінбації може призводити як до позитивних, так і до негативних наслідків, то деіндивідуалізація в основному призводить до негативних явищ кіберагресії.

3.3. Кіберагресія як прояв негативних наслідків анонімності

Незважаючи на те, що інтернет-простір пропонує безліч можливостей розширення кола спілкування, розширення своєї ідентифікації, він може нести в собі й негативні наслідки, в тому числі певні форми віртуальної агресії, які багато в чому поширюються внаслідок анонімності та відсутності. Віртуальне спілкування стирає допустимі межі етичних стандартів взаємодії, і тоді для деяких людей образи, хамство і запеклість стають нормою. За результатами статистичного дослідження Pew Research Center, 73% дорослих користувачів Інтернету були свідками агресії в Інтернеті та 40% зазнали її особисто на собі [25]. Термін «кіберагресія» був введений доктором філософії Д.Шабро у 2007 році та був визначений як «форма девіантної поведінки в інтернет-середовищі» [10]. Більш детально кіберагресію можна визначити як будь-яку поведінку, що здійснюється за допомогою цифрових засобів з підключенням до мережі, окремими особами або групами, які передають ворожі або агресивні повідомлення, призначені для заподіяння шкоди чи дискомфорту іншим людям. Основними видами кіберагресії, згідно зі статистикою дослідження 2014 року, є образи, приниження, знуцання, викриття, маніпулювання, агресивні нападки, переслідування за допомогою комунікативних технологій [25].

Основними формами кіберагресії є тролінг, кібербулінг, кіберсталкінг, інші ж форми кіберагресії можна звести до вищеперелічених і визначити через них. Тролінг (trolling) є формою реалізації мовної кіберагресії: навмисним актом публікації підбурливих, образливих коментарів, які дуже часто не стосуються справи, контенту з агресивним змістом на різних

інтернет-платформах або в особистому мережевому спілкуванні, метою якого є емоційна реакція з боку інших користувачів. Однією з форм тролінгу є флеймінг (flaming) — свого роду «словесна війна» в публічному просторі мережевих платформ, метод спілкування, що супроводжується яскраво вираженою мовною агресією, особистими атаками, образливими коментарями, що не має чіткої мети та часто триває як «суперечка заради суперечки».

Кібербулінг (cyberbullying) — акт агресії, знущання, образи над людиною або групою осіб, часто здійснюється анонімно за соціальних мереж, інтернет-платформ або в особистому спілкуванні через цифрові пристрої, мережеві платформи. Т.А.Фетісова визначає кібербулінг як «умисні агресивні дії з метою нанесення психологічної, систематично здійснюються групою осіб або індивідом з використанням електронних форм взаємодії та мобільного зв'язку проти жертви» [10]. До основних різновидів кібербулінгу відноситься харасмент — образливі повідомлення незнайомих людей конкретній жертві; очорнення — виставляння жертви в негативному світлі за допомогою публікації неправдивої чи негативної інформації, що принижує; публічне розголошення особистої інформації про жертву в Інтернеті; кіберсталкінг (cyberstalking) — акт переслідування будь-кого в Інтернеті, часто здійснюється анонімно через електронні засоби і мережеві платформи з метою виявлення його конфіденційної інформації, маніпулювання тощо.

Мотиви агресії в інтернет-просторі в цілому збігаються з мотивами агресії в соціальному реальному просторі: згідно з дослідженнями Л.Комптон, М.Кемпбелл і А.Мерглер, які у 2014 році опитували студентів, батьків і вчителів про їхні сприйняті мотивів кібербулінгу, основними мотивами були названі прагнення до влади, статусу, прагнення повеселитися, позбавлення від нудьги, отримання соціального контролю, а також використання кіберагресії як "безпечний" засіб помститися [21].

Багато дослідників відзначають схожість агресії, що проявляється в соціальному просторі, з агресією, яка проявляється в віртуальному просторі,

проте анонімність, невидимість, відчуття більшої свободи та меншої відповідальності, а також технічні інструменти спричиняють появу відмінних рис онлайн-агресії. Простір мережі передбачає глобальну комунікацію і, як наслідок, глобальну агресію. Якщо агресія в реальному соціальному просторі трапляється в більшості випадків між знайомими людьми, то агресія в віртуальному просторі не має кордонів, може поширюватися між людьми різних соціальних класів, різного віку, країн тощо. Глобальний характер поширення агресії доповнюється неймовірною швидкістю поширення агресивних повідомлень завдяки технічному обладнанню. Мережа і мережева комунікація «узурпували» право на поширення засудження у традиційних засобів масової інформації: прагнення засуджувати та проявляти агресію відтепер примножується на технології, що дозволяє багаторазово збільшити обсяги агресії, зробити її неконтрольованою.

Принциповою особливістю кіберагресії є відчуття захищеності людини, яка агресивно поводить, а також відсутність регламентованих норм поведінки, етичних порядків і правової відповідальності для більшості випадків. Дослідження К.Барлетт і Д.Джентіле вказали на існування прямого зв'язку між анонімністю і рівнем кіберагресії [14]. Результати їхнього дослідження підтвердили теоретичні постулати про анонімність як фактор ефекту мережевої дезінбації Дж.Сулера про те, що анонімність і невидимість для інших користувачів, яку усвідомлює агресор, провокує поведінку кіберагресії: віра в те, що хтось є анонімним і не може бути покараний за агресивну поведінку в Інтернеті, і розуміння того, що будь-хто, незалежно від того, наскільки він фізично сильний, який соціальний статус має, може атакувати інших в Інтернет-просторі, призводить до збільшення обсягів кіберагресії [14].

3.4. Формування вільного простору соціальної взаємодії як позитивний наслідок анонімності

Поширення форм кіберагресії, асоціальної та образливої поведінки на інтернет-платформах і в соціальних мережах все частіше мотивує дослідників звертатися саме до негативних наслідків анонімності, однак безсумнівним є те, що анонімність має і позитивні наслідки.

По-перше, анонімність звільняє людей від дискримінації. Приховуючи свою особистість людина звільняється від дискримінації за ознакою статі, раси, віку, етнічної приналежності, інвалідності, привабливості, соціального статусу тощо. Інтернет-анонімність діє як щит, за яким люди можуть спілкуватися на умовах рівності та безпеки. Анонімність в цьому випадку виступає мотиватором вільного спілкування, яке не відбувається під тиском влади, авторитету тощо.

По-друге, анонімність відводить увагу від індивідуальних особливостей і повертає увагу до групової ідентифікації, дуже часто беручи до уваги групи, які стигматизуються в суспільстві, що дозволяє анонімним користувачам уникати деяких руйнівних наслідків нетерпимості та забобонів. Анонімність і прихована ідентифікація відводять увагу від стереотипів і дискримінації, зосереджуючись на обговорення «по суті»; при відсутності особистої інформації про інших користувачі повинні зосереджуватися на проблемі, тексті, тезах. Звертаючись до термінології Ю.Габермаса, можна сказати, що в інтернет-просторі може скластися «ідеальна мовна ситуація» — спілкування стає вільним, користувачі отримують рівні можливості висловлювати свою думку, відповідати на висловлену думку інших. Таким чином, анонімність в мережевому просторі дозволяє дізнатися, що насправді думають люди, за що вони готові боротися, не побоюючись репресій.

Інструменти анонімності корисні також відносно особистісного зростання, вони роблять людей більш відкритими, дозволяють їм говорити на теми, які в реальному просторі табуються. К.Кристоферсон, посилаючись на дослідження Д.Педерсона, описує кілька факторів особистісних змін, які пов'язані з анонімністю: відродження, катарсис і автономія [20]. Відродження ґрунтується на почуттях активного споглядання своєї ідентичності, елементи

якої можуть «реабілітуватися» через відкриту анонімну комунікацію і почуття безпеки. Катарсис був визначений як безперешкодне вираження думок і почуттів: анонімність дозволяє не побоюватися бути ідентифікованим і соціально оціненим. Автономія передбачає можливість експериментувати з новою поведінкою, не побоюючись соціальних наслідків та отримання негативної оцінки з боку тих, кого людина знає в реальності.

Дані позитивні риси анонімності особливо простежуються на прикладах віртуальних груп або спільнот, в яких відбувається обговорення стигматизованих тем або соціальних груп. Дослідження К.МакКенна показує зміни в поведінці представників ЛГБТК+ спільноти від анонімної комунікації в групах взаємопідтримки [40]. Його дослідження проводилися в 1998 році, коли велика частина ЛГБТК+ спільноти перебувала в положенні маргінальних груп, а єдиними платформами для анонімного спілкування були нечисленні чати в мережевому просторі. К.МакКенн виявив, що участь в подібних чатах і анонімних обговореннях дозволяли згодом частини досліджуваних не тільки розкриватися про свою орієнтацію всередині мережевого простору, але також робити відкриті визнання про свою сексуальну орієнтацію своїм друзям і родині [40].

Таким чином, можна зробити висновок, що анонімність в віртуальній комунікації дійсно здатна змінювати поведінку і сприйняття людей, вона знімає багато обмежень висловлювань, комунікації, взаємодії, що може призводити як до негативних, так і до позитивних наслідків. Анонімність, яка стимулюється невидимістю та відсутністю соціальних норм і ослабленням почуття відповідальності, може призводити до проявів кіберагресії та "винагороджувати" правопорушення. Однак крім цього, анонімність також може стимулювати свободу слова і вирази, надає можливість взаємодії з особистим досвідом інших користувачів, надає можливість бути відкритим, чесним. Такий наслідок анонімності як свобода вираження і слова тісно пов'язаний з правовим полем анонімної комунікації та взаємодії як елементом здійснення демократичних цінностей.

Розділ 4. Правовий аспект розгляду анонімності. Анонімність як елемент здійснення прав людини

Анонімність не є новим явищем у правовій історії: вона фігурує паралельно з правом на свободу слова, свободу вираження і захист особистості; саме закритість списків учасників організацій, що боролися за права людей, їхня анонімність, певний рівень анонімності в натовпі громадських рухів свого часу зіграли важливу роль для закріплення багатьох пунктів Декларацій про права людини, Законів про протидію дискримінації тощо. Сам механізм анонімності часто ставав і стає основним елементом поліпшення правової бази та просування демократичних цінностей, він має вирішальне значення в широкому спектрі способів участі в політичному житті. У багатьох сферах суспільства анонімність стає ключовим елементом здійснення прав людини: право на таємне голосування, право на висловлювання думок без побоювання переслідувань, право на зібрання та на мирний протест, право на недоторканність приватного життя і захист конфіденційної інформації, і багато інших прав повністю або частково неможливі без механізмів анонімності, які є гарантією здійснення основних прав людини та громадянина.

Цифрові технології та мережевий простір примножили можливості анонімності у сфері реалізації прав і свобод людей, вони загострили також проблему контролю з боку державних структур і втручання в особисте життя. Нові умови підіймають проблему реалізації багатьох прав у віртуальному середовищі та мережі Інтернет. У правовому переліку щодо соціальної реальної взаємодії існує безліч законів та декларацій про право на свободу висловлювань, свободу думок і вираження, проте підіймається питання про те, в якій мірі ці права реалізуються в Інтернет-просторі і якими законними постановами та актами вони будуть регламентуватися в Інтернеті та соціальних мережах. Крім того, це питання загострюється необхідністю законодавчих, правоохоронних структур та різних правових організацій збалансувати фундаментальну природу прав людини та громадянина, яка

повинна поширюватися на мережеву взаємодію та Інтернет-комунікацію, з потенційними кібернебезпечностями індивідуальної, групової та глобальної взаємодії. Формування правової бази з питань забезпечення анонімності має зосередитися на питаннях співвідношення дій в віртуальному і реальному просторі, що передбачає збалансування правових норм цих просторів, регулювання застосування заходів санкцій та притягнення до правової відповідальності щодо дій, здійснених в мережевому просторі.

Правові документи про свободу слова, недоторканності приватного життя та інші існують вже багато років, в той час як правова база законів віртуального простору розробляється тільки недавно, і темпи її розробки та прийняття не встигають за темпами поширення Інтернет-простору, мережевої злочинності тощо. Крім того, можна говорити про те, що правова база регулювання діяльності та комунікації в віртуальному просторі розробляється в основному на міжнародному рівні, в якості прецедентів в Європейському суді через те, що національні законодавства не володіють достатньою базою для регулювання питань захисту прав людини в Інтернеті, залучення до відповідальності. Загальна декларація прав людини ООН стверджує право на приватне життя, право на свободу думок і їх вільне вираження, право таємного листування тощо. Міжнародний пакт про громадянські та політичні права, Конвенція про захист прав людини та основних свобод, Американська конвенція про права людини, Міжамериканська комісія з прав людини, Африканська хартія прав людини та народів та інші міжнародні документи також містять аналогічні формулювання. Резолюції Ради ООН з прав людини 2012 і 2014 постановили, що ті права, які людина має в офлайн середовищі, повинні також захищатися і в онлайн середовищі. У 2014 році Європейський Союз випустив Посібник з прав людини в галузі свободи вираження думок в Інтернеті та поза ним, яке покликане сприяти просуванню свободи слова та її захисту [54]. І все ж ці міжнародні акти не прописують детальну інформацію прав на шифрування інформації, прав на анонімність, прав провайдерів та інтернет-ресурсів не

передавати в державні структури інформацію про анонімних користувачів, що робить всі ці нормативні акти в питанні реалізації прав в Інтернет-просторі розмитими та іноді безпідставними.

У травні 2015 року Спеціальний доповідач ООН з питань про заохочення і захист права на свободу поглядів і їх вільне вираження опублікував новаторську доповідь про анонімність і шифруванні в Інтернеті [32]. У доповіді чітко вказується, що спроби урядів отримати доступ до прихованих повідомлень людей або спроби навмисно послабити стандарти шифрування є порушенням міжнародного права. Однак водночас на національному рівні приймаються закони та поправки, які суперечать цим міжнародним актам, адже вони вимагають від людей, інтернет-компаній розкривати свою особистість в певних ситуаціях. Деякі країни приймають закони, що обмежують свободу в віртуальному просторі та забороняють анонімне користування інтернет-ресурсами. У грудні 2012 року Китай оголосив, що він прийняв політику, що вимагає від усіх веб-користувачів реєструвати свої справжні імена в інтернет-провайдерів, що, як побоювалися деякі активісти, задушить політичну опозицію в країні. У 2014 році Росія прийняла закон, згідно з яким блогери, які мають понад 3000 щоденних читачів, повинні зареєструватися в державному органі та внести свої імена та контактну інформацію.

Дані приклади тільки підкреслюють важливість питань захисту анонімності та шифрування в міжнародному і національному праві, а також питань розробки та впровадження обмежень для засобів анонімності та шифрування і їх сумісності з правом на свободу вираження. Крім того, необхідно враховувати той факт, що Інтернет і соціальні мережі є глобальним простором і не є «територіальною» структурою будь-якої певної країни, тому діяльність в даному просторі досить часто неможливо визначити через юрисдикцію певної країни, а надання правового захисту або накладення правої відповідальності не може посилатися виключно на федеральні закони. Таким чином, анонімна діяльність часто виходить за межі

досяжності окремих державних структур, що тільки загострює необхідність розробки міжнародної правової бази.

4.1. Анонімність та право на свободу слова та вираження

Поширення Інтернету і нових технологій створили нові можливості для спілкування і свободи вираження думок, включаючи можливість повної анонімності. Анонімність має основоположне значення для повного здійснення права на свободу вираження поглядів, яке закріплене в 19 статті Загальної декларації прав людини, а також в інших міжнародних деклараціях. Анонімність заохочує свободу слова і здатність висловлювати свою думку з приводу непопулярних ідей, висловлювати непопулярні політичні погляди, викривати корупцію в уряді, шукати інформацію щодо делікатних тем без подальшого розголошення про це. Анонімність і шифрування мають вирішальне значення для розширення можливостей та захисту груп ризику. Спільноти, які соціально і політично виключені та стикаються з дискримінацією або насильством, часто звертаються до Інтернету як до «безпечнішого» простору. Анонімність є важливим фактором, що забезпечує право на свободу асоціацій і зборів в Інтернеті та право на свободу від дискримінації. Анонімність також нерозривно пов'язана з правом на недоторканність приватного життя. Ці приклади дозволяють розглядати здатність спілкуватися анонімно як частину основного права на свободу слова.

Анонімність особливо важлива в репресивному середовищі, в якому відсутність анонімності може привести до кримінальних звинувачень або інших правових або негативних неправових наслідків, а іноді й до ризику для життя. У 2015 році Спеціальний доповідач з питань свободи думок і вираження підкреслив, що анонімна мова необхідна для правозахисників, журналістів і учасників протесту. Він зазначив, що будь-яка спроба заборонити або перехопити анонімні повідомлення під час протестів є невинуватим обмеженням права на свободу мирних зібрань відповідно до

Загальної декларації прав людини та Міжнародного пакту про громадянські та політичні права [32]. В даному контексті анонімність проявляється як негативна свобода — як засіб стати «невидимим» та уникнути виявлення для несправедливого покарання. Цей же елемент анонімності можна спостерігати на прикладах соціально-політичних повстань і висловлювання непогоджень. В даному контексті доречно буде розглянути термін «Twitter Revolution», який вказує на важливість соціальних мереж і анонімного або псевдонімного медіапростору для здійснення революцій і протестів. Основна перевага даного феномена полягає в наданні доступу до безпечнішого і вільного простору висловлювань та поширення інформації, що підвищує інформованість і увагу не тільки населення країни, в якій відбувається протест, але також і міжнародних агентів, міжнародних ЗМІ та користувачів з усього світу.

Найбільш сучасним прикладом можуть слугувати події в Гонконзі у 2019 році. Протестуючі Гонконгу використовували соціальні мережі як платформи анонімної комунікації та передачі інформації, щоб їх не впізнали та не заарештували поліцейські. Трейсі Ло, старший викладач з управління комунікаціями в Сінгапурському університеті, стверджує, що соціальні мережі зіграли «більш очевидну» роль в протестах 2019 року, ніж будь-коли раніше: вони змінили спосіб документування історії, служили в якості поширення інформації, мобілізації демонстрантів і запобігання затримань [47]. Демонстранти також продемонстрували підвищену обізнаність про шифрування та анонімність. Анонімність дозволила їм обмінюватися новинними стрічками, інформацією про дії поліції та протестуючих, «розвідкою» про різні поточні та майбутні заходи. Такі соціальні мережі, як Instagram і Facebook, послужили платформами для демонстрації агітаційних плакатів, а також фото- та відеоматеріалів, які свідчили про насильство і жорстокість з боку поліції. Протести в Гонконзі, згідно з дослідженнями Трейсі Ло, значно підвищили трафік відвідування на різних онлайн-форумах, обсяги завантаження різних месенджерів і додатків для комунікації, а також,

що найголовніше, різних додатків-анонімайзерів і різних додатків для підвищення анонімності, які дозволяють приховувати місцезнаходження та особистість користувача [47]. Сервіси анонімізації засновані на концепції поширення інформації про маршрутизацію, що має на увазі те, що під час передачі даних є практично невідомий шлях між джерелом передачі та пунктом призначення. Основними сервісами анонімізації є анонімайзери, проксі-сервери, VPN-тунелі, і їх основні функції полягають у зміні IP-адреси, місцезнаходження, унікальної адреси пристрою або сервера тощо. Приклад протестів в Гонконзі показує, що все більша частина населення, особливо — молодого населення, обізнана про можливості віртуальних платформ для різної діяльності, а також про можливості здійснювати цю діяльність анонімно.

Таким чином, анонімність є найважливішим елементом здійснення права на свободу слова як в реальному соціальному світі, так і в віртуальному просторі, який служить безпечним місцем для висловлювання, пошуку підтримки та формування опозиційних груп. Для здійснення права на свободу слова необхідно брати до уваги ступінь надання права на недоторканність приватного життя у мережі.

4.2. Анонімність і захист конфіденційних даних. Право на недоторканність приватного життя

На національному рівні право на недоторканність приватного життя охоплюється більшістю конституцій. На міжнародному рівні це описано в Римських і Страсбурзьких договорах (Європейська рада) та Договорі про громадянські та політичні права (ООН). Регулювання в цій сфері часто ґрунтується на восьми принципах, сформульованих Європейською Радою ще в 1980 році. Найбільш важливими з них Я. ван Дайк вважає принцип обмеження використання — мінімально можлива кількість персональних даних має збиратися і використовуватися; принцип визначення мети — тільки особисті дані для строго визначених цілей повинні бути зібрані та

оброблені; якість — особисті дані повинні бути правильними та добре захищені; принцип відкритості — залучені люди мають право знати, які особисті дані збираються, з якою метою, хто має до них доступ, кому вони передаються [23, с.150].

В Європі захист приватної інформації, як правило, сильніший, ніж в Сполучених Штатах і Азії. Саме Рада Європи вже у 2003 році прийняла Декларацію про свободу спілкування в Інтернеті, яка закликала поважати бажання користувачів Інтернету не розкривати свою особистість, щоб забезпечити захист від онлайн-спостереження і розширити свободу вираження інформації та ідей. Європейський парламент у 2013 році схвалив оновлення закону Європейського Союзу про конфіденційність даних, згідно з яким компанії, що збирають приватні дані про громадян, повинні вжити заходів для анонімізації цих даних. У доповіді Спеціального доповідача з питань свободи інформації за 2013 рік підкреслювалась важливість взаємозв'язку між правами на недоторканність приватного життя і свободою вираження думок в кіберпросторі [34]. Європейський суд визнав важливість анонімності для прав на свободу вираження думок і недоторканність приватного життя. Одночасно, Суд ясно дав зрозуміти, що анонімність не є абсолютною і може бути обмежена для захисту інших законних інтересів. Зокрема, він заявив, що анонімність і конфіденційність в Інтернеті не повинні спонукати держави відмовлятися захищати права потенційних жертв.

У сучасному світі, де більшість структур і сфер суспільства переходять у віртуальний формат, а онлайн-життя стає невіддільною частиною життя великої кількості людей, інформація стає активом, валютою, силою. Бази даних зараз є найціннішим продуктом, який необхідний всім підприємствам з продажу товарів і послуг. Підприємства швидко зрозуміли, що дані про клієнтів можна легко збирати в Інтернеті, і почали інвестувати в технології, що полегшують збір даних. Соціальні мережі надають величезний масив інформації та даних про мільйони користувачів, просто спостерігаючи за

діями користувача на веб-сайті, можна визначити реакції клієнтів, їхні інтереси та потреби.

Більшість користувачів Інтернету знають, що ключові елементи особистої інформації про них доступні в Інтернеті, і все більша кількість інтернет-користувачів (50% на вересень 2013 року) говорять, що вони стурбовані кількістю особистої інформації про них в Інтернеті [44]. У більшості країн світу існує закон про захист персональних даних — захист будь-якої інформації, яка відноситься до певної фізичної особи (суб'єкту персональних даних) або особи, яка визначається на підставі такої інформації, в тому числі її ім'я, дата і місце народження, адреса, сімейне, соціальне, майнове становище, освіта, професія тощо. Наприклад, в Україні, збір, зберігання і передачу персональних даних регулює безліч законів — "Про захист персональних даних», «Про електронну комерцію», Цивільний кодекс, однак українське законодавство не має конкретних нормативних актів, спрямованих на регулювання поширення персональної інформації та можливості залишатися анонімними. Регулювання відносин в інтернет-просторі зараз відбувається за моделями офлайн-правового простору, що передбачає постійне підлаштовування, модернізацію, однак не формує і не забезпечує єдиної правової бази.

Законів Інтернет-регулювання конфіденційної інформації, які розглядали б виключно відносини в онлайн-просторі, майже немає. Винятками є, можливо, різні закони про cookies-файли, що я розгляну нижче, та невелика кількість законодавчих ініціатив в розвинених країнах. Можливо, відсутність нормативної бази пов'язана з досить складною структурою взаємодії в кіберпросторі, тонкощами процедури анонімізації, неможливістю точно провести межу між публічним і особистим, наприклад, в соціальних мережах. Дійсно, проблема розмежування публічної та особистої інформації у віртуальному просторі є дуже складною як для законодавчих ініціатив, комерційних проектів, так і для більшості користувачів в мережі. Навіть якщо користувач дотримується культури анонімності або псевдонімності в

соціальних мережах, він може, іноді не з власної волі, не дотримуватися подібних же заходів на інших мережевих ресурсах — під час онлайн-шопінгу, звернення до послуг онлайн-банкінгу, обов'язкової реєстрації на деяких сайтах або надання угоди про використання файлів cookie — невеликого фрагмента даних, який зберігається на комп'ютері або іншому пристрої, що використовується для відвідування сайту, і, крім технічного функціонала, служить для збору аналітичної інформації. Закон Євросоюзу про cookies набрав чинності у 2011 році та вимагав, щоб веб-сайт отримував дозвіл від відвідувачів перш, ніж записувати cookies на їхні комп'ютери, детально пояснюючи користувачам, яка саме інформація буде збиратися і використовуватися. Однак цей закон зараз виконують лише 11,8% сайтів з 10 000 перевірених дослідниками [22].

Веб-сайти використовують різні засоби, щоб порушувати правила ЄС і ускладнювати для споживачів відмову від відстеження. Найбільш поширеним способом обходу веб-сайтів в обхід законів ЄС є «неявна згода», якою користуються близько 32,5% досліджених сайтів [22]. Цей варіант передбачає, що якщо користувач не відреагував на спливаюче вікно, він дав свою згоду. Дані приклади показують, що обов'язок щодо захисту своїх конфіденційних даних лягає на самих користувачів. Все більше мережевих ресурсів привертають увагу до того, що необхідно підвищити свідомість і обізнаність користувачів та інтернет-спільноти про проблеми конфіденційності. Самі користувачі повинні проявляти більший інтерес до тієї технології та компаній, які прагнуть отримати персональну інформацію.

Дослідження 2013 року від Дослідницького центру П'ю показують, що близько 68% інтернет-користувачів вважають, що діючі закони недостатньо ефективні для захисту конфіденційності людей в Інтернеті [44]. Люди хотіли б контролювати свою інформацію, кажучи, що в багатьох випадках для них дуже важливо, щоб тільки вони або особи, які отримали від них дозвіл, мали доступ до такої інформації, як вміст їхніх електронних листів, їхніх контакти, місце, де вони знаходяться, коли вони онлайн, і вміст файлів, які вони

завантажують. Таким чином, питання про право на конфіденційність багато в чому поширюється не тільки на відповідальність зовнішніх агентів регулювання — держави, компанії, але і на відповідальність і бажання самих користувачів ділитися особистою інформацією, що має передбачати вибір — розкривати особисті дані чи ні, бути анонімним чи ні. В такому випадку функція зовнішніх агентів буде полягати в тому, щоб дати користувачам здійснювати даний вибір в межах закону.

4.3. Анонімність і право на захист честі, гідності та ділової репутації

Вимоги свободи слова, які формують комунікаційну культуру в Інтернеті, багатьма розглядаються як достатні підстави для захисту віртуального простору від правового регулювання, особливо щодо свободи слова та обговорення. Ілюзія повної анонімності, можливості псевдонімності та відчуття відсутності відповідальності дозволять деяким користувачам мережі Інтернет розміщувати образливі висловлювання та повідомлення, неправдиву інформацію, яка порочить честь і гідність громадянина або груп людей, об'єднаних спільними ідеологічними, релігійними або професійними інтересами, а також виявляти інші форми агресивної поведінки. Закони більшості країн світу передбачають покарання за подібні дії в соціальному реальному просторі, проте чи володіють держави та громадяни технічними та правовими можливостями поширювати подібну правову практику на віртуальну взаємодію? В даному питанні правове регулювання стикається з декількома проблемами. По-перше, всі позови, пов'язані з образою, клеветою і неправдивою інформацією, належать до справ приватного обвинувачення, тобто потерпілий має право на звернення до суду із заявою про притягнення особи до відповідальності, приклавши до заяви докази вчиненого щодо нього злочину. Доведенню підлягає факт нанесення образ конкретною особою, що часто неможливо здійснити в умовах анонімних користувачів і можливості видаляти повідомлення та опубліковану інформацію.

По-друге, образи в Інтернет-просторі в більшості випадків будуть розглядатися як публічні акти — пости в соціальних мережах, коментування, обговорення на форумах і блогах. На відміну від образ, які виражені особисто — через месенджери, особисті повідомлення, щодо публічних образ не завжди вдається визначити, чи були образливі слова спрямовані саме на жертву. Кривдник може сказати, що описував ситуацію або використовував оцінювальне судження про віртуальну ідентичність, віртуальний образ, який або зовсім не представляв людину, або представляв її частково через псевдонімність. Якщо кривдник не звертався до конкретного юридичного справжнього імені, то довести, що образи спрямовані на конкретну людину, майже неможливо. У разі образи через пряму вказівку або приватне повідомлення, кривдник може посилатися на те, що помилково вибрав адресата тощо.

По-третє, складність залучення до відповідальності кривдника полягає ще й в тому, що неможливо довести, що повідомлення або пост були написані та відправлені саме їм.

Ці пункти у своїй сукупності багато в чому визначають ще одну проблему правового регулювання права на захист честі та гідності — інтернет-платформи не просто глобальний простір, а простір з багатомільйонним обсягом користувачів, велика частина яких не пов'язує свою віртуальну ідентифікацію зі своєю реальною юридичною ідентифікацією, що унеможливорює процедуру правових наслідків. Жодна країна не володіє такими ресурсами правоохоронних і судових структур, щоб залучити до відповідальності всіх користувачів, які коли-небудь написали образливі слова в бік іншого.

Більшу увагу з боку правоохоронних органів заслуговують образи не в бік окремої особистості, а в бік соціальних груп, етнічних, релігійних тощо. Такі образи часто мають незліченну кількість кривдників, які об'єднуються в «групи ненависті». Анонімність, невидимість користувачів і глобальний характер інтернет-платформ зробили Інтернет і соціальні мережі ідеальним

інструментом для пропаганди ненависті, екстремізму. З кожним роком спостерігається колосальне зростання кількості різних форумів, веб-сайтів, онлайн-груп, пов'язаних з поширенням ненависті, екстремізму, расизму, сексизму тощо. Подібні веб-ресурси стають ключовим каналом, через який користувачі можуть передавати ідеї та переконання, мобілізуватися для демонстрацій і мітингів.

Показовим є судовий випадок *Yahoo! Inc. v. La Ligue Contre Le Racisme et l'Antisemitisme* — судовий розгляд між *Yahoo! Inc.* — друга за популярністю у світі пошукова система та між LICRA — Міжнародна ліга проти расизму та антисемітизму. Дві французькі студентські організації намагалися притягти до відповідальності *Yahoo!* за порушення французького закону, що забороняє продаж нацистських товарів, які сервіс розмістив на своєму веб-сайті аукціону. Французький суд ухвалив, що продаж нацистської атрибутики є образою колективної пам'яті країни. Хоча веб-сайт аукціону значився в Сполучених Штатах, французький суд постановив, що *Yahoo!* повинен виключити доступ французьких громадян до продажу нацистських товарів. *Yahoo!* стверджував, що його дії виходять за межі французької територіальної юрисдикції, оскільки матеріал був завантажений в США, де така поведінка захищена Першою поправкою.

Випадок з *Yahoo!* демонструє ще одну проблему правового регулювання права на захист честі та гідності та різних законів про протидію екстремізму і поширенню ненависті — він ілюструє культурну напруженість, властиву спробам екстериторіального регулювання комунікації та дії в Інтернеті. Спроби національних держав нав'язати географічні кордони віртуальному світу тільки підкреслюють труднощі, властиві європейським країнам, які прагнуть розширити свою юрисдикцію екстериторіально, забезпечуючи дотримання законів про зміст матеріалів, що завантажуються, за межі національних кордонів. Таким чином, національні держави просто не зможуть розширити правове регулювання за межі своїх власних

територіальних кордонів — мультиюрисдикція Інтернету підриває зусилля держав щодо розміщення географічного розмежування в кіберпросторі.

Конвенція Ради Європи про кіберзлочинність є першим багатостороннім договором, метою якого є боротьба з кіберзлочинністю шляхом розширення співробітництва між країнами, узгодження національних законів. Хоча Сполучені Штати не є членами Ради Європи, США підписали та ратифікували Конвенцію про кіберзлочинність. Однак підпис США був отримана тільки після того, як протокол про ненависть, образливі висловлювання був більшою мірою вилучений. Рада Європи ввела Додатковий протокол до Конвенції про кіберзлочинність, згідно з яким сторони зобов'язані криміналізувати дії расистського та ксенофобського характеру, що здійснюються за допомогою комп'ютерних систем і мережевих ресурсів. До початку 2010 року додатковий протокол був підписаний 32 державами-членами та ратифікований 15 державами. США відмовилися від підписання даного протоколу, оскільки це не відповідає їхнім конституційним гарантіям. Хоча Додатковий протокол є похвальною спробою, він, без сумніву, обмежений у своїй здатності об'єднувати реальні відмінності в тому, як держави регулюють розпалювання ненависті, і створювати правові межі, за допомогою яких можна протидіяти поведінки на підставі ненависті.

Дж.Бенкс вважає, що розширення співробітництва між європейськими країнами може призвести до збільшення кількості «груп ненависті», створених в США, оскільки расисти та екстремісти прагнуть уникнути судового переслідування, тому вони будуть переносити веб-ресурси в «вільний» простір, з якого і буде відбуватися поширення інформації [12]. Це призведе до того, що результатом підсиленя правового регулювання європейською спільнотою стане не уникнення такої діяльності, а її перенесення на веб-сервіси США і подальше поширення з них.

Отже, правових односторонніх і навіть багатосторонніх зусиль з регулювання мережі буде недостатньо, щоб зменшити поширення онлайн-

ненависті. Епізодичне судове переслідування окремих користувачів мережі навряд чи утримає інших від публікації подібних висловлювань. Веб-сайти, які закриті в одній юрисдикції, можуть просто знову відкритися в іншій, залишаючись доступними для користувачів Інтернету зі всього світу. Крім того, глобальна природа Інтернету унеможлиблює повне правове регулювання кіберпростору. Дж.Бенкс бачить альтернативу для розв'язання даного питання у взаємодії правових і технічних механізмів через Інтернет-провайдерів. Різні угоди про кодекси поведінки або умови надання послуг дозволяють Інтернет-провайдерам видаляти образливі веб-матеріали, які порушують їхню політику. Добровільні кодекси поведінки, з якими клієнти повинні погодитися, дозволяють інтернет-провайдерам видаляти контент, що порушує їхню політику [12].

Однак даний шлях вирішення також обмежений, тому що за законом більшості країн інтернет-провайдери не несуть відповідальність за дії та висловлювання своїх користувачів. Крім того, контроль поведінки користувачів несе додаткові фінансові витрати, через що багато інтернет-провайдерів не мають бажання або коштів для усунення шкідливого контенту. Так, соціальна мережа Facebook відмовляється "грати роль арбітра" щодо того, що вважається образливим, а, наприклад, в контексті багатьох блогів і веб-форумів політика обмеження контенту може розцінюватися як протидія здійсненню свободи слова.

Таким чином, єдиним ефективним способом співіснування права на захист честі та гідності, свободи слова і регулювання висловлювань, які розпалюють ненависть, ображають особистість або певні групи людей, є коаліція урядових зусиль і правового регулювання, технічного регулювання з боку Інтернет-провайдерів і діяльність самих користувачів, яка може полягати як в моніторингу інтернет-контенту і сповіщенні відповідних органів про протиправні випадки, так і в створенні Інтернет-культури без образ, цькування і ненависті.

4.4. Анонімність і авторське право

Принципи функціонування всього Інтернет-простору будуються навколо анонімності або псевдонімності. Через цю ілюзію безкарності, яка виникає при анонімній діяльності в Інтернеті, складається стереотип, що неможливо захистити авторське право. З одного боку, багато людей вважають інформацію соціальним продуктом, який не повинен присвоюватися виключно приватними інтересами. З іншого боку, інформація стала одним з найважливіших економічних продуктів в сучасній економіці, і тому вона повинна бути представлена принципам ринкової економіки, як і будь-який інший товар. Говорячи про порушення авторських прав в Інтернеті, маються на увазі в першу чергу різні види так званої піратської діяльності — незаконне розповсюдження фільмів, музики, програм тощо. З кожним роком зростає кількість сайтів з піратською інформацією і контентом, видалення яких майже неможливо у зв'язку з великою кількістю копій подібних сайтів і інформації на них. Основна проблема здійснення правосуддя щодо порушень авторських прав в мережі Інтернет полягає в конфлікті між авторами оригінальних творів, які захищені авторським правом, і анонімними користувачами, які захищені правом спілкуватися анонімно і свободою поширення інформації.

Багато міжнародних та національних законодавчих структур зараз сходяться на думці, що поширення матеріалів та інформації, захищених авторським правом, не може підпадати під право на анонімність, свободу поширення інформації тощо. З 2010 року почався етап, коли правовласники починають активно залучати правоохоронну і судову системи для захисту своїх прав в Інтернеті проти індивідуальних користувачів і веб-платформ. У 2011 році такі музичні корпорації як Sony Music, Universal Music посилили політику використання музичних композицій без прямої угоди правовласника, прийняли позицію з видалення музичних композицій на всіх майданчиках Інтернету і соціальних мережах, які не мали певного дозволу для публікування. У 2007 році компанія Google стала просувати систему

ContentID, яка здатна розпізнати нелегально скопійований авторський контент по файлу-відбитку, і в разі виявлення надати правовласнику право заблокувати ролик.

Міжнародна угода по боротьбі з контрафактною продукцією (АСТА) розробляє програми для контролювання порушень авторського права як в мережевому просторі шляхом зобов'язання Інтернет-провайдерів видаляти контент, що порушує дане право, і видавати ідентифікацію користувачів, які його порушали, так і стосовно цифрових пристроїв шляхом оглядів телефонів, ноутбуків, планшетів на кордонах на предмет зберігання в них файлів, пов'язаних з порушенням закону про авторське право. Організація Electronic Frontier Foundation (EFF) висловлює занепокоєння з приводу методів, за допомогою яких деякі організації або державні структури можуть викривати анонімних завантажників і вимагати від інтернет-провайдерів миттєвого видалення контенту. EFF наполягає на тому, щоб подібні рішення проводилися тільки після рішення суду. На захист авторського права через суд наполягають органи США, що демонструє Закон про авторське право в цифрову епоху (Digital Millennium Copyright Act — DMCA). Згідно з цим Законом розкрити інформацію про користувача, який порушує права правовласника, правовласник може тільки через отримання в суді судового наказу. Крім того, Закон захищає Інтернет-провайдерів, які не несуть відповідальності у всіх без винятку випадках виявлення на певній платформі матеріалів, контенту, що порушують авторське право.

У праві Європейського Союзу є кілька Директив, що регулюють ті чи інші аспекти інтелектуальної власності, загальна мета яких — встановлення загальних правил, які кожна держава має реалізувати у своєму національному праві. Основним документом в даній сфері є Директива ЄС 2001 року «Про гармонізацію окремих аспектів авторського права і суміжних прав в інформаційному суспільстві». В Директиві йдеться, що повинен бути досягнутий справедливий баланс прав та інтересів між різними категоріями правовласників і користувачами [52]. Однак у 2019 році завершився процес

прийняття нової Директиви, яка змусить Інтернет-платформи фільтрувати контент на предмет дотримання авторського права і являє собою жорстке обмеження поширення інформації в Інтернеті. Стаття 13 цієї Директиви потенційно може покласти край існуванню реміксів та іншого контенту, що створюється користувачами Інтернету на основі матеріалів, захищених авторським правом. Стаття покладає на веб-сайти відповідальність за відповідність контенту, який публікують користувачі, нормам авторського права. Для її виконання сайтам знадобляться певні системи розпізнавання контенту, тобто фільтри, через які будуть проходити всі тексти, аудіозаписи та зображення, що публікуються на ресурсі. Критики Статті 13 вважають, що подібні фільтри можуть спрацювати як цензура і змінити всю культуру використання Інтернету [11]. З цієї причини Польща вже відмовилася від виконання даної Директиви, тому що бачить в цьому порушення права на свободу слова. Петицію в інтернеті, спрямовану проти Статті 13, підписало понад 5,2 мільйона користувачів. Подібні протести є частим явищем у Франції, політика якої відрізняється найжорсткішими заходами щодо захисту авторських прав в Європі: у 2010 році був прийнятий законопроект, який передбачає захист креативного контенту в Інтернеті шляхом покарання користувачів через відключення від Інтернету. Французьке законодавство ухвалило наступну процедуру: правовласники передають провайдерам списки IP-адрес, з яких зафіксовані порушення, провайдери протягом 8 днів повинні ідентифікувати за цими адресами своїх клієнтів і вислати їм попередження; після трьох попереджень до справи залучаються судді, які в бліц-режимі відключають винних від Інтернету.

Думки критиків щодо захисту авторського права і права на анонімну передачу і поширення інформації розділилися: деякі бачать в цьому пряме порушення права на анонімність, і єдиним шляхом видалення контенту, який порушує авторське право, і шляхом розкриття особистості злочинця називають судові рішення, до моменту прийняття яких користувач повинен залишатися анонімним; інші не визнають право на анонімність в умовах

незаконного обміну файлами та не бачать вагомих причин соціальної політики чи закону для захисту анонімності тих, хто самостійно не вносить нічого цінного в ринок ідей.

4.5. Держава у протистоянні з простором анонімної мережевої комунікації та діяльності. Кіберзлочинність як стимул заборони анонімної комунікації

Витік інформації від Едварда Сноудена змусив американців і згодом весь світ звернутися до проблеми того, що уряди прагнуть контролювати діяльність і спілкування в Інтернеті, а також прагнуть мінімізувати анонімну взаємодію в мережі. Крім того, найсильнішою протидією захисту конфіденційності та анонімності в Інтернеті є злочинна діяльність. Інтернет надає злочинцям вільну платформу для організації та здійснення злочинної діяльності; все частіше в новинах можна побачити повідомлення про торгівлю наркотиками, шахрайство, розповсюдження дитячої порнографії та поширення небажаних матеріалів, що відбувається через Інтернет-простір. Наповнення Інтернет-простору подібними злочинними групами, а також різними діями антигуманної або неправової поведінки дає аргументи для повної спостережливості та простежуваності Інтернет-комунікації з боку урядових структур. Все частіше з кіберзлочинністю і хаосом на Інтернет-платформах пов'язують анонімність і псевдонімність, породжуючи недовіру до тих, хто не хоче розкривати свою «справжню» особистість в Інтернеті. Дуже часто зняття анонімності в цілях захисту проти кіберзлочинності служить приводом для більш широкого моніторингу Інтернет-ресурсів. Основні переваги деанонімізації в Інтернеті для державних структур полягають в більш ефективному відстеженні фінансових операцій, в більш ефективному попередженні або покаранні хакерів, в контролі організацій, які здійснюють спостереження за діяльністю урядів, в регулюванні організації протестів і відстеженні опозиційних громадян і груп тощо.

Ральф Емерсон якось зазначив, що "лампа — найкраща нічна поліція», і цю ідею намагаються перенести на Інтернет-простір шляхом зниження рівня анонімності та можливостей шифрування, підвищення зобов'язань Інтернет-провайдерів у відповідному національному органі правопорядку, встановлення різних методів відстеження цифрових пристроїв і користувачів. За останні роки політики, співробітники правоохоронних органів і групи з особливими інтересами все частіше звертаються до уряду різних країн і міжнародних структур з клопотанням щодо моніторингу активності в Інтернеті, пропонуючи, щоб урядові органи забезпечували такий же рівень контролю в Інтернеті, як у сферах радіо і телебачення.

На міжнародному рівні кроком в напрямку загальної спостережливості стала Європейська конвенція про кіберзлочинність, яку я розглядала вище, в рамках якої громадська безпека і приватна анонімність суперечать один одному. Можливість відстеження злочинної діяльності потребує засобів спостереження та ідентифікації, і останнім часом реакція уряду на міжнародний тероризм і глобальні випадки кіберзлочинності знову показала, що «анонімність — це перше, що кидається за борт в разі небезпеки». Багато міжнародних та національних організацій приходять до висновку, що індивідуальні права на недоторканність приватного життя, анонімність, можливо, доведеться послабити, прагнучи скоротити кіберзлочинність та використання Інтернету для злочинної діяльності. Все частіше урядовими структурами озвучуються пропозиції мережевих ідентифікаторів, які могли б функціонувати як «водійські права» для підвищення довіри серед користувачів і можливості постійного відстеження для держави.

Верховний суд США неодноразово виносив постанову про те, що право на анонімну свободу слова захищено Першою поправкою: анонімність розглядалася як життєво важливий елемент демократичного дискурсу, вона є інструментом захисту думок меншості осіб від «руки нетерпимого суспільства». Закони США встановлюють право говорити анонімно в Інтернеті, а також право читати анонімно в Інтернеті, людям дозволяється

взаємодіяти один з одним псевдонімно та анонімно, якщо ці дії не порушують закон. Однак сучасні реалії показують, що в США анонімність все частіше піддається критиці як інструмент, який сприяє незаконній та аморальній діяльності більшою мірою, ніж служить інструментом забезпечення прав і свобод. Вже з 2014 року США відносять до країн-ворогів Інтернету згідно з міжнародною неурядовою організацією Reporters sans frontières («Репортери без кордонів»), яка виступає за свободу преси, свободу висловлювань та обговорень. Основними противниками вільного Інтернету є Бахрейн, Китай, Іран, Сирія і В'єтнам. До цього списку належать не тільки авторитарні й тоталітарні країни, але і Великобританія, Росія, Білорусь, які формально закріплюють демократичні цінності та свободи як основні [59]. Росія і Китай наклали вимоги реєстрації реальних юридичних імен для користувачів соціальних мереж або блогерів, обмеживши тим самим анонімність. У Китаї уряд вже заблокував віртуальні приватні мережі (VPN), які дозволяли його громадянам обходити національні міжмережеві екрани та залишатися анонімними. У 2017 році Росія також заборонила VPN, TOR — систему проксі-серверів, що дозволяє встановлювати анонімне з'єднання з мережею, і анонімне користування месенджерів.

Прем'єр-міністр Великобританії Д.Кемерон закликав до придушення анонімізації та шифрування. У 2018 році міністр з цифрових питань Марго Джеймс пообіцяла, що нове законодавство, яке вимагає, щоб люди реєстрували свою юридичну особистість при використанні Інтернету, було внесено «при першій же можливості» [33]. Урядовці в США і Великобританії висловили стурбованість тим, що більш широке використання шифрування в соціальних мережах або на мобільних пристроях утруднить запобігання тероризму. Ці чиновники звинуватили Інтернет-провайдерів та Інтернет-компанії в створенні «зон беззаконня» і «темних місць», де терористи та злочинці можуть вільно взаємодіяти.

Ситуацію в Україні звіти Freedom on the Net від Freedom House схарактеризували як «вільну» на 2012 і 2013 рік, і як «частково вільну» з

2014 по 2017 роки: в Україні відсутні практики інституціоналізованого блокування або фільтрації або нормативної бази для цензури контенту в Інтернеті. Однак кризові моменти внутрішньої та зовнішньої політики повпливали на свободу поширення інформації та висловлювань в пресі та Інтернет-просторі. В травні 2017 року Порошенко підписав указ, що вимагає від провайдерів блокувати доступ до ряду російських сайтів, включаючи чотири найпопулярніші сайти в Україні: «ВКонтакте», «Однокласники», «Яндекс» і «Mail.Ru». Дані дії піддалися критиці з боку організації «Репортери без кордонів», яка позначила їх як дії, що спрямовані на підривання прав українського народу на інформацію та свободу вираження. Онлайн-опитування на сайті УНІАН показало, що 66% опитаних були «категорично проти» заборони російських сайтів, а ще 11% заявили, що буде простіше «заборонити весь інтернет, як у Північній Кореї» [37]. Однак в 2020 році Кіберполіція виявила бажання деанонізувати українців у мережі: департамент Кіберполіції надіслав редакції інтернет-видання “Полтавщина” листа з пропозицією розмістити на сайті медіа програмний скрипт, який дозволить ідентифікувати користувачів, що намагаються себе анонімізувати [53]. Коаліція “За вільний Інтернет” розкритикувала спробу поліцейських деанонізувати користувачів мережі, зауваживши, що така пропозиція потенційно загрожує порушенням права на приватність та анонімність користувачів, а також права на свободу вираження поглядів [53]. Даний приклад ілюструє ситуацію, при якій Україна також може втратити статус вільних країн для Інтернет-взаємодії.

Як показують вищенаведені приклади, а також політика і практика інших країн, закон про анонімність в Інтернеті значною мірою не дотримується у всьому світі. Серед країн, які мають давню історію поваги прав на свободу вираження думок і недоторканність приватного життя, існує певний консенсус щодо обмеженого права на анонімне спілкування. Існує також певна згода з тим, що Інтернет-провайдери не несуть юридичної

відповідальності за дії своїх користувачів. У деяких випадках від Інтернет-провайдерів може знадобитися ідентифікувати своїх користувачів [29].

Більшість експертів з питань свободи та анонімності в Інтернеті, а також дослідники правового поля забезпечення анонімної взаємодії сходяться на думці, що, як правило, справжня, повна анонімність в мережевому просторі недоступна. Оскільки кожен комп'ютерний портал в Інтернеті має унікальну IP-адресу, яка реєструється кожен раз, коли користувач відвідує веб-сайт, анонімність майже завжди простежується, а сучасні технології відстеження і дешифрування, якими володіють правоохоронні структури всіх країн, роблять неефективними навіть особливі методи анонімізації. На цей момент у сфері правового регулювання Інтернет надає певний рівень "анонімності, що простежується», що означає, що, в той час як вигадані імена користувачів створюють ілюзію анонімності для більшості відвідувачів і користувачів веб-платформ, номер Інтернет-протоколу кожного комп'ютера записується і відстежується правоохоронними та іншими державними структурами за необхідністю [49].

Підхід до правового регулювання мережевого простору залежить від внутрішньої та зовнішньої політики, що проводиться на національному та міжнародному рівні. Однак сучасна тенденція демонструє, що багато держав з демократичною політикою і міжнародним співробітництвом також прагнуть обмежити широку доступність анонімної взаємодії та шифрування в мережі Інтернет та в соціальних мережах. Основне питання, яке постає в контексті правового регулювання анонімності, полягає в пошуку балансу між беззаперечним виконанням прав на недоторканність приватного життя, свободу висловлювань та поширення інформації та повним усуненням анонімності, введенням методів ідентифікації, криміналізацією технологій анонімізації. Що являє собою баланс між правоохоронними та державними органами, особистою недоторканністю і правами людини? Я вважаю, що питання здійснення права на анонімність виходить з внутрішньої політики країни, адже справедлива судова система, чітко прописані права та обов'язки

користувачів, Інтернет-провайдерів і державних структур, а також їх чітке виконання зі сторони усіх агентів може зберегти баланс між категоричними сторонами проблеми. Існування і поширення анонімності має здійснюватися в межах діяльності, що не є загрозовою для свобод інших людей, громадського порядку. Однак це не означає, що уряди володіють повним правом відстежувати, перехоплювати або читати повідомлення, а також отримувати за бажанням інформацію про користувачів. Дані дії повинні здійснюватися в межах справедливого закону і через звернення до незалежних судів.

Необхідною умовою контролю з боку урядових структур є рішення судів, які могли б встановити джерело повідомлення, ідентифікувати особистість, її місцеперебування тільки за умови, якщо вона стає предметом правового спору. Користувачі змогли б приховувати свою юридичну реальну ідентифікацію при комунікації в Інтернет-просторі та в соціальних мережах, поширенні інформації та висловлюванні думок, але при цьому вони б точно усвідомлювали, в яких випадках вони будуть притягнуті до відповідальності згідно із законом.

Висновки

Сучасне суспільство неможливо уявити без нового соціального простору — Інтернет-простору та простору соціальних мереж, всередині яких склався новий тип віртуальної комунікації та віртуальної взаємодії, основним елементом котрих є анонімність. У результаті проведеного дослідження було виявлено, що в ХХ ст. інформаційне суспільство, технологічні інновації та цифрові комунікаційні технології дійсно мали характер глибокого проникнення в життя людей, що спричинило становлення нової соціальної організації, трансформацію всіх сфер діяльності людини, появу нових платформ, просторів комунікації та взаємодії, а також нових мережевих структур. На цій підставі було виявлено, що в кінці ХХ ст. мережеві структури стають умовою розвитку нового типу суспільства — мережевого суспільства, котре можна визначити як глобальне суспільство, яке побудоване навколо персональних та організаційних мереж, котрі засновані на цифрових мережах та мережі Інтернет.

На підставі розгляду еволюції мережевого суспільства було виявлено становлення нового типу комунікації, яке було спричинено, по-перше, універсалізацією мережевої структури взаємодії на індивідуальному, груповому, міжнародному рівнях, по-друге, глобальним використанням персональних електронних засобів з доступом до мережі та розповсюдженням систем масової самокомунікації — соціальних мереж, блогів, форумів тощо, та, по-третє, вільною та глобальною конкуренцією культурних кодів.

Розглянувши основні характеристики нового типу комунікації в умовах мережевого суспільства, можна зробити припущення, що саме вільний обмін інформацією, можливості розвитку самих різних цінностей та інтересів, відношення рівності та відсутність цензурування спричинили затвердження нового мережевого простору як простору вільної комунікації. Основним механізмом забезпечення цієї свободи стала анонімність, яка дозволяла

людям вільно висловлювати свою думку, не побоюючись відплати або засудження, в абсолютно різних контекстах та спільнотах.

На підставі проведеного дослідження був визначений поняттєвий апарат анонімної комунікації та анонімної взаємодії у віртуальному мережевому просторі, який складається з таких понять як «мережева особистість», «анонімність», «псевдонімність», «конфіденційність», «рівень анонімності». Крім того, в ході дослідження було з'ясовано, що головні термінологічні проблеми пов'язані з неможливістю точного розмежування рівнів функціонування анонімної комунікації, типів анонімності. За для цього було розглянуте поняття «континуум анонімності», яке дозволяє розглядати анонімність та псевдонімність в Інтернет-просторі не як чітко розділені елементи, а як безліч можливостей представити реальну або сконструйовану віртуальну ідентичність, як безлічі відтінків ідентифікації, можливих в Інтернет-просторі.

Під час написання дипломної роботи було з'ясовано, що анонімність впливає на усвідомлення себе, інших, простору, саме тому гостро постало питання зміни поведінки в умовах анонімної комунікації та анонімної взаємодії у віртуальному мережевому просторі. Було виявлено декілька причин такої зміни в умовах анонімності, основними з котрих є зниження рівню психологічного та соціального ризику через позбавлення значення цілого ряду бар'єрів спілкування; можливості конструювання ідентичності за власним бажанням, незалежно від соціальних ролей в реальному світі; можливості виходу з жорстких меж бажаної соціальної поведінки та від впливу соціальних норм; відсутність в більшості випадків правової або неправової відповідальності. Ці причини зумовили розповсюдження ефекту мережевої дезінбації — який описує зниження психологічних обмежень, відсутність регулювання поведінки, що призводить до того, що в онлайн-соціальному середовищі люди поведуться так, як вони зазвичай не поводитися в реальному житті, висловлюють себе більш відкрито — та віртуальну деіндивідуалізацію — в результаті якої зніжується рівень

саморефлексії та самоконтролю та підвищується потенціал до злиття з масовою свідомістю простору комунікації.

Анонімність, анонімна комунікація та зміна поведінки через анонімність може призводити, як було проаналізовано в ході дослідження, до позитивних наслідків — стимулювання свободи вираження та вільного спілкування, генерування істинних ідей, які не створюються під тиском влади, авторитету, зменшення рівня дискримінації та стигматизації через відсутність етнічних, статевих, вікових атрибутів, створення умови «ідеальної мовної ситуації», та до негативних наслідків, основним елементом котрих є кіберагресія та її різновиди — тролінг, кібербулінг, кіберсталкінг.

Велика частина роботи була присвячена аналізу взаємин між анонімною комунікацією, анонімною взаємодією та основними правами людини та громадянина. Порівняльний аналіз анонімності з декількома основними правами людини показав, що в залежності від самого права сильно змінюється ставлення до анонімної комунікації та анонімної взаємодії з боку користувачів, правових організацій та державних структур. В ході дослідження був здійснений аналіз відносин між анонімністю і свободою слова, правом на недоторканність приватного життя, який показав, що анонімність в віртуальному просторі є важливим елементом реалізації цих прав як у віртуальному мережевому просторі, так і в реальному соціальному просторі. Анонімність має основоположне значення для здійснення права на свободу слова, для захисту соціальних груп ризику і відстоювання прав в недемократичних режимах. Анонімність також служить важливим інструментом для забезпечення права на недоторканність приватного життя. Однак щодо авторського права і права на захист честі, гідності та ділової репутації анонімність має протилежний ефект, служить інструментом ухилення від відповідальності при порушенні даних прав. Крім того, дослідження питання правового регулювання за порушення даних прав показало, що існує кілька проблем залучення до відповідальності саме через

анонімність і фізичну неподставленість користувача, а також відсутність єдиної територіальної юрисдикції правового регулювання.

В ході дослідження було визначено, що основною проблемою правового регулювання анонімної діяльності є проблема обмеження права на саму анонімність в прагненні реалізації інших прав. Порівняльний аналіз національної та міжнародної політики та аналітичний метод дозволили виявити тенденцію скорочення можливостей анонімної комунікації, яке відбувається унаслідок практично повсюдного обмеження інструментарію анонімізації, більшого контролю з боку державних правоохоронних і судових органів і їх більш частого втручання у сферу анонімного спілкування. В ході роботи були описані механізми для збору інформації про користувачів, механізми деанонімізації користувачів з боку урядових структур, механізми дешифрування шляхом впровадження обов'язків деанонімізації користувачів для Інтернет-провайдерів. Дослідження також показало тенденцію до введення законів та правових ініціатив щодо обмеження анонімної комунікації та введення мережевих ідентифікаторів, а в деяких країнах щодо часткового або повного регулювання Інтернет-простору з боку держави.

Визначивши основні проблеми та тенденції державного і правового регулювання проблеми анонімної комунікації та анонімної взаємодії в Інтернет-просторі, я зробила наступні припущення: регулювання негативних і неправових дій у віртуальному мережевому просторі можливо тільки шляхом розробки міжнародної правової бази, яка могла б охоплювати такий нетериторіальний і глобальний простір як Інтернет; формування правової бази з питань забезпечення анонімності має зосередитися на питаннях співвідношення дій в віртуальному і реальному просторі, що передбачає збалансування правових норм цих просторів, регулювання застосування заходів санкцій та притягнення до правової відповідальності щодо дій, здійснених в мережевому просторі; необхідно здійснити пошук балансу між беззаперечним виконанням прав на недоторканність приватного життя, свободу висловлювань та поширення інформації та повним усуненням

анонімності, введенням методів ідентифікації, криміналізацією технологій анонімізації.

Дослідження показало, що практика анонімної комунікації та анонімної взаємодії в Інтернет-просторі та соціальних мережах є багатоплановим і багатопроблемним явищем, вона не існує тільки в негативних проявах. Анонімність в Інтернет-просторі дозволяє людям контролювати те, що вони розкривають про себе і кому вони це розкривають, відкриває можливості для дослідження ідентичності, рівного спілкування без упереджень і дискримінації. Негативні наслідки, кіберагресія, кіберзлочинність і питання їх правового регулювання повинні більш детально розглядатися в міждисциплінарному дослідженні анонімності. Сумарна програма відповідальності самих користувачів, чітко прописаних прав, обов'язків і можливостей всіх суб'єктів правових відносин в Інтернет-просторі, діяльності незалежних судів, які зможуть деанонімізувати користувачів тільки в разі судового розгляду, може зберегти демократичні тенденції в Інтернет-просторі та мати вирішальне значення для подальшої стабільності вільного і справедливого як офлайн, так і онлайн суспільства.

Список використаних джерел

1. Бодрийяр Ж. Символический обмен и смерть / Жан Бодрийяр. – Москва: Добросвет, 2000. – 387 с.
2. Ди Ч. Социальные сети и их влияние на события в арабских государствах (2010– 2013 гг.) / Чэнь Ди. // Вестник Санкт-Петербургского университета. – 2013. – №4. – С. 189 – 194.
3. Жичкина А. Е. Социально-психологические аспекты общения в Интернете [Электронный ресурс] / А. Е. Жичкина // CYBERPSY Online Press. – 2017. – Режим доступа до ресурсу: <http://cyberpsy.ru/articles/zhichkina-online-obshhenie/>.
4. Кастельс М. Галактика Интернет: Размышления об Интернете, бизнесе и обществе / Мануэль Кастельс. – Екатеринбург: У-Фактория, 2004. – 328 с.
5. Кастельс М. Информационная эпоха: экономика, общество и культура / Мануэль Кастельс. – Москва: Национальный исследовательский университет "Высшая школа экономики", 2000. – 608 с
6. Королева Н. Н. Влияние коммуникации в сети Интернет на личностные особенности пользователей / Н. Н. Королева. // Известия Российского государственного педагогического университета им. А.И. Герцена. – 2004. – №9. – С. 168–179.
7. Курочкин А. В. Концепция сетевого общества в системе социального знания / А. В. Курочкин, Г. К. Антонов. // Общество: социология, психология, педагогика. – 2016. – №12. – С. 14–17.
8. Серкина Н. Е. Понятие сетевого общества М.Кастельса / Надежда Евгеньевна Серкина. // Вестник Майкопского государственного технологического университета. – 2019. – №2. – С. 161–169.
9. Уэбстер Ф. Теории информационного общества / Фрэнк Уэбстер. – Москва: АСПЕКТ ПРЕСС, 2004. – 222 с.

10. Фетисова Т. А. Агрессивное поведение в Интернет-коммуникации / Т. А. Фетисова. // Журнал «Вестник культурологии». – 2018. – №4. – С. 185–197.
11. Шмырова В. Евросоюз принял закон об авторском праве [Электронный ресурс] / Валерия Шмырова // CNews. – 2019. – Режим доступа до ресурсу: https://www.cnews.ru/news/top/2019-04-16_evrosoyuz_bezvozvratno_prinyal_zakon_ob_avtorskom.
12. Banks J. Regulating hate speech online / James Banks. // International Review of Law, Computers and Technology. – 2010. – №24. – С. 233–239.
13. Bareket-Bojmel L. Emotional and Interpersonal Consequences of Self-Disclosure in a Lived, Online Interaction / L. Bareket-Bojmel, G. Shahar. // Journal of Social and Clinical Psychology. – 2011. – №30. – С. 732–759.
14. Barlett C. Predicting Cyberbullying From Anonymity / C. Barlett, D. Gentile. // Psychology of Popular Media Culture. – 2016. – №5. – С. 171–180.
15. Barlow J. A Declaration of the Independence of Cyberspace [Электронный ресурс] / John Perry Barlow // Electronic Frontier Foundation. – 1996. – Режим доступа до ресурсу: <https://www.eff.org/cyberspace-independence>.
16. Beyer J. What does anonymity mean? Reddit, activism, and “Creepshots” [Электронный ресурс] / Jessica Beyer // Jessica L. Beyer Blog. – 2012. – Режим доступа до ресурсу: <https://www.jlbeyer.com/what-does-online-anonymity-mean-reddit-activism-and-creepshots/>.
17. Bishop J. The effect of de-individuation of the Internet Troller on Criminal Procedure implementation: An interview with a Hater / Jonathan Bishop. // International Journal of Cyber Criminology. – 2013. – №7. – С. 28–48.
18. Borgmann A. Technology and the Character of Contemporary Life: A Philosophical Inquiry / Albert Borgmann. – Chicago: The University of Chicago Press, 1987. – 310 с.
19. Castells M. The Rise of the Network Society. Information Age / Manuel Castells. – Hoboken: Blackwell Pub, 1996. – 556 с.

20. Christopherson K. The positive and negative implications of anonymity in Internet social interactions: “On the Internet, Nobody Knows You’re a Dog ”/ Kimberly Christopherson. // *Computers in Human Behavior*. – 2007. – №23. – С. 3038–3056.
21. Compton L. Teacher, parent and student perceptions of the motives of cyberbullies / L. Compton, M. Campbell, A. Mergler. // *Social Psychology of Education*. – 2014. – №17. – С. 383–400.
22. Dent S. Most websites don't follow European cookie consent laws, study shows [Электронный ресурс] / Steve Dent // *Engadget OnlinePress*. – 2020. – Режим доступа до ресурсу: <https://www.engadget.com/2020-01-13-websites-not-following-eu-gdpr-rules-study.html>.
23. Dijk J. *The Network Society: Aspects of the New Media* / Jan van Dijk. – Thousand Oaks: SAGE Publications Ltd, 2005. – 304 с.
24. Dreyfus H. *On the Internet (Thinking in Action)* / Hubert Dreyfus. – London: Routledge, 2008. – 192 с.
25. Duggan M. *Online Harassment* [Электронный ресурс] / Maeve Duggan // *Pew Research Center Press*. – 2014. – Режим доступа до ресурсу: <https://www.pewresearch.org/internet/2014/10/22/online-harassment/>.
26. Ellison N. *Social Network Sites: Definition, History, and Scholarship* / Nicole Ellison. // *Journal of Computer-Mediated Communication*. – 2007. – №13. – С. 210–230.
27. Froomkin M. *Anonymity and its Enmities* / Michael Froomkin. // *Journal of Online Law*. – 1995. – №4. – С. 15.
28. Goddyn B. *Defining Anonymity and its Dimensions in the Electronic World* / Bart Goddyn. // *Interdisciplinary Centre for Law and Information Technology*. – 2001. – С. 35.
29. Heatherly K. *Anonymous Online Comments: The Law and Best Media Practices from Around the World* [Электронный ресурс] / К. Heatherly, А. Fargo, J. Martin // *International Press Institute*. – 2014. – Режим доступа до

- ресурсы: https://ipi.media/wp-content/uploads/2016/12/IPI_AnonymousSpeech_Oct2014.pdf.
30. Hilbert M. The World's Technological Capacity to Store, Communicate, and Compute Information / M. Hilbert, P. Lopez. // *Science*. – 2011. – №332. – С. 60–65.
 31. Hollenbaugh E. The Effects of Anonymity on Self-Disclosure in Blogs: An Application of the Online Disinhibition Effect / Erin Hollenbaugh. // *Journal of Computer-Mediated Communication*. – 2013. – №18. – С. 283–302.
 32. Kaye D. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression [Электронный ресурс] / David Kaye // UN Human Rights Council Press. – 2015. – Режим доступа до ресурсы: <https://www.refworld.org/docid/5576dcfc4.html>.
 33. Kosseff J. Do we have a right to online anonymity? [Электронный ресурс] / Jeff Kosseff // Reporters Without Borders Press – Режим доступа до ресурсы: <https://www.rcfp.org/journals/news-media-and-law-winter-2014/do-we-have-right-online-ano/>.
 34. La Rue F. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression [Электронный ресурс] / Frank La Rue // UN Human Rights Council Press. – 2013. – Режим доступа до ресурсы: https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.
 35. Levin S. As Facebook blocks the names of trans users and drag queens, this burlesque performer is fighting back [Электронный ресурс] / Sam Levin // *The Guardian Press*. – 2017. – Режим доступа до ресурсы: <https://www.theguardian.com/world/2017/jun/29/facebook-real-name-trans-drag-queen-dottie-lux>.
 36. Lloyd I. Privacy, Anonymity and the Internet / Ian Lloyd. // *Electronic Journal of Comparative Law*. – 2009. – №13. – С. 16.

37. Luhn A. Ukraine blocks popular social networks as part of sanctions on Russia [Электронный ресурс] / Alec Luhn // The Guardian Press. – 2017. – Режим доступа до ресурсу: <https://www.theguardian.com/world/2017/may/16/ukraine-blocks-popular-russian-websites-kremlin-role-war>.
38. Martino F. Social Network Analysis: A brief theoretical review and further perspectives in the study of Information Technology / F. Martino, A. Spoto. // PsychNology Journal. – 2006. – №4. – С. 53–86.
39. Marx G. What's in a Name? Some Reflections on the Sociology of Anonymity / Gary Marx. // An International Journal. – 1999. – №15. – С. 99–112.
40. McKenna K. Coming out in the age of the Internet: Identity "demarginalization" through virtual group participation / K. McKenna, J. Bargh. // Journal of Personality and Social Psychology. – 1998. – №75. – С. 681–694.
41. Nagel E. Anonymity, pseudonymity, and the agency of online identity: Examining the social practices of r/Gonewild [Электронный ресурс] / E. Nagel, J. Frith // First Monday: peer reviewed journal on the Internet. – 2015. – Режим доступа до ресурсу: <https://firstmonday.org/ojs/index.php/fm/article/view/5615>.
42. Paskuda M. The Influence of Anonymity on Participation in Online Communities : дис. докт. соц. наук / Paskuda Malte – Université de Technologie de Troyes, 2016. – 118 с.
43. Quittner J. An Interview with Johan Helsingius: Anonymously Yours [Электронный ресурс] / Joshua Quittner // Wired OnlinePress. – 1994. – Режим доступа до ресурсу: <https://www.wired.com/1994/06/anonymous-1/>.
44. Rainie L. Anonymity, Privacy, and Security Online [Электронный ресурс] / L. Rainie, S. Kiesler // Pew Research Center Press. – 2013. – Режим доступа до ресурсу: <https://www.pewresearch.org/internet/2013/09/05/anonymity-privacy-and-security-online/>.

45. Rheingold H. The Virtual Community: Homesteading on the Electronic Frontier / Howard Rheingold. – Massachusetts: Addison-Wesley, 1993. – 447 с.
46. Scott C. Anonymity and Self-Disclosure on Weblogs / C. Scott, H. Qian. // Journal of Computer-Mediated Communication. – 2007. – №12. – С. 1428–1451.
47. Shao G. Social media has become a battleground in Hong Kong's protests [Електронний ресурс] / Grace Shao // CNBCNews. – 2019. – Режим доступу до ресурсу: <https://www.cnbc.com/2019/08/16/social-media-has-become-a-battleground-in-hong-kongs-protests.html>.
48. Silver L. Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally [Електронний ресурс] / Laura Silver // Pew Research Center Press. – 2019. – Режим доступу до ресурсу: <https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/>.
49. Solove D. I've Got Nothing to Hide and Other Misunderstandings of Privacy / Daniel Solove. // San Diego Law Review. – 2007. – №44. – С. 28.
50. Suler J. The Online Disinhibition Effect / John Suler. // CyberPsychology & Behavior. – 2004. – №7. – С. 321–326
51. Townsend L. Social Media Research: A Guide to Ethics [Електронний ресурс] / L. Townsend, C. Wallace // The University of Aberdeen. – 2016. – Режим доступу до ресурсу: https://www.gla.ac.uk/media/Media_487729_smxx.pdf.
52. Директива Європейського Парламенту і Ради «Про гармонізацію окремих аспектів авторського права і суміжних прав в інформаційному суспільстві» [Електронний ресурс] // Європейський Парламенту, Європейська Рада. – 2001. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/984_005-01.
53. Кіберполіція хоче деанонімізувати українців у мережі [Електронний ресурс] // ZMINA OnlinePress. – 2020. – Режим доступу до ресурсу:

- <https://zmina.info/news/kiberpolicziya-hoche-deanonimizuvaty-ukrayincziv-u-merezhi-programu-vzhe-zaproponuvaly-poltavskomu-vydannyyu/>.
54. Рекомендація Комітету міністрів Ради Європи «Посібник з прав людини для Інтернет-користувачів та Пояснювальний меморандум» [Електронний ресурс] // Рада Європи. – 2014. – Режим доступу до ресурсу: <https://rm.coe.int/16802e3e96>.
 55. European Convention on Human Rights [Електронний ресурс] // European Court of Human Rights. – 1950. – Режим доступу до ресурсу: https://www.echr.coe.int/Documents/Convention_ENG.pdf.
 56. Freedom on the Net: An annual study of internet freedom around the world [Електронний ресурс] // Freedom House Press – Режим доступу до ресурсу: <https://freedomhouse.org/report/freedom-net/2016/silencing-messenger-communication-apps-under-pressure>.
 57. Internet usage growth statistics [Електронний ресурс] // Internet World Stats – Режим доступу до ресурсу: <https://www.internetworldstats.com/emarketing.htm>.
 58. Silencing the Messenger: Communication Apps Under Pressure [Електронний ресурс] / S.Kelly, M. Truong, A. Shahbaz, M. Earp // Freedom on the Net Press. – 2016. – Режим доступу до ресурсу: <https://freedomhouse.org/report/freedom-net/2016/silencing-messenger-communication-apps-under-pressure>.
 59. The Enemies of the Internet [Електронний ресурс] // Reporters Without Borders Press. – 2014. – Режим доступу до ресурсу: <https://rsf.org/sites/default/files/2014-rsf-rapport-enemies-of-the-internet.pdf>.
 60. The latest social media trends to know for 2020 [Електронний ресурс] // Global Web Index Report. – 2020. – Режим доступу до ресурсу: <https://www.globalwebindex.com/reports/social>.
 61. UNESCO Series on Internet Freedom [Електронний ресурс] // UNESCO. – 2009. – Режим доступу до ресурсу: <https://en.unesco.org/unesco-series-on-internet-freedom>.