

347.1/7:(007:004.7)
А 437

Національний університет
«Одеська юридична академія»
Факультет цивільної та господарської юстиції
Кафедра цивільного права

Серія
ЦИВІЛІСТИКА ТА «ІТ-ПРАВО»

АКТУАЛЬНІ ПРОБЛЕМИ ЦИВІЛІСТИКИ У ЦИФРОВУ ДОБУ: ОНЛАЙНОВІ СОЦІАЛЬНІ МЕРЕЖІ

Монографія



Одеса
«Юридична література»
2018

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

НАУКОВА БІБЛІОТЕКА

Інв. №

185734

Серія заснована 2018 року

У монографії досліджуються актуальні проблеми, що виникають у зв'язку з інтенсивним розвитком інформаційних технологій, IT-права, призначеного забезпечити регулювання відносин в IT-сфері, та соціальних мереж. Аналізуються особливості правового регулювання соціальних мереж, зокрема концептуальні питання правового регулювання відносин у онлайн-ових соціальних мережах, правочинів, акаунтів, реклами, захисту персональних даних, блокування, фільтрації та видалення контенту в соціальних мережах, цивільної та кримінальної відповідальності при користуванні соціальними мережами.

Монографія розрахована на наукових та науково-педагогічних працівників вищих навчальних закладів і наукових установ, студентів юридичного напрямку, практичних працівників судових, правоохоронних, правозастосовних органів, а також усіх, хто цікавиться проблемами IT-права та соціальними мережами.

Автори:

Є. О. Харитонов — розд. 1; розд. 3 (у спіавт. з О. І. Харитоновою); **О. І. Харитонova** — розд. 2; розд. 3 (у спіавт. з Є. О. Харитоновим); **О. О. Кулініч** — розд. 8; **О. М. Берназ-Лукавeцька** — розд. 9; **І. В. Давидова** — розд. 5; **Д. О. Колодін** — розд. 13 (у спіавт. з Б. В. Фасієм); **К. Г. Нeкiт** — розд. 6; **Р. І. Радeйкo** — розд. 11; **О. І. Сафончик** — розд. 12; **Б. В. Фасій** — розд. 7; розд. 13 (у спіавт. з Д. О. Колодіним); **С. І. Цуркану** — розд. 10; **Ю. О. Толмачевська** — розд. 4.

За редакцією

доктора юридичних наук, професора **Є. О. Харитонova**,
доктора юридичних наук, професора **О. І. Харитонovoi**

Укладач

кандидат юридичних наук, доцент **Б. В. Фасій**

Рецензенти:

О. С. Яворська, доктор юридичних наук, професор, завідувач кафедри інтелектуальної власності, інформаційного та корпоративного права Львівського національного університету ім. Івана Франка;

О. С. Кізова, доктор юридичних наук, професор, завідувач кафедри цивільного і господарського права та процесу Міжнародного гуманітарного університету

Рекомендовано до друку вченою радою

Національного університету «Одеська юридична академія»

(протокол № 2 від 28 вересня 2018 р.)

СОЦІАЛЬНІ МЕРЕЖІ У СИСТЕМІ ПРАВОВИХ ЗВ'ЯЗКІВ

Книга, що пропонується увазі читачів, є другою у циклі монографічних досліджень проблем цивілістики у цифрову добу.

Якщо перша книга циклу була спробою створити загальну мапу Викликів інформаційного суспільства традиційним цивілістичним поняттям, то ця монографія присвячена розгляду проблем цивільного права, які виникають у онлайн-ових соціальних мережах.

Перед тим як надати читачу можливість ознайомитись з власними результатами нашої наукової розвідки, очевидно, необхідно мотивувати вибір предмета дослідження і зробити кілька застережень стосовно вживання суттєво важливих термінів (позначень).

Отже, по-перше, чому предметом дослідження обрано саме соціальні мережі?

Соціальна мережа розуміється як соціальна структура, утворена індивідами або організаціями, котра відображає різні взаємодії та зв'язки між окремими людьми або групами людей, які встановлюються в процесі їхньої спільної практичної та духовної діяльності¹. Ця категорія є узагальнюючою і охоплює соціальні спільноти різного рівня, масштабу, з різним типом взаємозв'язків між їх учасниками.

Попри те, що наразі теорія соціальних мереж у цілому є активно досліджуваною галуззю науки, цивілістичні аспекти її залишаються дослідженими недостатньо.

Цим і зумовлена доцільність з'ясування місця соціальних мереж у системі категорій та соціальних, у тому числі правових, зв'язків.

По-друге, чому предметом дослідження, як уточнюється у назві монографії, є не «соціальні мережі» взагалі, а саме «онлайн-ові соціальні мережі»?

«Онлайн-ові соціальні мережі» є частиною Інтернет-простору. Фактично йдеться про інтернет-програми, які допомагають друзям, бізнес-партнерам або іншим особам спілкуватись та встановлювати зв'язки між собою, використовуючи набір інструментів.

¹ Соціальна мережа. URL: https://uk.wikipedia.org/wiki/Соціальна_мережа.

Пошук терміна «онлайніві соціальні мережі» приводить до поняття «служба соціальних мереж» (що дозволяє припустити їхню тотожність), котрим позначається веб-сайт або інша служба у Веб, яка дозволяє користувачам створювати публічну або напівпублічну анкету, складати список користувачів, з якими вони мають зв'язок, та переглядати власний список зв'язків і списки інших користувачів. Природа та номенклатура зв'язків може різнитись залежно від системи.

На відміну від служб соціальних мереж в Інтернет-спільнотах користувач не знаходиться в центрі системи; ставлення користувача до інших учасників спільноти знаходиться на другому плані. Основна увага Інтернет-спільноти зосереджена на внеску користувача в досягнення спільних цілей, цінностей та спілкуванні. У соціальних мережах користувач знаходиться в центрі системи та може належати до кількох груп водночас¹.

При цьому у розумінні сутності поняття «онлайніві соціальні мережі» існують певні розбіжності. Так, у одній і тій самій статті може йтися про «роботу із соціальними мережами», «форму соціальних мереж, яка широко використовується у віртуальних спільнотах», про «сайти з можливостями організації соціальних мереж», «створення соціальної мережі», про «веб-сайт з можливостями роботи із соціальними мережами», про те, що «соціальні мережі почали розглядатись як складова інтернет-стратегії», «соціальні мережі в Інтернеті все більше зосереджуються на певних галузях», «більшість із соціальних мереж в Інтернеті є публічними, дозволяючи будь-кому приєднатись», «приватні служби соціальних мереж»².

Досить химерним виглядає визначення місця соціальних мереж у сучасному світі. Так, Мануель Кастельс запропонував термін «Мережемве суспільство (Network society)» для позначення суспільства, яке ґрунтується на горизонтальних соціальних зв'язках і головну роль в якому відіграють не ієрархічні моделі, а соціальні мережі. Значну роль у формуванні такого суспільства відіграють сучасні комунікації, особливо мережевого типу на зразок Інтернету³. З одного боку, тут ніби йдеться про «соціальні мережі» взагалі, але, з іншого, — Інтернет характеризується як «сучасна комунікація мережевого типу», і це наводить на думку, що маються на увазі, передусім, онлайніві соціальні мережі.

Разом із тим мають місце договори про продаж онлайніві соціальної мережі або окремого її сегмента, зміну власника мережі

¹ Соціальна мережа. URL: https://uk.wikipedia.org/wiki/Соціальна_мережа.

² Там само.

³ Мережеве суспільство. URL: https://uk.wikipedia.org/wiki/Мережеве_суспільство.

тощо, тобто, по суті, вона розглядається як об'єкт цивільних правовідносин.

Зазначені розбіжності роблять необхідним дослідження сутності соціальних мереж, аналіз правовідносин, що виникають у цій сфері.

Концепція монографії ґрунтується на тому методологічному посиленні, що, досліджуючи «онлайніві соціальні мережі», доцільно розрізняти «он-лайніві соціальні мережі» як:

1) ІТ-середовище (сегмент ІТ-середовища), у якому створюються/ забезпечуються можливості спілкування за допомогою інформаційних технологій;

2) система соціальних зв'язків / відносин, що виникають між користувачами онлайніві (соціальної) мережі;

3) організаційні форми / структури, організації, які надають послуги по забезпеченню користувачам спілкування в онлайніві соціальній мережі.

При цьому враховується, що «онлайніві соціальні мережі» у першому зі згаданих розумінь є сферою існування, радше фактичних / технологічних, ніж юридичних відносин. Тому, враховуючи, що правовому впливу піддаються «онлайніві соціальні мережі» у другому та третьому значенні, предметом дослідження були обрані саме пов'язані з ними цивільні відносини.

Водночас була взята до уваги та обставина, що правовий статус «соціальних мереж» у значенні «організаційні форми / структури, організації, які надають послуги по забезпеченню користувачам спілкування в онлайніві соціальній мережі», з погляду дослідження цивілістичних проблем цифрової доби, є менш цікавим, оскільки їх створення, функціонування, придбання та відчуження відбуваються на загальних підставах. Вони можуть належати окремій фізичній особі або їхнім об'єднанням (це може бути товариство з обмеженою відповідальністю, акціонерне товариство тощо). У своїй діяльності фізичні особи та організації, як власники онлайніві соціальних мереж, підпорядковуються національному законодавству та міжнародним угодам.

Значно цікавішими є питання правового регулювання відносин, що виникають у зв'язку з функціонуванням онлайніві соціальних мереж – усередині такої мережі та зовні, але у зв'язку з нею.

Їх дослідженню і присвячена, головним чином, ця монографія. Структура монографії обумовлена актуальністю питань, що виникають у зв'язку з функціонуванням соціальних мереж.

Перший розділ присвячено визначенню підходів до правового регулювання відносин в онлайніві соціальних мережах. Аналізується можливість, необхідність та співвідношення імперативних та

диспозитивних методів регулювання таких відносин. Зосереджена увага на механізмі саморегулювання та приватноправовому регулюванні відносин у соціальних мережах як кореляту інформаційного суспільства.

Другий розділ присвячено такому важливому питанню, як забезпечення захисту прав інтелектуальної власності в Інтернеті. Висвітлюються класичні та новітні підходи до захисту прав інтелектуальної власності, піднімаються питання необхідності захисту нових об'єктів авторських прав в Мережі, як-от файли HTML. Аналізуються такі способи захисту авторських прав в Інтернеті, як веб-блокування, процедура Takedown Notice. Досліджуються новітні підходи до використання засобів інформаційних технологій з метою полегшення судового процесу.

У третьому розділі висвітлюються питання функціонування інтерактивних соціальних мереж. Розглядається взаємовплив інтерактивних соціальних мереж і громадянського суспільства, роль інтерактивних соціальних мереж у реалізації діяльності громадянського суспільства. Робиться висновок, що усі відносини інтерактивного громадянського суспільства є правовим полем «ІТ-права» у широкому сенсі, включаючи як приватноправові, так і публічно-правові його складові.

У четвертому розділі розглядаються питання правового регулювання відносин у соціальних мережах. Аналізуються внутрішні правила поведінки користувачів у соціальних мережах на прикладі соціальної мережі Facebook, досліджується практика зарубіжних країн у питаннях регулювання відносин у соціальних мережах та захисту прав користувачів.

У розділі, присвяченому правочинам у соціальних мережах, розглядаються питання дійсності таких правочинів. Наводяться приклади платформ, що використовуються для електронної комерції, випадки найбільш поширених правопорушень, пов'язаних із укладенням електронних правочинів.

У розділі, присвяченому акаунтам у соціальних мережах, розглядаються актуальні сьгодні проблеми купівлі-продажу акаунтів, можливості заповідати акаунти та особливості вирішення проблем, що виникають у зв'язку із акаунтами у випадку смерті користувача. Зроблена спроба визначити правову природу акаунту в соціальній мережі як різновиду майнового активу. Проаналізовані проблеми захисту персональних даних та можливість їх кваліфікації як об'єкта права влансості.

Розділ, присвячений рекламі у соціальних мережах, містить спробу визначення поняття реклами у соціальній мережі, відмежування випадків, які не вважаються рекламою, аналіз недобро-

совісної реклами. Здійснено пошук відповіді на питання про те, хто повинен нести відповідальність за можливі порушення у разі визнання конкретного інформаційного повідомлення рекламою в соціальних мережах.

Восьмий розділ монографії присвячено проблемам правової охорони зображень людини у соціальних мережах. Проаналізовані випадки правомірного та неправомірного поширення зображень людини в соціальних мережах, можливості встановлення режиму доступу до зображень особи на її соціальній сторінці. Здійснено класифікацію випадків неправомірного використання фотографічних творів із зображенням фізичної особи. Визначені проблеми українського законодавства у питаннях правової охорони зображень людини у соціальних мережах.

У дев'ятому розділі монографії досліджуються проблеми захисту персональних даних у соціальних мережах. Увага акцентується на Правилах GDPR стосовно захисту та обробки персональних даних. Досліджуються основні права, що гарантуються користувачам вказаним актом, наслідки порушень у цій сфері.

Положення GDPR аналізуються й в наступному розділі, але вже під кутом зору реалізації прав дитини на захист персональних даних. Вказаний розділ містить також аналіз світової практики стосовно прав дітей на персональні дані, реалізації їх повноважень у соціальних мережах, співвідношення батьківських прав та прав дитини під час користування дитиною Інтернетом та, зокрема, соціальними мережами.

У десятому розділі проаналізовані моделі блокування доступу до інтернет-ресурсів, окрема практика блокування доступу до деяких соціальних мереж. Наведені випадки фільтрації контенту в Інтернеті та соціальних мережах, основні причини видалення контенту в Інтернеті та соціальних мережах, визначено, яка саме інформація може бути обмежена в соціальних мережах. Проаналізовано співвідношення необхідності блокування, фільтрації та видалення контенту в соціальних мережах та зобов'язань держави і корпорацій щодо гарантування права на свободу слова.

В одинадцятому розділі монографії висвітлено поняття та сутність інформаційного правопорушення, методи та засоби попередження та припинення інформаційних деліктів. Проаналізовано види інформаційних правопорушень у соціальних мережах.

Логічним завершенням монографії виступає розділ, присвячений відповідальності за дії, вчинені під час користування соціальними мережами. В останньому розділі аналізуються форми суспільної поведінки, які можуть призвести до відповідальності користувача соціальної мережі, а саме, так звані «тролінг» і «наклеп»,

проблеми кваліфікації репостів та лайків як підстав відповідальності, особливості відповідальності у соціальній мережі Facebook, законодавчі проблеми, що існують у вказаній сфері.

Також анонсуємо підготовку нової монографії «Кібербезпека: приватноправові аспекти» (серії «Цивілістика та «ІТ-право»). Колег, що займаються відповідною проблематикою, запрошуємо до участі.

Дякуємо за увагу!

Враження від монографії та побажання можна висловити за електронною адресою – civillaw@onua.edu.ua.

Автори монографії присутні також на сторінках Facebook.

Є. О. Харитонов,

доктор юридичних наук, професор,
член-кореспондент Національної академії
правових наук України,
заслужений діяч науки та техніки України,
завідувач кафедри цивільного права
Національного університету
«Одеська юридична академія»

К. Г. Некім,

кандидат юридичних наук, доцент,
доцент кафедри цивільного права

КОНЦЕПТУАЛЬНІ ПИТАННЯ ПРАВОВОГО РЕГУЛЮВАННЯ ВІДНОСИН У ОНЛАЙНОВИХ СОЦІАЛЬНИХ МЕРЕЖАХ

Одним з ключових питань забезпечення належного функціонування онлайнових соціальних мереж, прав та інтересів їхніх користувачів є визначення засад впорядкування, зокрема, правового регулювання відносин, що складаються у цій сфері.

Враховуючи багатозначність терміно-поняття «онлайнові соціальні мережі», у процесі дослідження проблем їхнього правового регулювання доцільно розрізняти «онлайнові соціальні мережі» як:

- 1) ІТ-середовище (сегмент ІТ-середовища), у якому забезпечуються можливості спілкування за допомогою інформаційних технологій;
- 2) система соціальних відносин, що виникають між користувачами онлайнової (соціальної) мережі;
- 3) організаційні форми / структури, організації, які надають послуги по забезпеченню користувачам спілкування в онлайновій соціальній мережі.

Що стосується першого зі згаданих розумінь терміно-поняття «онлайнові соціальні мережі», то у такому значенні це сфера існування, швидше, фактичних/ технологічних, ніж юридичних відносин. Тому, попри усю значущість і актуальність пов'язаних з цим проблем, залишимо тут поки що їх без розгляду, взявши до уваги, що правовому регулюванню підлягають «онлайнові соціальні мережі» у другому та третьому значенні.

Розглядаючи ці питання, зробимо попереднє зауваження щодо загального методологічного підґрунтя дослідження.

Такою основою є посилення, що правове впорядкування відносин у ІТ-сфері може і має здійснюватися за допомогою ІТ-права.

Про визначення поняття та сутності ІТ-права вже йшлося раніше, тому тут згадаємо лише основні принципово важливі положення авторського розуміння цієї категорії.

Передусім, ІТ-право не є цілісною сукупністю норм, яка могла б бути визнаною окремою галуззю права. Це впливає з того, що в ІТ-сфері складаються різноманітні суспільні відносини, котрі можуть впорядковуватися за допомогою юридичних прийомів як публічного, так і приватного характеру.

Та обставина, що до ІТ-сфери належать різноманітні інформаційні, інформаційно-технологічні, комунікативні тощо відносини, які за своєю сутністю є соціальними зв'язками по «горизонталі» та «вертикалі», а для їхнього впорядкування використовують як диспозитивний, так і імперативний методи, дає підстави для висновку про відсутність єдиного предмета та методу правового регулювання відносин ІТ-сфери. Натомість залежно від типу відносин, що регулюються, і конкретних завдань можуть застосовуватися цивільно-правовий або адміністративно-правовий методи. Звідси впливає, що «ІТ-право» не має єдиних предмета і методу правового регулювання, властивих лише йому, а тому не може бути визнане самостійною галуззю права.

Разом із тим, враховуючи існування сукупності нормативних актів, що регулюють відносини, пов'язані з ІТ, з певною мірою умовності можна вести мову про «ІТ-законодавство»¹.

Що стосується сутності феномена «ІТ-права», то вона має розглядатися не під кутом зору позитивістського / нормативістського праворозуміння, а з позицій цивілізаційного / культурологічного підходу, відповідно до якого право є цивілізаційним феноменом, виступаючи як елемент соціально-політичного устрою та як елемент суспільної свідомості. Відтак право розглядається як концепт – сукупність уявлень, понять, знань, асоціацій, емоцій, що виникають у зв'язку з використанням терміна «право», супроводжують і характеризують його. Відповідно «ІТ-право» розуміється як сукупність уявлень, понять, знань, асоціацій, емоцій, що виникають у зв'язку з правовим впорядкуванням суспільних відносин, пов'язаних зі створенням та використанням інформаційних технологій.

При цьому розгляд «ІТ-права» як концепту не заперечує «нормативного» наповнення цього поняття, але позбавляє необхідності оцінки його як системи правових норм, що утворюють галузь права, відповідні правові інститути тощо. Натомість може йтися про «структуру ІТ-права», яка відображає систему «нормативного наповнення» цього концепту.

¹ Пестова К. В., Кравчук В. В. ІТ-законодавство: проблеми, пріоритети та напрями розвитку // ІТ право: проблеми і перспективи розвитку в Україні: зб. матеріалів наук.-практ. конф. (Львів, 18 листоп. 2016 р.). Львів: НУ «Львів. політехніка», 2016. С. 126–127.

Розгляд «ІТ-права» під таким кутом зору зумовлює створення його парадигми, яка є альтернативою позиціям, котрі зараз набули певної популярності у вітчизняній юриспруденції, але не забезпечені відповідним науково-теоретичним підґрунтям. Запропонований підхід дає можливість зняти проблеми методологічного характеру, котрі неминуче виникають при використанні терміно-поняття «ІТ-права» на основі «нормативістського» розуміння права, у тому числі стосовно відносин у онлайнових соціальних мережах.

Розмаїття відносин, пов'язаних з інформаційними технологіями, зумовлює необхідність з'ясування орієнтирів для встановлення кола норм, які пов'язані з концептом «ІТ-право».

При визначенні таких орієнтирів виходимо з того, що поза межами «ІТ-права» знаходяться охоронні норми адміністративного, кримінального, митного, податкового тощо права, оскільки вони можуть стосуватися різних видів суспільних відносин, забезпечуючи їхню охорону.

Таким чином, нормативний масив концепту «ІТ-право» становлять регулятивні норми приватноправового (передусім цивільно-правові) та публічно-правового (адміністративно-правові) характеру.

У свою чергу, характеризуючи згадану умовну сукупність регулятивних норм, доцільно розрізняти «ІТ-право» у широкому та вузькому значеннях.

Під «ІТ-правом» у широкому значенні розуміємо сукупність усіх засад, норм і правил, що регулюють діяльність по використанню інформаційних технологій та інформаційної правомірної активності в Інтернеті. Структура «ІТ-права» у широкому значенні виглядає як відносно інтегрована система багаторівневого порядку, що містить приватноправові та публічно-правові елементи. Необхідність врахування приватноправового та публічно-правового забарвлення ІТ-відносин має враховуватися, аби визначити пріоритетність інтересів (приватні чи публічні) і на цьому підґрунті особливості методів правового регулювання, що застосовуються.

ІТ-відносини, пов'язані зі створенням та припиненням юридичних осіб, відносини інтелектуальної власності, договірні відносини у сфері ІТ, спадкування за заповітом тощо належать до приватноправової сфери правового регулювання. Такі відносини переважно є регулятивними, але можуть також супроводжуватися цивільними організаційними відносинами (створення юридичних осіб тощо). Оскільки йдеться про сферу приватного права, де принцип «Дозволено все, що не заборонено законом» надає договору значення норми цивільного законодавства, можна стверджувати, що

саме за його допомогою складається основний масив норм, які можуть бути віднесені до «ІТ-права».

«ІТ-право» у вузькому значенні – це сукупність регулятивних норм (переважно цивільно-правових), що правовими засобами забезпечують функціонування ІТ-відносин.

Крім того, доцільним є виокремлення «ІТ-права у спеціальному значенні». При цьому до відповідного нормативного масиву мають бути віднесені вже лише ті норми, що стосуються суто сфери ІТ-інформаційних відносин; створення та використання програмного забезпечення; Інтернет-відносин, функціонування онлайн-соціальних мереж тощо.

Спираючись на таке методологічне підґрунтя розуміння «ІТ-права», спробуємо з'ясувати особливості правового регулювання відносин, пов'язаних з онлайн-соціальними мережами.

Насамперед, маємо зазначити, що правовий статус «соціальних мереж» у значенні «організаційні форми /структури, організації, які надають послуги по забезпеченню користувачам спілкування в онлайн-соціальній мережі», менше вартує уваги, оскільки їх створення, функціонування, придбання та відчуження відбуваються на загальних підставах. Вони можуть належати окремій фізичній особі або їхнім об'єднанням (це може бути товариство з обмеженою відповідальністю, акціонерне товариство тощо. Так, 1 жовтня 2006 року доменне ім'я *vkontakte.ru* було зареєстроване товариством з обмеженою відповідальністю «ВКонтакте». Цю дату прийнято вважати датою заснування сайту¹.

Власниками соціальної мережі *Odnoklassniki.ru* спочатку була група фізичних та юридичних осіб: Альберту Попкову належало 31,9 % компанії, а його дружині Ірині – 31,8 %, 18 % акцій було в *Digital Sky Technologies* і 18,3 % – в естонської *Ou Tobias*. У вересні 2008 року у подружжя Попкових залишилося по 21 %, у *Ou Tobias* і *Digital Sky Technologies* у сумі 58 %, але контроль над мережею в останніх. Керуючою компанією є *Odnoklassniki Ltd.*, що зареєстрована в Лондоні. Її статутний капітал становить 1402 фунти стерлінгів (\$2800)².

У своїй діяльності фізичні особи та організації, як власники онлайн-соціальних мереж, підпорядковуються загальним та спеціальним нормам міжнародних угод та національного законодавства.

Значно важливішими є питання правового регулювання відносин, що виникають у зв'язку з функціонуванням онлайн-со-

¹ *ВКонтакте*. URL: <https://uk.wikipedia.org/wiki/ВКонтакте>.

² *Однокласники*. URL: <https://uk.wikipedia.org/wiki/Однокласники>.

ціальних мереж: 1) усередині такої мережі та 2) зовні мережі, але у зв'язку з нею.

Передусім, варто звернути увагу на існування низки труднощів щодо визначенням характеру типу та обсягу нормативного масиву, що стосується впорядкування відносин у онлайн-ових соціальних мережах.

Зокрема, це пов'язане з недостатністю (а у багатьох випадках — просто з відсутністю) законодавчих актів, які б регулювали відносини у таких мережах, на чому загострюють увагу практично усі дослідники відповідної проблематики.

Крім того, існує специфічна проблема «внутрішньо мережевого» впорядкування відносин між учасниками останніх, частина з яких може й не мати ознак суб'єктів права. Наприклад, повідомлялося, що кілька років тому на сайті «Однокласники» з'явилася можливість створювати так звані «групи». Після цього на сайті виникли нові форми спілкування. З'явилися різноманітні «фамільні», «армійські» групи та групи за інтересами, очолювані своїми адміністраторами (групи: «Ангели у камина», «ПіК» та ін.) тощо. Між деякими групами точаться «війни», ведуться «перемовини» та укладаються «угоди». Автори допису про сайт «Однокласники» стверджують, що таким чином цей сайт став цікавим об'єктом для соціологів і політологів¹. Не заперечуючи цю тезу, варто наголосити, що не менш цікавим об'єктом ці стосунки є для правознавців.

Отже, розглянемо засади та можливі способи вирішення проблем основи регулювання відносин, що виникають при спілкуванні користувачів у онлайн-ових соціальних мережах.

Для початку повернімося до висловленого раніше твердження, що основою впорядкування відносин у ІТ-сфері є регулятивні норми, а наслідком такого впорядкування — регулятивні правовідносини.

Однак при цьому необхідно розрізнати регулювання функціонування соціальної мережі, тобто її статусу стосовно «зовнішнього» світу, і регулювання діяльності її користувачів, тобто відносин усередині мережі. Якщо функціонування онлайн-ової соціальної мережі (нагадаємо, що з погляду опису системи категорій ІТ-сфери вона може бути охарактеризована як сайт, сервіс, програма) може регулюватися за допомогою традиційних засобів (видання актів законодавства тощо), то діяльність її користувачів внаслідок специфіки ІТ регулювати таким чином, практично, неможливо (та й необхідності у цьому в громадянському суспільстві нема). Коли ж йдеться про обмеження чи заборони, то обмеження і заборони,

¹ *Однокласники*. URL: <https://uk.wikipedia.org/wiki/Однокласники>.

по-перше, стосуються діяльності такої мережі, а не її користувачів, а по-друге, тут має місце апеляція до охоронної, а не регулятивної функції права.

Разом із тим авторами публікацій на теми правового регулювання у цій галузі зазначена необхідність розмежування впливу на «зовнішній» і «внутрішній» бік буття онлайнової соціальної мережі враховується далеко не завжди. До того ж часом ігноруються й засади правового регулювання у сучасних умовах.

Наприклад, А. В. Галунько, досліджуючи «соціальні інтернет-мережі як об'єкт адміністративно-правового регулювання» (так називається його стаття і про це йдеться в анотації до неї), зазначає, що держава має регулювати на основі норм права діяльність таких мереж «тільки в тому випадку і в тому об'ємі, в якому поступають скарги від громадян про порушення їх прав». Така теза дає підстави для припущення, що йдеться про регулятивну функцію права у об'єктивному сенсі. Однак автор доволі своєрідно розуміє поняття «правове регулювання», а відтак вибудовує досить оригінальну конструкцію, яку варто навести дослівно: «Спочатку встановлюються державою норми цивільного права, щоб на їх основі фізичні і юридичні особи могли на основі диспозитивного методу самостійно чи через суд вирішувати свої суперечки, відновлювати порушені права. Якщо цього стає недостатньо, кількість порушень прав осіб зростає, незважаючи на цивільно-правове регулювання, держава має переходити до публічного регулювання цих відносин. Поперед всього на основі норм адміністративного права, а коли порушенням стає притаманна значна небезпека, переходить до кримінально-правового захисту. Таким чином, місце адміністративно-правового регулювання діяльності Інтернет-мереж полягає в об'єктивних засадах необхідності захистити права фізичних і юридичних осіб нормами адміністративного права, коли здійснити такий захист на основі цивільно-правових та інших соціальних норм неможливо, а протиправні діяння... не набули значної суспільної небезпеки»¹. Отже, анонсувавши дослідження проблем адміністративно-правового регулювання, у статті автор фактично описує алгоритм введення в дію охоронної функції адміністративного права (іменуючи при цьому охоронні правовідносини «регулятивними»). Це приводить його до висновку, вартого того, аби знов-таки навести його дослівно: «Отже, соціальні інтернет-мережі як об'єкт адміністративно-правового регулювання – це система прав фізичних і юридичних осіб (засновників, авторів аудіовізуального кон-

¹ Галунько А. В. Соціальні інтернет-мережі як об'єкт адміністративно-правового регулювання // Науковий вісник Ужгородського національного університету. Серія ПРАВО. 2013. Вип. 22, ч. 1, т. 2. С. 127–129.

тенту та численних користувачів), які порушуються третіми особами в таких мережах, охорона яких здійснюється публічною адміністрацією на основі адміністративно-правових норм, у випадку неможливості їх захисту на основі цивільно-правових та інших соціальних норм»¹.

Наведений вище текст, можливо, не був би вартий окремої згадки, якби не відображав досить наочно поширені хиби спрощеного бачення регулювання відносин у ІТ-сфері, а також і наслідки недостатньо чіткого розрізнення категорій суб'єктивного та об'єктивного права.

Тому доцільно згадати засади соціального управління, котре є засобом впорядкування соціальної взаємодії, у тому числі в онлайнових соціальних мережах, та значення у такому контексті дихотомії «приватне право» – «публічне право».

Не витрачаючи тут час і місце на характеристику зазначеної дихотомії та критеріїв її складових, нагадаю лише, що поширеним критерієм розмежування приватного та публічного права, який був використаний свого часу Ульпіаном і став відомим завдяки Дигестам Юстиніана, є надання переважного значення інтересам людини (приватної особи) або держави. Неодноразово він використовувався і правознавцями новіших часів.

Як зазначав К. Ф. фон Савіньї, у публічному праві ціле (держава) виявляється метою, а окрема особистість підпорядкованою, тоді як у приватному праві кожна окрема людина сама по собі є метою, а кожне правове відношення стосовно її існування або особливого становища є лише засобом².

З точки зору оцінки спрямованості захисту інтересів приватне право захищає приватні інтереси окремих осіб, а публічне право – інтереси держави, загальні, суспільні інтереси.

Разом із тим «природні права» людини, що складають найважливіший елемент її загального статусу, належать саме до приватного права та існують незалежно від того, чи визнані вони об'єктивним правом, чи ні. Іншими словами, вони є об'єктивними в силу своєї природності, невідчужуваності від людини і вважаються такими, що надані Богом.

У зв'язку з цим важливе значення має врахування положень «вольової теорії» Єлінека, суть якої полягає в тому, що право у суб'єктивному сенсі трактується як пріоритет людської волі, спря-

¹ Галуцько А. В. Соціальні інтернет-мережі як об'єкт адміністративно-правового регулювання // Науковий вісник Ужгородського національного університету. Серія ПРАВО. 2013. Вип. 22, ч. I, т. 2. С. 127–129.

² Савіньї Ф. К. фон. Система современного римского права. Т. 1 / пер. с нем. Г. Жигулина; под ред. О. Кутателадзе, В. Зубаря. Москва, 2011. С. 286–287.

мованої на певне благо або інтерес. Ця пріоритетність визнається і захищається правопорядком. Переважання волі — це формальний елемент, а благо чи інтерес — матеріальний елемент у суб'єктивному праві. У свою чергу, окремі інтереси, на думку Єлінека, розпадаються на такі, що встановлені переважно задля індивідуальних цілей (цілей окремих осіб), і такі, які встановлено переважно задля суспільних цілей. Визнаний переважно для суспільного інтересу індивідуальний інтерес складає зміст публічного права. Суб'єктивне публічне право зі свого матеріального боку є таким правом, що належить окремій особі на підставі його статусу як члена держави.

Щодо формального елемента прав, пріоритетності волі Єлінек розрізняє два його види: *dürfen* (бажання, прагнення, устремління) і *können* (можливість). *Dürfen* буквально перекладається з німецької як «мати бажання, сміти щось робити». У цьому випадку «правопорядок визнає відповідні дії індивідуума дозволеними, тобто він дозволяє індивідуальній волі здійснювати у певних напрямках свою свободу». *Können* означає «могти, бути в змозі» і тут «правопорядок може до природної можливості індивідуума до дій додати таке, що йому від природи не належить... а саме, надати йому право на те, що певні його дії визнаватимуться юридично дійсними і такими, що матимуть позовний захист». Таким чином, приватне суб'єктивне право містить у собі як *dürfen*, так і *können*, а публічне суб'єктивне право — тільки *können*. Отже, у приватному праві завжди є устремління (*dürfen*), а у публічному — лише можливість (*können*). Публічні права ґрунтуються не на таких, що дозволені, а лише на таких, які надані владою. Тому вони являють собою не частину природної, врегульованої правом свободи, а розширення прав природної свободи¹.

Підсумовуючи викладене, можна дійти висновку, що сфера публічного права — це, передусім, питання субординації і підпорядкування однієї особи іншій, питання компетенції державних органів і посадових осіб, з одного боку, а з іншого — пасивної, як правило, правосуб'єктності підпорядкованих і підвладних осіб, їх обов'язків та відповідальності, що випливають із владних актів державних органів і посадових осіб. У приватноправовій сфері правосуб'єктність учасників цивільних відносин є однаковою і ґрунтується на засадах юридичної рівності, свободи їхньої волі та ініціативності при встановленні правовідносин, а потім — реалізації ними відповідних суб'єктивних прав і обов'язків.

Не торкаючись тут детально проблем визначення поняття, сутності та змісту приватного права, згадаємо лише, що у вітчизня-

¹ Еллинек Г. Общее учение о государстве / вступ. ст. И. Ю. Козлихина. Санкт-Петербург, 2004. С. 376.

ній цивілістиці в якості характерних рис приватного права зазвичай називається те, що воно: 1) регулює відносини між приватними особами, тобто між особами, жодна з яких не є фігурантом держави; 2) має визначальним принципом визнання пріоритету інтересів приватної особи (суверенітету індивіда); 3) забезпечує приватний інтерес: акцентує увагу на економічній свободі, вільному самовираженні та рівності товаровиробників, захисті власників від сваволі держави; 4) ґрунтуючись на засадах юридичної рівності учасників цивільних відносин, забезпечує ініціативність сторін при встановленні цивільних відносин та вільне волевиявлення суб'єктів при реалізації їхніх прав; 5) припускає широке використання договірної форми регулювання; 6) містить норми, які «звернені» до суб'єктивного права і забезпечують захист останнього; 7) характеризується переважанням диспозитивних норм, які спрямовані на максимальне врахування вільного розсуду сторін при виборі правил поведінки, прямо не заборонених законодавством; 8) визначає судовий позов як основний порядок захисту інтересів суб'єктів цивільних відносин у суді.

Джерелами приватного права, що визначають його сутність та зміст, є: 1) природне право — як основа визначення статусу приватної особи; 2) національні правові системи, що визначають юридичний статус приватної особи, а також засади захисту прав та інтересів останньої; 3) колізійні норми, що передбачають компроміси при визначенні статусу приватної особи у різних національних правових традиціях тощо; 4) міжнародно-правові угоди, що стосуються зазначених питань.

Приватне право, так само як і право публічне, є наднаціональною системою права.

Цивільне та адміністративне право є проявом приватного та публічного права на рівні національних правових систем, виступаючи тут як галузі національного права (цивільне/ адміністративне право в об'єктивному сенсі).

Разом із тим при визначенні поняття, скажімо, цивільного права необхідно враховувати такі обставини, як структурний поділ права на об'єктивне (сукупність чинних у країні юридичних норм, правил і принципів) і суб'єктивне (належить певним суб'єктам), зумовлений соціальними і спеціально-юридичними закономірностями. При цьому розрізняють суб'єктивне право у широкому та вузькому значенні. Суб'єктивне право у широкому значенні — це все те, що впливає з правових норм (об'єктивного права) для його носія і характеризує його як суб'єкта права. Визнання особи і організації суб'єктом права дістає вияв у тому, що вони через норми об'єктивного права набувають якостей учасника відповідних



правовідносин. Суб'єктивне право у вузькому сенсі розуміється як право (можливість певної поведінки) особи, яке передбачене правовою нормою¹.

Проте більшість правознавців ведуть мову про суб'єктивне право як єдине поняття, визначаючи його як зумовлену об'єктивним правом міру можливої поведінки уповноваженого суб'єкта. Зміст суб'єктивного права, на їхню думку, охоплює три правоможності: 1) праводію – право уповноваженого суб'єкта на певні дії; 2) протиправного вимогу – право уповноваженого суб'єкта вимагати певної поведінки від інших осіб; 3) право претендування – право уповноваженого суб'єкта звернутися до державних органів за захистом своїх порушених прав².

Об'єктивне (цивільне) право знаходиться в одній площині з правом приватним, цивільним законодавством та іншими правовими категоріями, які стосуються абстрактного суб'єкта відносин, передбачаючи і закріплюючи існування для останнього потенційних прав та обов'язків. Натомість суб'єктивне право належить конкретному суб'єкту – учаснику цивільних відносин, які знаходяться у сфері правового регулювання. Перебуваючи у діалектичній єдності, вони разом із тим не можуть бути однаковими за сутністю призначенням, змістом тощо.

При цьому слід згадати висловлену вище тезу, що поділ права на приватне і публічне є науковою абстракцією, яка дозволяє у найбільш загальних рисах характеризувати два головних напрями правового регулювання суспільних відносин. Що стосується реальних відносин, то вони підлягають регулюванню на засадах приватного або публічного права в залежності від їх конкретного змісту. На рівні національного права це знаходить відображення у розрізненні галузей національного права, зокрема, цивільного та адміністративного, які виступають як прояв засад приватного або публічного права при регулюванні відповідних груп відносин.

Проте некоректним є ототожнення приватного права з правом цивільним, а права публічного – з правом адміністративним. Натомість має йтися про те, що у цивільному праві переважно проявляються засади, правила та норми приватного права, а у праві адміністративному – засади та норми публічного права.

Зазначеним детермінуються особливості галузевих методів правового регулювання, котрими, зокрема, визначається: 1) яким є юридичне становище осіб, визначене правовою нормою; 2) з яки-

¹ Колодій А. М. Принципи права України: монографія. Київ: Юрінком Інтер 1998. С. 93–94, 169.

² Крестовская Н. Н., Матвеева Л. Г. Теория государства и права: учебник. Харьков: Одиссей, 2007. С. 287–288.

ми обставинами (юридичними фактами) норма права пов'язує виникнення, зміну, припинення та інші трансформації правовідносин; 3) яким чином визначаються права і обов'язки учасників відповідних правовідносин; 4) яким є порядок захисту прав та інтересів учасників правовідносин.

Базовими категоріями при визначенні особливостей галузевих прийомів юридичного впливу на суб'єктів цивільних відносин є імперативний та диспозитивний методи правового регулювання, що визначають головне у вихідних юридичних позиціях суб'єктів.

Імперативний метод (метод субординації) характеризується тим, що регулювання здійснюється згори вниз і ґрунтується на владно-імперативних засадах.

Диспозитивний метод (метод координації) характерний для регулювання на засадах формальної рівності, ініціативності та вільного розсуду учасників відповідних відносин. На процес такого регулювання впливає активність учасників суспільних відносин, що регулюються за його допомогою. Його характерними властивостями є: 1) регулювання відносин між юридично рівними учасниками немайнових та майнових цивільних відносин (особами приватного права); 2) визнання пріоритетності волевиявлення приватної особи стосовно положень актів законодавства, що виражається у перевазі в останньому диспозитивних норм; 3) забезпечення приватного інтересу із акцентуванням уваги на економічній свободі та рівності товаровиробників, захисті власників від сваволі держави; 4) широке використання «уповноважуючих» норм, які забезпечують ініціативність сторін при встановленні цивільних відносин та вільне волевиявлення суб'єктів при реалізації їхніх прав; 5) широке використання договірної форми регулювання цивільних відносин; 6) максимальне врахування вільного розсуду сторін при виборі правил поведінки, прямо не заборонених законом.

У характерних рисах диспозитивного методу проявляються особливості приватного права, що складається із сукупності гуманітарних ідей, правових принципів, правил і норм, що стосуються визначення статусу і захисту інтересів людини.

У свою чергу, диспозитивний метод є одним із визначальних чинників особливостей методу цивільно-правового регулювання, котрий розуміємо як сукупність специфічних засобів впливу на учасників цивільних відносин, що характеризуються, передусім, юридичною рівністю сторін, а також наданням останнім можливості врегулювання цих відносин на засадах їхнього вільного розсуду.

Для методу цивільно-правового регулювання у більшості випадків властивою є відсутність категоричних приписів учасникам цивільних відносин діяти певним чином (виняток складають цивільні

охоронні правовідносини – зобов'язання відшкодувати шкоду, деякі вимоги стосовно оформлення правочинів тощо), тобто останнім надаються повноваження обрати тип поведінки, самостійно врегулювати свої відносин. Разом із тим цивільно-правовий метод може містити й обов'язкові (імперативні) приписи, включаючи в себе не лише уповноважуючий елемент, але й елемент імперативний. Характерними рисами уповноважуючого (диспозитивного) елемента методу цивільно-правового регулювання є: 1) юридична рівність сторін; 2) ініціатива сторін при встановленні правовідносин; 3) можливість вибору учасниками цивільних відносин варіанта поведінки, що не суперечить засадам цивільного законодавства і моральності суспільства. Характерними рисами імперативного елемента цивільно-правового методу є: 1) юридична рівність сторін; 2) виникнення правовідносин незалежно від бажання учасників цивільних відносин – внаслідок безпосереднього припису закону; 3) можливість вибору учасниками цивільних відносин варіанта поведінки лише у межах, точно визначених актами цивільного законодавства. Таким чином, метод цивільно-правового регулювання охоплює як диспозитивні (у регулятивних цивільних відносинах), так і імперативні (у охоронних і, значною мірою, в організаційних цивільних відносинах) засоби впливу на учасників цивільних відносин, маючи, однак, при цьому основою засади юридичної рівності сторін, справедливості, добросовісності та розумності.

Отже, метод цивільно-правового регулювання, як система юридичних засобів впливу на учасників цивільних відносин, характеризується, передусім, забезпеченням диспозитивності поведінки останніх, припускаючи водночас можливість застосування у випадках, встановлених законом, імперативного впливу на учасників цивільних відносин.

Стосовно відносин, що виникають у онлайн-ових соціальних мережах, викладені вище положення виглядають наступним чином.

Регулювання відносин у Мережі відбувається за допомогою цивільно-правового методу, внаслідок чого виникають регулятивні цивільні відносини, особливістю яких є їхня подвійна природа: імперативно-приписуюча та уповноважувальна.

Ця «подвійність» виражається у тому, що при «позитивному» регулюванні цивільних відносин відбувається «надання» цивільних прав та обов'язків учасникам цих відносин, відповідно до встановлених норм та правил поведінки суб'єктів цивільних прав. При цьому «нормативною» основою їхнього виникнення можуть бути як норми цивільного законодавства, так і норми природного права. У цьому випадку має місце застосування імперативного спектра цивільно-правового методу. Такого типу відносини виникають за-

звичай між онлайнною соціальною мережею (організаційно-правовою формою, в якій вона існує) та її учасниками. Договір, який пропонується Мережею для підписання потенційному користувачу, містить односторонньо сформовані умови і є по суті договором приєднання. Варто зазначити, що у тих випадках, коли відносини Мережа – Користувач (зміст відповідного договору) не врегульовані актами законодавства, сам договір встановлює норми поведінки (тобто є нормою законодавства). Це, однак, не заперечує імперативного характеру встановлених ним правил.

Разом із тим регулятивні цивільні правовідносини в онлайнних соціальних мережах можуть виникати в результаті реалізації цивілістичної функції уповноваження, за допомогою якої створюється нормативна база – передумови для саморегулювання у сфері приватного права. Завдяки цій специфічній цивілістичній функції учасники цивільних відносин можуть самі визначати для себе правила поведінки, створювати фактично нормативні акти локальної дії тощо. Її концептуальною основою є відома ще римському приватному праву сентенція «Дозволено усе, що не заборонено законом». Відтак на зазначеному підґрунті за наявності певних умов виникають цивільні права і обов'язки.

Цивільні правовідносини такого типу виникають між користувачами онлайнних соціальних мереж, їхній зміст визначається домовленостями учасників. Вони не потребують додаткового правового регулювання і можуть обійтися без такого, якщо тільки не йдеться про відносини, норми щодо яких вже містяться в актах цивільного законодавства.

Звісно, можлива радикальна спроба тотального врегулювання відносин між учасниками онлайнних соціальних мереж за допомогою актів законодавства. Однак вони навряд чи можуть бути ефективними.

Звісно, такий висновок не є заклик до повернення у так званий «романтичний період розвитку Інтернету» з його гіпертрофованими сподіваннями на механізм саморегулювання у цій галузі, неодноразово підданий критиці правознавцями¹.

Натомість йдеться про використання потенціалу і засад приватноправового регулювання, як кореляту інформаційного суспільства (з усіма перевагами і недоліками останнього).

¹ Баранов А. А. Інтернет: объект правоотношений и предмет регулирования: монография. Киев: Ред. журн. «Право Украины»; Харьков: Право, 2013. 144 с. (Науч. сб. «Академичні правові дослідження». Прил. к юрид. журн. «Право України»; вып. 30); Битяк О. Ю. Правове регулювання суспільних відносин, пов'язаних із використанням мережі Інтернет // Проблеми законності: зб. наук. пр. Харків, 2015. Вип. 129. С. 198–207. URL: http://nbuv.gov.ua/UJRN/Pz_2015_129_26.

СОЦІАЛЬНІ МЕРЕЖІ І ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ: ПРОБЛЕМИ І ПЕРСПЕКТИВИ

Головними тенденціями у сфері соціальних мереж на сьогодні є активне збільшення їхньої аудиторії, постійна поява нових сервісів та глобалізація. Позитивними напрямками розвитку соціальних мереж стає їхнє використання як інструментів для бізнесу, освіти та набуття ними рис повноцінних засобів масової інформації¹.

Попри велику кількість переваг соціальних мереж, вони несуть низку небезпек: за допомогою мереж можлива активізація сепаратистських та інших незаконних рухів, порушення прав інтелектуальної власності, знищення приватності, крадіжка особистості та ін.

Так, за результатами аналізу даних із судового реєстру в Україні за період з 2014 до 2017 року винесено 50 вироків у справах про заклики до насильницького повалення влади, з яких 36 вироків суду так чи інакше пов'язані з поширенням відповідних закликів через соціальні мережі. Іншими словами, щонайменше одну особу в місяць за останні три роки було виявлено та затримано за антиукраїнську агітацію в соцмережі. Крім того, предметом дослідження слідства стають навіть коментарі у публічних дописах. Наприклад, Прес-центр СБУ повідомив, що у місті Березівка Одеської області 19 жовтня 2017 року затримано місцевого мешканця, який на своїх персональних сторінках через російські соціальні мережі поширював матеріали із закликами до зміни державного кордону і конституційного ладу України та популяризував терористичні організації «ДНР/ЛНР». Відкрите кримінальне провадження за частиною другою статті 110 Кримінального кодексу України, якою встановлюється кримінальна відповідальність за умисні дії, вчинені з метою зміни меж території або державного кордону України на порушення порядку, встановленого Конституцією України, а також

¹ *Попова Т.* Соціальні мережі, кібератаки та гібридні війни. URL: <https://www.radiosvoboda.org/a/28598299.html>.

публічні заклики чи розповсюдження матеріалів із закликами до вчинення таких дій, якщо вони вчинені за попередньою змовою групою осіб¹.

З появою Web 2.0, як уже зазначалося, відбулася трансформація ролі звичайного користувача зі споживача на активного автора онлайн-контенту. Якщо в перші роки популярності мережі звичайний користувач був пасивним споживачем і його активність відображалася лише на деяких спеціальних сайтах, то зараз практично кожен, хто хоч зрідка заходить в Інтернет, є активним автором, творцем сучасного Інтернету. Адже людина залишає коментарі, спілкується в соцмережах, відзначає статті кнопками «клас» та «Like». Це означає, що діяльності навіть не дуже активного користувача достатньо для того, щоб скласти його онлайн-портрет.

Вчені Кембріджського університету виявили, що навіть те, як користувач ставить «лайки» у Facebook, може розповісти багато що про його політичні та релігійні погляди, сексуальну орієнтацію, сімейний стан, шкідливі звички й інші аспекти особистої інформації, які він не хоче розкривати у своєму профілеві. А сучасні комп'ютерні програми дозволяють «витягти» усю цю інформацію з соцмереж і проаналізувати її. За підсумками цього дослідження науковцям, аналізуючи «лайки», вдалося з вірогідністю 88 % визначити сексуальну орієнтацію чоловіків, які брали участь у дослідженні, 95 % – расову приналежність, 80 % – політичні і релігійні погляди, які не були відображені в профілях².

Показовим в цьому є нещодавній скандал з використанням персональних даних соцмережі Facebook – Фейсбуктейт. Витік персональних даних понад 50 млн користувачів соцмережі, через які здійснювався вплив на вибори в США та Brexit. Як так сталося та чим це може обернутися для Facebook і світу? Почалося все з безпечного на вигляд психологічного додатку-тесту, розміщеного в Facebook в 2015 році. Його розробником був співробітник Кембриджського університету Александер Коган. Що цікаво, вчений має російське походження та є чинним доцентом Санкт-Петербурзького університету. Ще більш цікаво, що він отримував гранти від російського уряду на вивчення поведінки користувачів у мережі.

Офіційно тест у мережі розміщували винятково «для наукових цілей», тому у Facebook це дозволили. Вчені намагалися дослідити психологічні портрети користувачів на основі їхніх лайків.

¹ Ситницька А. Анонімність у мережі. Правові засади затримання користувачів соціальних мереж. URL: <http://jurblog.com.ua/2017/10/anonymnist-u-merezhi-pravovi-zatrimannya-koristuvachiv-sotsialnih-merezh>.

² Соціальні мережі – вільний обмін думками чи маніпулювання свідомістю? URL: <http://xpress.sumy.ua/articles/5700>.

Коган розмістив тест в Facebook, пропонуючи респондентам за відповіді на питання невелику грошову винагороду. Загалом інформацію про себе під час проходження тесту розкрили близько 270 тис. користувачів (здебільшого американців). Потім ці дані потрапили до рук Cambridge Analytica, яка займається впливом на поведінку користувачів у соціальних мережах. Цікаво, що компанія створена в 2013 році за участю сім'ї Мерсер, головних донорів передвиборного штабу Дональда Трампа, а віце-президентом компанії є Стівен Беннон – колишній радник Трампа. До того ж свого часу Беннон був редактором Breitbart News – британського видання, яке просувало ще не надто популярну на той час ідею Brexit. Дізнавшись про витік даних, Facebook вимагає видалити додаток та знищити всю інформацію про користувачів. Домовленості з Коганом та СА ніби-то вдалося досягти, але нещодавно виявилося, що зібрані дані про користувачів досі існують. Журналісти закидають Facebook нехтування належним захистом персональних даних користувачів, а Вайлі стверджує, що соцмережа не перевіряла їх знищення¹. Цукерберг пообіцяв докласти всіх можливих зусиль, щоб подібна ситуація більше не повторилася. Тож тепер у Facebook видалять апікації, що викликають підозри, та обмежать доступ для розробників додатків. Буде доступними лише ім'я, фото та електронна пошта юзера, щоб отримати решту даних розробнику потрібно буде підписувати окремий контракт з користувачем.

Однак після цього скандалу світ ніколи не стане таким, як раніше. Ймовірно, регулятори в США та інших країнах світу почнуть жорсткіше пильнувати соціальні мережі та ухвалюють законодавчі обмеження, пов'язані зі збиранням та використанням персональних даних, а також рекламою в Facebook.

Принаймні, перші кроки до цього вже є. 21 березня 2018 року Європейська комісія заявила про плани щодо введення 3 % податку на прибуток (від реклами, продажу цифрових даних) технологічних гігантів на кшталт Google, Facebook і Amazon, пише Financial Times².

Джон Нотон, професор такої науки, як суспільне розуміння технології, пише в The Guardian: «Ми спостерігаємо наростання страху на кшталт «Господи, що ми накоїли?» серед колишніх працівників Google і Facebook, які почали усвідомлювати, що чудовий матеріал, над котрим вони працювали, міг мати антисоціальні наслідки. Коли сказати просто, то Google і Facebook виробили кіль-

¹ *Фейсбукгейт*. Як соцмережа для знайомства студентів стала політичною зброєю. URL: https://espreso.tv/article/2018/03/23/feysbukgeyt_yak_socmerezha_dlya_znayomstva_studentiv_stala_politychnoyu_zbroyeyu_ta_scho_z_cogo_bude.

² Там само.

ка навдивовижу складних, заснованих на комп'ютерах механізмів для видобування особистої інформації користувачів та електронних реєстрів їхніх дій у мережі, конкретизації їх для продажу рекламодавцям на швидкісних аукціонах даних – абсолютно нерегульованих і непрозорих для всіх, крім самих компаній». Сенді Паракілас, що працювала у Facebook директоркою-розпорядницею, відверто пише в The New York Times: «Зсередини я бачила компанію, яка надає пріоритет зборові даних від своїх користувачів, а не захисту їх від зловживань... Facebook знає, хто ви, про ваше перебування, які ваші друзі, зацікавлення, чи перебуваєте ви у стосунках, які інші сторінки ви відвідуєте в мережі. Ця інформація дає рекламодавцям змогу досягнути понад мільярд відвідувачів Facebook за день... Коли росіяни вирішили доступитися до американців під час виборів 2016-го, то не купували телевізійних чи газетних рекламних оголошень, не наймали літак, щоб випишував гасла на небі, а звернулися до Facebook, де їхній контент дійшов принаймні до 126 млн американців. Саме те, що цей ресурс надає пріоритет зборові даних, а не захисту користувачів, і робить його таким привабливим»¹.

Законодавчому регулюванню захисту персональних даних присвячено закони України «Про захист персональних даних» та «Про доступ до публічної інформації». Останній визначає види інформації: конфіденційна, таємна та службова. В цій ситуації заслуговує на увагу конфіденційна інформація – це інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку, за їхнім бажанням, відповідно до передбачених ними умов.

Згідно із Законом України «Про захист персональних даних», згодою суб'єкта персональний даних є добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди. Головною вимогою Закону «Про захист персональних даних» є обов'язок володільців, розпорядників персональних даних і третіх осіб забезпечити захист цих даних від випадкової втрати чи знищення, від незаконної обробки, в тому числі від незаконного знищення та доступу до персональних даних. На жаль, Facebook не завжди може гарантувати таке забезпечення.

¹ Єжи Онух. Як і чому нам загрожують соціальні мережі? URL: <http://uainfo.org/blognews/1513336173-yak-i-chomu-nam-zagrozhuut-sotsialni-merezhi.html>.

З метою забезпечення захисту персональних даних в Європейському Союзі були розроблені нові правила обробки персональних даних і прийнятий Загальний регламент щодо захисту даних (Регламент ЄС 2016/679 від 14 квітня 2016 року або GDPR – General Data Protection Regulation), який вступив в силу з 24 травня 2016 року і після дворічного перехідного періоду почав застосовуватися з 25 травня 2018 року. Тепер компанії, що порушують правила обробки персональних даних, ризикують бути залученими до відповідальності з накладенням штрафів у 2 млн євро або 4 % річного доходу компанії.

До основних принципів обробки персональних даних по GDPR відносяться: 1) законність, справедливість і прозорість: персональні дані повинні оброблятися законно, справедливо і прозоро. Будь-яку інформацію про цілі, методи і обсяги обробки персональних даних слід висловлювати максимально доступно і просто; 2) обмеження мети: дані повинні збиратися і використовуватися виключно в тих цілях, які заявлені компанією (онлайн-сервісом); 3) мінімізація даних: не можна збирати особисті дані в більшому обсязі, ніж це необхідно для цілей обробки; 4) точність: особисті дані, які є неточними, повинні бути видалені або виправлені (на вимогу користувача); 5) обмеження зберігання: особисті дані повинні зберігатися у формі, яка дозволяє ідентифікувати суб'єктів даних на термін не більше, ніж це необхідно для цілей обробки; 6) цілісність і конфіденційність: при обробці даних користувачів компанії зобов'язані забезпечити захист персональних даних від несанкціонованої або незаконної обробки, знищення та пошкодження¹.

Отже, найважливішим для збору даних є згода людини на такий збір і обробку. Згідно з GDPR, згода користувача має бути активною, тобто людина має здійснити дію або низку дій з метою висловлення такої згоди. Не вважається відповідним умовам GDPR відмітка про згоду, представлена «за замовчуванням». Другим за важливістю документом є політика обробки даних. Політика має бути висловлена простими, зрозумілими для користувача словами. У доступному вигляді слід повідомити, які персональні дані збираються, з якою метою здійснюється їх обробка, кому дані передаються, як ці дані захищаються і як користувач може контролювати дані, а також строк зберігання персональних даних. GDPR допускає політику не лише у вигляді тексту, але і в іншому доступному для розуміння форматі: відео, зображення тощо. Відповідність умовам GDPR перевіряється за шляхом аудиту. Якщо ІТ-компанія пра-

¹ GDPR – новые правила обработки персональных данных в Европе для международного IT-рынка. URL: <https://habrahabr.ru/company/digitalrightscenter/blog/344064>.

цює з персональними даними користувачів з Європи, вона має відповідати умовам GDPR¹.

Викрадання персональної інформації відбувається, як правило, завдяки вірусам, шпигунським програмам, необдуманому висвітленню власної конфіденційної інформації.

Практично щодня медіа публікують повідомлення про те, як та чи інша відома особистість постраждала через зайву відвертість у соцмережах. Наприклад, під час останньої Олімпіади було зафіксовано кілька скандалів, пов'язаних з соціальними мережами. Чемпіонка Греції в потрійному стрибку Воула Папахрісту була виключена зі складу національної збірної та усунена від участі у змаганнях. Причиною цього стало її висловлювання у Twitter такого плану: «В Греції так багато африканців, що нільським комарам буде достатньо звичної їжі». Цей расистський твіт, про який дізналися представники НОК Греції, призвів до виключення спортсменки зі збірної. За кілька днів стало відомо, що з аналогічної причини постраждав гравець футбольної збірної Швейцарії Мішель Морганелла, якого виключили з команди за «дискримінацію, образу і приниження гідності футбольної команди Південної Кореї, а також південнокорейського народу». Після того як Швейцарія програла Південній Кореї з рахунком 2:1, швейцарський футболіст назвав у своєму мікроблозі жителів Південної Кореї «купою монголоїдів»².

Слід зазначити, що роботодавець має право перевіряти, чи не використовували працівники комп'ютер компанії для особистих цілей (рішення ЄСПЛ від 12 січня 2016 року). Рішення ЄСПЛ відтепер офіційно визнає право роботодавця відслідковувати активність працівників у мережі в робочий час, а також звільняти працівників не лише за такі крайні випадки, як непристойна поведінка чи висловлювання на шкоду компанії, а також за простий обмін повідомленням через мережу в робочий час з робочого комп'ютера.

Крім порушень, пов'язаних з персональними даними, соціальні мережі є місцем масового порушення прав інтелектуальної власності: авторських прав, прав на торговельні марки тощо. Найпоширенішими видами порушень в Інтернеті є: незаконне відтворення і копіювання музичних, художніх, літературних творів чи комп'ютерних програм без попереднього надання на це згоди автором чи правовласником. Серед типових порушень прав інтелектуальної власності у соціальних мережах називають: розміщення об'єктів авторського права; використання торговельної марки; розміщення

¹ GDPR в Україні: інструкція як підготуватися. URL: https://www.protocol.ua/ua/gdpr_v_ukraine_instruktsiya_kak_podgotovitsya.

² Баловсяк Н. Соціальні мережі вбивають приватність. URL: <http://tyzhden.ua/Society/70950>.

HTML-файлу, JAVA-applets, інших файлів, програм, створених іншою особою. Різноманітність порушень прав інтелектуальної власності пов'язана з великою кількістю авторських прав, які існують мережі. Зокрема, до них належать: авторські права провайдерів комп'ютерні програми і бази даних, що реалізують сам доступ до Інтернету або розміщення веб-сайтів на їх технічних платформах (серверах); авторські права виробників програмного забезпечення для цих серверів провайдерів; авторські права власників веб-сайтів на власне контент веб-сайта, його програмну частину і інші об'єкти авторського права, на ньому розміщені – статті, зображення музику, бази даних і т. д.; авторські права конкретних власників прав на об'єкти, розміщені на веб-сайтах: комп'ютерні програми, музика, статті, зображення, бази даних тощо, які дуже активно використовуються користувачами Інтернету тощо.

Відповідно до узгоджених заяв щодо ст. 1 (4) Договору ВОІВ про авторське право та ст. ст. 7, 11, 16 Договору про виконання і фондограми, процес оцифрування ототожнюється з відтворенням, а у Зеленому документі (Green Paper), прийнятому Комісією ЄС 19 липня 1995 року, що враховувався при розробленні зазначених Договорів, визначається, що термін «відтворення» слід застосовувати й у випадку застосування цифрових технологій¹.

Фотографії та інші нерухливі зображення на екрані комп'ютера (карти, схеми, діаграми тощо) є другою категорією поширених творів, які передаються за допомогою соціальних мереж. При цьому ці зображення можуть створюватися на екрані комп'ютера спеціальними програмами, призначеними для полегшення користування людиною самим комп'ютером (операційні системи) та сервісами Інтернету (програми, призначені для «пересування» Інтернетом, – браузері та інші прикладні програми) або бути розміщеними в Інтернеті і мати незалежний від комп'ютерів користувачів характер. У першому випадку зображення на екрані є частиною комп'ютерної програми, її інтерфейсом і охороняється разом із усією програмою, а в другому – зображення є цифровою фотографією і охороняється як звичайна фотографія² або є результатом переведення в цифрову форму звичайної фотографії, іншого двовимірного (кар-

¹ Авторське право і суміжні права в інформаційному просторі: «Зелений документ», прийнятий Комісією Європейського Співтовариства 19 лип. 1995 р. URL: <http://litterref.ru/qasujgmermer.html>.

² Про авторське право і суміжні права: Закон України в ред. Закону України «Про внесення змін до Закону України «Про авторське право і суміжні права» від 14 лип. 2001 р. // Голос України. 2001. 16 серп. (№ 146). Ст. 8 ч. 1 п. 10; Бернская конвенция об охране литературных и художественных произведений: Парижский акт от 24 июля 1971 г., изменённый 2 окт. 1979 г. Женева: ВОИС, 1990. Ст. 2 (1).

тини, малюнку) або тривимірного (скульптури, будівлі) твору і, при відповідності критерію оригінальності, охороняється як похідний від них твір.

Музичні твори, як з текстом, так і без, традиційно охороняються авторським правом¹. Від поняття «музичний твір» слід відрізнити поняття «фонограма». Остання також є результатом творчої праці, але вторинним, результатом фіксації у матеріальній формі виконання першого. Права на музичний твір належать його автору, на виконання – виконавцю, а на фонограму – її виробнику. Відповідно до положень Конвенції про захист інтересів виробників фонограм від незаконного відтворення їхніх фонограм 1971 року фонограмою є виключно звуковий запис звуків². У законодавстві України під фонограмою мається на увазі звукозапис на відповідному носії (магнітній стрічці чи магнітному диску, грамофонній платівці, компакт-диску тощо) виконання або будь-яких звуків, крім звуків у формі запису, що входить до аудіовізуального твору³. Відповідно до положень Інтернет-Договорів ВОІВ автори, виконавці, виробники фонограм мають виключні права дозволяти відтворення своїх творів, виконань, фонограм у цифровому середовищі, а також здійснювати доступ до своїх творів, виконань, фонограм. Під правом дозволяти відтворення твору, виконання, фонограми, відеограми, програми мовлення розуміється дозвіл на виготовлення одного або більше примірників в будь-якій матеріальній формі, а також їх запис для тимчасового чи постійного зберігання в електронній (у тому числі цифровій), оптичній або іншій формі, яку може зчитувати комп'ютер. Здійсненням доступу є доведення до загального відома через дротові та не дротові засоби зв'язку творів, виконань, фонограм таким чином, що представники публіки можуть здійснювати до них доступ з будь-якого місця і в будь-який час за їхнім власним вибором. Таким чином, правомірне використання об'єктів авторського права і суміжних прав у соціальних мережах потребує дозволу від суб'єктів відповідних прав.

Слід зазначити, що в Україні вже сформоване певне правове підґрунтя для захисту прав інтелектуальної власності в Інтернеті.

¹ Про авторське право і суміжні права: Закон України в ред. Закону України «Про внесення змін до Закону України «Про авторське право і суміжні права» від 14 лип. 2001 р. // Голос України. 2001. 16 серп. (№ 146). Ст. 8 ч. 1 п. 5; Бернська конвенція об охороне літературних і художественних произведений: Паризький акт от 24 июля 1971 г., изменённый 2 окт. 1979 г. Женева: ВОИС, 1990. Ст. 2 (1).

² Конвенция об охране интересов производителей фонограмм от незаконного воспроизводства их фонограмм: от 29 окт. 1971 г. Женева: ВОИС, 1972. Ст. 1(а).

³ Про авторське право і суміжні права: Закон України в ред. Закону України «Про внесення змін до Закону України «Про авторське право і суміжні права» від 14 лип. 2001 р. // Голос України. 2001. 16 серп. (№ 146). Ст. 1.

Правова основа захисту прав інтелектуальної власності в Україні складається із близько десяти спеціальних законів та понад два десятки багатосторонніх міжнародних договорів. Проте досі не розроблено нормативно-правового акта, за яким би передбачалися способи та методи захисту прав інтелектуальної власності у мережі Інтернет. З метою вирішення цієї проблеми було розроблено проект Концепції механізмів захисту прав на об'єкти авторського та суміжних прав в мережі Інтернет (український сегмент). Передбачалося створення дієвих механізмів захисту прав на об'єкти авторського та суміжних прав в українському сегменті мережі Інтернет відповідності із директивами ЄС та Угодою про асоціацію з ЄС з метою зниження рівня неправомірного використання об'єктів (у тому числі унеможливлення монетизації ресурсами, що незаконно використовують авторські та(або) суміжні права) з одночасним розвитком легальних платформ розповсюдження об'єктів авторського та суміжних прав.

Відповідно до п. 9 ч. 3 ст. 15 Закону України «Про авторське право і суміжні права», право на дозвіл чи заборону використання твору іншими особами шляхом подання своїх творів до загальноно відомої публіки таким чином, що її представники можуть здійснити доступ до творів з будь-якого місця і у будь-який час за їх власним вибором, є виключним правом автора (чи іншої особи, яка має авторське право). Таким чином, розміщення творів в Інтернеті є правомірним лише з дозволу автора (чи іншої особи, яка має авторське право). Таке твердження підтверджується Постановою Пленуму Верховного Суду України «Про застосування судами норм законодавства у справах про захист авторського права і суміжних прав» від 4 червня 2010 року № 5, відповідно до п. 31 якої розміщення творів у мережі Інтернет у вигляді, доступному для публічного використання, є поданням творів до загальноно відомої публіки таким чином, що її представники можуть здійснити доступ до творів з будь-якого місця і у будь-який час за їх власним вибором, тобто таке розміщення є правомірним лише з дозволу автора (чи іншої особи, яка має авторське право). Відповідно до нещодавно внесених доповнень розміщення твору в оцифрованому вигляді в Інтернеті вважається публікацією твору або його поширенням і тому потребує дозволу власника авторського права.

Формується і відповідна судово-практична. Так, з позиції Верховного Суду України публікація в соціальній мережі Facebook на сторінці, користувачем (розпорядником) якої є відповідач, відеозапису, що належить позивачеві, без його дозволу є порушенням майнових авторських прав (ВС/ВГС, справа № 918/186/17, 13.03.16). Відповідно до фабули судового акта громадська організація та то

вариство з обмеженою відповідальністю (позивачі) звернулися до господарського суду з позовом до ТОВ «Екологічні інвестиції» про стягнення 64 000 грн компенсації за порушення виключних майнових авторських прав. Позов мотивовано тим, що відповідач здійснив неправомірне використання аудіовізуального твору щодо поводження з небезпечними побутовими відходами на своїй офіційній бізнес-сторінці у соціальній мережі Фейсбук без дозволу його власників – позивачів та без сплати авторської винагороди. На підтвердження розміщення та публічного показу цього твору позивачами надано звіт про спеціальне комп'ютерно-технічне дослідження Інтернет-ресурсів, відповідно до якого відеозапис опубліковано в соціальній мережі Facebook на сторінці, користувачем (розпорядником) якої є саме відповідач – ТОВ «Екологічні інвестиції». Рішенням господарського суду, залишеним без змін постановою апеляційного господарського суду, позов задоволено; з відповідача стягнуто на користь кожного з позивачів по 32 000 грн компенсації. Верховний Суд у складі колегії суддів Касаційного господарського суду з цими рішеннями погодився, зазначивши, зокрема, наступне.

Статтею 9 Закону України «Про авторське право і суміжні права» передбачено, що частина твору, яка може використовуватись самостійно, у тому числі й оригінальна назва твору, розглядається як твір і охороняється відповідно до цього закону. Використання твору без дозволу суб'єкта авторського права є порушенням авторського права, передбаченим п. «а» ст. 50 Закону, у зв'язку з яким п. «г» ч. 2 ст. 52 цього ж Закону визначено можливість притягнення винної особи до відповідальності у вигляді сплати компенсації в розмірі від 10 до 50 000 мінімальних заробітних плат.

Отже з боку відповідача мало місце здійснення публічного показу контрафактного примірника твору, чим допущено порушення виключних майнових прав позивачів¹.

В інтересах суспільства вільне використання творів в окремих випадках визнається законодавством усіх держав світу і прямо допускається міжнародними конвенціями з авторського права. Таке використання стосується лише правомірно оприлюднених творів, не зачіпаючи особистих немайнових прав авторів, і допускається

¹ ВС/ВГС: публ. в соціальній мережі Facebook на сторінці, користувачем (розпорядником) якої є відповідач, відеозапису, що належить позивачеві, без його дозволу, є порушенням майнових авторських прав. URL: [http://protokol.com.ua/ru/vs_vgs_publikatsiya_v_sotsialniy_meregi_facebook_na_storintsi_koristuvachem_\(rozporiadnikom\)_yakoi_e_vidpovidach_vidеозапису_shcho_nalegit_pozivachevi_bez_yogo_dovolu_e_porushennyam_viklyuchnih_maynovih_avtorskih_prav_\(vs_vgs_sprava_918_186_17_13_03_16\)/?utm_source=newsletter&utm_medium=email](http://protokol.com.ua/ru/vs_vgs_publikatsiya_v_sotsialniy_meregi_facebook_na_storintsi_koristuvachem_(rozporiadnikom)_yakoi_e_vidpovidach_vidеозапису_shcho_nalegit_pozivachevi_bez_yogo_dovolu_e_porushennyam_viklyuchnih_maynovih_avtorskih_prav_(vs_vgs_sprava_918_186_17_13_03_16)/?utm_source=newsletter&utm_medium=email).

лише за умови, що цим не завдає шкоди нормальному поширенню творів і не обмежує законні інтереси авторів.

Цивільним кодексом України та Законом України «Про авторське право і суміжні права» передбачено вичерпний перелік випадків вільного використання творів: у особистих цілях; в інформаційних, наукових, навчальних або культурних цілях; використання творів шляхом репродукування, цитування; використання твору, що є суспільним надбанням; копіювання, модифікація і декомпіляція комп'ютерних програм. При цьому обов'язково мають бути зазначені ім'я автора, твір якого використовується, і джерела запозичення.

Треба зазначити, що в Інтернеті з'являються і нові об'єкти авторського права, правова природа яких досі не з'ясована. Це стосується, зокрема, основного компонента всесвітньої мережі – файлу HTML. Файл HTML втілює в собі відразу декілька об'єктів інтелектуальної власності. З точки зору внутрішньої структури – це комп'ютерна програма. Але з точки зору зовнішнього оформлення сторінка HTML може являти собою літературний твір, твір художника, дизайнера і т. п. Жоден з існуючих способів охорони не враховує повною мірою специфіку HTML. Безперечно, виходом було б розробка особливого механізму охорони HTML сторінок і внесення відповідних змін до законодавства про інтелектуальну власність. Незважаючи на відсутність спеціального регулювання, права автора сторінки HTML можуть бути в даний час захищені нормами авторського права. При бажанні, автор HTML-файлу може зареєструвати свій HTML-файл у Державному підприємстві «Українське агентство з авторських і суміжних прав» (надалі – ДП УААСП) як комп'ютерну програму, тим самим підтвердивши своє авторство і пріоритет. Існує також проблема використання так званих «Java applets» – програм, написаних мовою Ява (Джава), призначених для роботи в Інтернеті. Якщо мова HTML досить примітивна, то мову «Java» повною мірою можна назвати повноцінною мовою програмування. Особливості функціонування програм, написаних мовою «Java», полягають у тому, що програма існує весь час як некомпільований текст. При запуску через Інтернет програми, написаної мовою «Java», користувач копіює на свій комп'ютер не тільки ту програму, яку він запускає, але і компонент, необхідний для компіляції і запуску виконуваної програми безпосередньо на комп'ютері користувача. Таким чином використовується відразу декілька програм, що охороняються авторським правом.

Останні зміни до законодавства свідчать про певні зрушення у вирішенні проблем захисту прав інтелектуальної власності у мережі. Йдеться про веб-блокування, яке отримало своє законодавче закріплення у Законі України «Про державну підтримку кінемато-

графії в Україні» від 23 березня 2017 року і яким внесено відповідні зміни до низки законодавчих актів: Закону України «Про авторське право і суміжні права», Кодексу України про адміністративні правопорушення, Закону України «Про кінематографію», Цивільного процесуального кодексу, Господарського процесуального кодексу тощо.

Так, у разі порушення авторських прав у мережі можуть застосовуватися ті ж способи захисту, що застосовуються у разі їх порушення у реальному середовищі, а положення нової ст. 52-1 закріплюють особливості захисту у разі порушень авторських і (або) суміжних прав у цифровому середовищі. Можливість застосування процедури Takedown Notice в нашій країні підкріплена відповідальністю за порушення авторських прав з використанням Інтернету та за Інтернет-тролінг. Сутність процедури Takedown Notice полягає у можливості звернення особи, чиї права було порушено, до конкретного провайдера з вимогою блокування доступу до незаконно розміщеного контенту протягом 48 годин. Крім переваг зазначеної новели (визначення суб'єктів, до яких може бути звернута вимога у формі заяви про усунення порушень, чітка регламентація дій та строків розгляду заяв), у ній міститься також низка вад, що ускладнює процедуру. Так, запроваджено адвокатську монополію на здійснення такої процедури, встановлено закритий перелік об'єктів: порядок захисту авторського права і (або) суміжних прав застосовується до відносин, пов'язаних з використанням аудіовізуальних творів, музичних творів, комп'ютерних програм, відеограм, фонограм, передач (програм) організацій мовлення. За межами опиняються інші об'єкти, перелік яких закріплений у ст. 8 цього ж Закону, у разі їх неправомірного використання у мережі: фотографії, літературні твори різного жанрового спрямування, бази даних тощо. Тому процедура потребує вдосконалення.

Соціальні мережі використовуються учасниками безоплатно, однак вони все частіше стають майданчиком для поширення комерційної інформації, яка пов'язана з використанням засобів індивідуалізації учасників цивільного обігу. Відповідно до ст. 16 Закону України «Про охорону прав на знаки для товарів і послуг» власнику свідоцтва належить виключне право використовувати знак для товарів і послуг. Засоби індивідуалізації за своєю природою виконують функцію індивідуалізації, створюють асоціації у споживачів із товарами певного виробника. Результат поширення такого об'єкта у соціальній мережі має економічний ефект прямої або опосередкованої дії. Зокрема, на сторінках мережі може міститись інформація про товар із пропозицією його купити, про послуги з відповідним посиланням про те, де її можна отримати,

про рекламні акції, знижки, які спонукатимуть споживача придбати товар¹. На підтвердження того, що просування брендів за допомогою соціальних мереж справді використовується, наводить ухвала Київського апеляційного адміністративного суду від 21 лютого 2013 року у справі № 2а-13438/12/2670 про визнання протиправними та скасування податкових повідомлень-рішень за позовом дочірнього підприємства «Провід» до Державної податкової інспекції у Голосіївському районі м. Києва. Розглядаючи справу, суд дійшов висновку, що компанія позивач мала доступ (логін та пароль) до сторінок Facebook компаній Honda Ukraine та WinnerAutomotive для інформаційної підтримки сторінок, тобто наповнення зазначених сторінок короткими повідомленнями та банерами², тоді позивач надавала послуги з просування цих брендів у соціальній мережі. Отже, суд кваліфікував діяльність із поширення інформації з використанням торгової марки у соціальній мережі як таку, яка має на меті просування бренду.

Порушення прав на знак для товарів і послуг у разі реалізації товарів через сторінку у соціальній мережі з використанням знаку для товарів і послуг можливе також особою, яка не є власником прав на нього. Приклад такого порушення міститься у рішенні Солом'янського районного суду від 24 грудня 2014 року у справі № 760/26510/14-ц. Суд визнав порушенням розміщення у мережі Інтернет, у тому числі на сторінках соціальних мереж facebook; instagram; twitter; vk, ювелірних виробів для продажу. Усі товари були марковані знаком для товарів і послуг, права на які належали іншій особі – позивачу. Вирішуючи дану справу, суд виходив із того, що реалізовувати товари, марковані знаком для товарів і послуг, у тому числі і через сторінки соціальних мереж, можуть тільки ті суб'єкти, які мають такі права, підтверджені свідоцтвом³.

У науковій та фаховій літературі виділяють дві форми використання позначень торговельних марок: традиційну та нетрадиційну. До традиційних відносять рекламу, замовлення та поставки, до нетрадиційних – використання у якості найменувань своїх domen власних фірмових найменувань або торговельних марок. Метою

¹ *Огневюк Г.* Особливості використання об'єктів інтелектуальної власності в соціальних мережах. URL: <http://pravoznavec.com.ua/period/article/50173/%C3>.

² *Ухвала* Київського апеляційного адміністративного суду від 21.02.2013 р. у справі № 2а-13438/12/2670 про визнання протиправними та скасування податкових повідомлень-рішень за позовом дочірнього підприємства «Провід» до Державної податкової інспекції у Голосіївському районі м. Києва. URL: <https://scourt.info/doc/ABq7Mg>.

³ *Рішення* Солом'янського районного суду від 24.12.2014 р. у справі № 760/26510/14-ц про заборону та зобов'язання вчинення певних дій та здійснення перереєстрації доменних імен. URL: <http://www.reyestr.court.gov.ua/Review/42182855>.

цього є створення і підтримання у споживача асоціативного зв'язку між своєю діяльністю і змістом своїх сайтів¹.

Порушення прав на торговельні марки офлайн і онлайн відрізняються тим, що у порушників онлайн є більше варіантів як можна використовувати торговельну марку: фішинг, брендджекінг (brandjacking), хайджекінг (hijacking), використання торговельних марок у своїх мета тегах для залучення трафіка до свого продукту за рахунок впізнаваності чужого бренда і т. д. З'явився також термін «cybersquatting» (кіберсквотінг), що означає реєстрацію доменного імені, ідентичного або схожого до ступеня змішення з товарним знаком третьої особи з метою подальшого продажу доменного імені цій особі за суму, що значно перевищує витрати на реєстрацію. У Законі України «Про телекомунікації» від 18 листопада 2003 року домен – частина ієрархічного адресного простору мережі Інтернет, яка має унікальну назву, що її ідентифікує, обслуговується групою серверів доменних імен та централізовано адмініструється². У Законі «Про охорону прав на знаки для товарів і послуг» від 15 грудня 1993 року (із змінами і доповненнями)³ під доменним ім'ям розуміється ім'я, яке використовується для адресації комп'ютерів і ресурсів в Інтернеті. У Порядку підключення до глобальних мереж передачі даних, затвердженому Постановою Кабінету Міністрів України № 522 від 12 квітня 2002 року, доменне ім'я означає буквено-цифрове позначення (вираз), яке ідентифікує будь-який комп'ютер абонента в мережі Інтернет.

На даний час правилами ICANN (Інтернет-корпорація з призначення доменних імен та номерів) регулюється реєстрація доменних імен. Ця корпорація була створена в інтересах світової Інтернет-спільноти для покращення функціональності та стабільності Інтернету.

«Кіберсквотінг» з'явився в 1995–1996 роках у США для позначення практики реєстрації доменного імені, ідентичного або схожого до ступеня змішення з товарним знаком третьої особи з метою подальшого продажу доменного імені цій особі за суму, що значно перевищує витрати по реєстрації. Відповідно до розділу 4 (b) UDRP (Уніфікована політика розгляду суперечок про доменні іме-

¹ Бошицький Ю. Л., Рассомахіна О. А. Охорона прав на торговельні марки у мережі Інтернет: монографія. Київ: «ТОВ ВП Логос-М», 2017. С. 52, 54.

² Про телекомунікації: Закон України від 18 листоп. 2003 р. URL: <https://ur-list-ua.net/%D0%B7%D0%B0%D0%BA%D0%BE%D0%BD%D0%B8/%D0%BF%D1%80%D0%BE%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D0%BE%D0%BC%D1%83%D0%BD%D1%96%D0%BA%D0%B0%D1%86%D1%96%D1%97/%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%8F> 1.

³ Про охорону прав на знаки для товарів і послуг: Закон України від 15 груд. 1993 р. URL: <http://zakon0.rada.gov.ua/laws/show/3689-12>.

на)¹, невичерпний перелік ознак, які вказують на те, що доменне ім'я зареєстроване і використовується недобросовісно, включає обставини, що свідчать про наступне: а) доменне ім'я зареєстроване або придбане, головним чином, з метою подальшого продажу, здачі в оренду або іншого роду передачі доменного імені володарю схожого товарного знака, або його конкуренту за суму, що перевищує документально підтверджені, безпосередньо пов'язані з цим доменним ім'ям витрати; б) доменне ім'я зареєстроване з метою перешкодити використанню товарного знака його володарем в координуючому доменному імені, за умови, що особа, яка зареєструвала доменне ім'я, залучена до такого роду діяльності; в) доменне ім'я зареєстроване з метою підриву діяльності конкурента; г) використовуючи дане доменне ім'я, його власник навмисно, з метою отримання комерційної вигоди, намагається привернути користувачів Інтернету до свого сайту, створюючи за допомогою чужого товарного знака вірогідність введення публіки в оману щодо походження, джерела фінансування, приналежності або підтримки сайту, або товарів або послуг, пропонованих на сайті.

В якості основного недоліку використання UDRP називають те, що фактично існує лише 2 варіанти прохальних вимог. Арбітри з результатом розгляду заяви можуть прийняти одне з двох рішень – передати або скасувати домен. Використання адміністративної процедури не є перешкодою для звернення до суду після її закінчення, тобто, отримавши домен в своє володіння, є можливість ще окремо звернутись до суду з вимогою про відшкодування збитків.

Передача оспорюваного домену заявнику може бути здійснена при доведенні таких трьох підстав: 1) доменне ім'я є ідентичним або бентежно схожим з торговою маркою або маркою обслуговування, щодо яких у заявника є права та інтереси (англ. «your domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights»); 2) відсутність прав або законних інтересів щодо доменного імені (англ. «you have no rights or legitimate interests in respect of the domain name»); 3) доменне ім'я було зареєстровано та використовується недобросовісно («domain name has been registered and is being used in bad faith»).

Стосовно ідентичності або схожості, то, відповідно до консенсусного погляду в узагальненій практиці, наявність зареєстрованої торгової марки є достатнім для визнання доменного імені бентежно схожим. Місце, в якому торгова марка зареєстрована, дата реєстрації такої марки, вид діяльності чи продукту, який реалізовується під цією маркою, не є визначальним для знайдення схожості.

¹ UDRP. URL: <http://www.icann.org/udrp/udrp-policy-24oct99.htm>.

Даний пункт UDRP включає в себе порівняння оспорюваного доменного імені з торговою маркою заявника для визначення ступеня схожості та того, як така схожість може заплутати користувача Інтернету.

Стосовно відсутності прав або законних інтересів щодо доменного імені, у літературі зазначається, що обов'язок доказування на початку розгляду справи лежить на заявникові. Проте, як неодноразово вказувалося арбітрами, інколи такий тягар доказування просто неможливо здійснити, тому що вся необхідна інформація для такого доведення доступна лише відповідачу. Таким чином, існує практика доведення prima facie випадку. Тобто випадку, який «на перший погляд» доводить, що у відповідача немає законних інтересів у такому доменному імені. Якщо заявником буде наведено такий приклад, то тягар доказування наявності своїх інтересів у доменному імені переходить на відповідача. Обов'язком відповідача буде надати докази і довести, що законні права та інтереси на доменне ім'я існують. У випадку, якщо відповідач не надасть доказів, то як правило вважається, що другий елемент UDRP задоволено¹.

До видів кіберсквотінгу відносять: 1) typosquatting (від англ. Туро – опечатка) – в цьому випадку зловмисник сподівається, що ви помилитесь у доменному імені – тобто замість, наприклад, Instagram.com введете instafram.com; 2) кіберсквотінг спрямований на використання чужих торгових марок або їх частин. Прикладом такого типу кіберсквотінгу може бути реєстрація доменного імені iphonephones.com. або apple.net, з урахуванням того, що справжня компанія Apple здійснює діяльність з домену apple.com.

Закон про захист споживачів від кіберсквотінга (ACPA) відкрив для власників прав на товарні знаки можливість судового переслідування особи, яка реєструє, продає або використовує схоже доменне ім'я, за умови, якщо ця особа «мала недобросовісні наміри отримання прибутку з цього позначення»². ACPA містить перелік чинників, які слід враховувати суду при розгляді питання наявності в особи «недобросовісних намірів». Даний перелік, що складається з дев'яти пунктів, як і у випадку з UDRP, не є виключним³.

Проблеми з кіберсквотінгом з'явилися тому, що доменні імена за своєю природою є подібними до засобів індивідуалізації учасників цивільного обороту, товарів і послуг, тільки у віртуальному

¹ Докійчук. Доменні батли worldwide. URL: <https://www.legalitgroup.com/domain-battle>.

² Шахбазян К. Міжнародна співпраця держав у сфері правового регулювання діяльності в Інтернеті // Український часопис міжнародного права. 2003. № 1. С. 70–74.

³ Борисов В. Ю. Информационный век и защита прав на товарные знаки // Юрист. 2001. № 4. С. 40–43.

світі. Тому серед науковців точаться дискусії про те, чи є домен імя засобом індивідуалізації, а отже і об'єктом прав інтелектуальної власності чи ні. Йдеться навіть про те, щоби виділити право на доменне імя як самостійний субінститут інституту засобів індивідуалізації. Справа в тому, що система індивідуалізації віртуального мережевого світу існує нібито паралельно системі індивідуалізації реального світу, тобто системі фірмових найменувань і товарних знаків¹. Але ВОІВ не розглядає доменні імена у якості однієї з форм інтелектуальної власності. І на практиці це призводить до непорозумінь і суперечок.

Слід зазначити, що за допомогою соціальних мереж не лише порушуються права інтелектуальної власності, але і уможливорюється їх легалізація. Так, уже сьогодні діє PatentBot – бот-реєстратор торгових марок в месенджері Facebook. З його допомогою можна зареєструвати торгову марку протягом 10–15 хвилин. PatentBot вже працює в Україні і в США. У найближчих планах команди – кинути його в Європу, зокрема в країни ЄС і Китай. Власники першої в Україні торгової марки, офіційно зареєстрованої через PatentBot, на початку 2018 року отримали документи, що підтверджують успішне завершення процедури реєстрації. Торгова марка була зареєстрована за прискореною процедурою – за 4,5 місяця².

Проблеми захисту прав інтелектуальної власності у цифрову епоху пов'язані також з формуванням доказової бази у процесі судового захисту порушених прав інтелектуальної власності у мережі. Зокрема, з тим, що веб-сторінки з огляду на положення ч. 1 ст. 6 Закону України «Про електронні документи та електронний документообіг» є електронними документами. Електронні докази можуть стати ефективним інструментом захисту. І хоча судова практика у цій сфері ще не сформована, запровадження електронних доказів значно спростить процес доведення порушення прав інтелектуальної власності у суді. Новелою є також можливість огляду судом веб-сайта (сторінки) з метою встановлення і фіксування його змісту. Тому зараз не потрібно надавати докази порушення прав інтелектуальної власності на веб-сайті зі завіренням нотаріусами інших країн (зазвичай РФ), як це мало місце раніше.

Засоби доказування порушення прав інтелектуальної власності поповнилися висновком експерта, який може бути отриманий учасником справи без рішення суду. Таким чином, самостійність учасників процесу у формуванні доказової бази стала більшою, що

¹ Жилинкова І. Правовая природа доменного имени // Підприємство, право, спадарство і право. 2002. № 6. С. 30–33.

² В Україні вперше зареєстрували торгову марку через бота. URL: <https://www.pravda.com.ua/news/2018/02/13/634037>.

має позитивно вплинути на процес розгляду справ. Крім того, експертом з питань права в процесі вже є не лише суддя, а такий новий учасник судового процесу. Хто може бути таким експертом – фахівцем у певній галузі знань, має визнати, очевидно, Верховний Суд України.

Виробляється також судова практика використання засобів інформаційних технологій з метою полегшення судового процесу. Зокрема, на сьогоднішній день додаток Viber досить широко використовується і в судових рішеннях українських судів. Так, суд визнав виклик свідка через додаток Viber належним і таким, що відповідає вимогам закону¹. Крім того, при розгляді судом справи за позовом про усунення перешкод у спілкуванні з дитиною та її вихованні, визначення способу участі у вихованні дитини та спілкуванні з нею, в т. ч. мати необмежену можливість спілкуватися з дитиною засобами телефонного зв'язку за допомогою додатку Viber, суд з урахуванням всіх обставин надав позивачу необмежену можливість спілкуватися з дитиною за допомогою додатку Viber². Таких прикладів стає все більше.

Цікавим є питання визначення загальновідомих обставин, на які може спиратися суд. Так, відповідно до положень ч. 3 ст. 82 ЦПК України, обставини, визнані судом загальновідомими, не потребують доказування, зважаючи на їх очевидність (*manifestum non eget probatione* – очевидне не потребує доказування). Водночас законодавством не визначається перелік обставин, які з тих чи інших причин можуть бути визнані загальновідомими. Як наслідок, це питання вирішується судом, який розглядає справу, в кожному випадку індивідуально, про що виноситься відповідна ухвала. Хоча в законодавстві України і упускається питання віднесення деяких відомостей, які містяться на надійних чи офіційних ресурсах в Інтернеті, до загальновідомих фактів, однак на практиці дане питання знаходить своє вирішення.

Так, до подібних відомостей українська судова практика відносить інформацію, розміщену на веб-сайтах Національного банку України (наприклад, офіційний курс гривні станом на певну дату) [рішення в ЄДРСР під номером 28168539], Фонду гарантування вкладів фізичних осіб [рішення в ЄДРСР під номером 68281203], окремих банків (наприклад, наявність ліцензії, виданої Національним банком України) [рішення в ЄДРСР під номером 60193347], інших установ, підприємств, організацій (наприклад, для визначення середньої вартості майна) [рішення в ЄДРСР під номером

¹ Справа № 127/18121/16-к (Вінницький міський суд Вінницької області).

² Справа № 562/1271/17 (Здолбунівський районний суд Рівненської області).

ми 11921698 та 26358781] тощо¹. Відкритим у цьому контексті залишається питання визначення загальновідомими відомостей, що містяться у соціальних мережах.

Навіть побіжне ознайомлення зі станом справ із захистом прав інтелектуальної власності у соціальних мережах дозволяє зробити висновок про позитивні та негативні моменти і необхідність у зв'язку з цим активізації наукових досліджень у цій сфері із залучення зусиль як правників, так і фахівців з інших галузей науки.

¹ Зозуляк Н. Чи можна відомості з Інтернету вважати «загальновідомими обставинами в розумінні ЦПК України? URL: http://protokol.com.ua/ru/chi_mozna_vidomosti_z_internetu_vvagati_zagalnovidomimi_obstavinami_v_rozuminni_tspk_ukraini/?utm_source=newsletter&utm_medium=email.

ІНТЕРАКТИВНІ СОЦІАЛЬНІ МЕРЕЖІ — ПАРАДИГМА ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА ЦИФРОВОЇ ДОБИ?

Розбудова громадянського суспільства в Україні в сучасних умовах набула значення одного з реальних чинників виходу зі складної ситуації, що склалася. Вирішення цього завдання неможливе без встановлення ознак, умов виникнення та функціонування громадянського суспільства.

Громадянське суспільство — це феномен, що існує у демократичній системі (просторі демократизації). Поряд з ним у згаданому просторі існують такі сили, як: політична еліта; економічна спільнота (бізнес); сфера законодавства; державна бюрократія. Останні дві складові, засновані на загальних принципах державного устрою, складають сутність кожної сучасної демократичної системи. Усі інші — це певні організації і групи людей, котрі і надають демократичній системі конкретного характеру. При цьому, коли економічна та політична спільноти складаються переважно з фігурантів та інститутів, що мають метою отримання влади або прибутку, то громадянське суспільство — це сфера дії пересічних людей, котрі об'єднуються для виразу своїх інтересів, захисту й реалізації повсякденних потреб. Громадянське суспільство, власне, і являє собою сукупність незалежних і конституційно захищених громадських організацій, груп та асоціацій, добровільно створених пересічними громадянами у різноманітних галузях, які ґрунтуються на загальних ліберальних принципах¹.

Зазначені обставини роблять доцільним розгляд громадянського суспільства через призму лібералізму і ринку. Під таким кутом зору приваблює розуміння громадянського суспільства як сфери соціальної інтеракції між економікою і державою, що складається, у першу чергу, зі сфер найбільш близького спілкування (зокрема, сім'ї, родини), об'єднань (зокрема, добровільних), соціальних рухів

¹ Ховард Марк М. Слабость гражданского общества в посткоммунистической Европе / пер. с англ. И. Е. Кокарева. Москва: Аспект-Пресс, 2009. С. 49–57.

та різноманітних форм публічної комунікації. Сучасне громадянське суспільство створюється за допомогою певних форм самоорганізації та самооболітання. Воно інституціоналізується і генерується за посередництва законів і, особливо, суб'єктивних прагматичних соціальних диференціацій. Самотворення (незалежність) та інституціоналізація не обов'язково припускають одне одного, вони можуть існувати незалежно одне від одного, але у довгостроковій перспективі обидва ці процеси складають неодмінну невід'ємну умову відтворення громадянського суспільства¹.

Погляд з позицій лібералізму зумовлює необхідність врахування особливостей людської складової громадянського суспільства, в що звертали увагу як зарубіжні, так і вітчизняні науковці².

При цьому має йтися про принципово новий тип людини, який сформувався на підґрунті розподілу праці завдяки ринку³ (та звана – «модульна людина»). Саме ця постать дозволяє вирішити проблему створення громадянського суспільства, існування якого забезпечує унікальну можливість досягнення індивідуалізації та одночасного створення політичних асоціацій, що врівноважують державу, але не покріпачують своїх членів. Відсутність модульності виключає можливість вибору технології за принципом ефективності. Натомість кожен людський діяльність доводиться розглядати з врахуванням безлічі невідомих та вкрай складних відносин, що пов'язують її органічним, неподільним культурним цілим. Модульна людина здатна входити в ефективні інститути та асоціації, може покидати ці союзи, якщо вона не згодна з їхньою політикою. Ринкове суспільство живе в умовах не лише мінливих цін, але і союзів та думок, які змінюються. Водночас ці спеціалізовані, інструментальні зв'язки, хоча й не освячені верховним авторитетом, але є надійними та ефективними. Саме в цьому вбачається сутність громадянського суспільства: люди почали дотримуватися договору, навіть якщо він ніяк не співвідноситься з оформленою офіційно позицією у суспільстві або приналежністю до тієї чи іншої громадської групи. При цьому таке суспільство не є якоюсь м'якою, інертною масою. Навпаки, його структура рухлива і легка.

¹ Джин Л. Козн, Ендрю Арато. Гражданское общество и политическая теория / пер. с англ. / общ. ред. И. И. Мюрберг. Москва: Весь мир, 2003. С. 7.

² Сучасна правова енциклопедія / О. В. Зайчук, О. Л. Копиленко, Н. М. Оніщенко [та ін.]; за заг. ред. О. В. Зайчука; Ін-т законодавства Верхов. Ради України. Київ: Юрінком Інтер, 2009. С. 80; Біленчук П. Д., Івондецький В. Д., Сливка С. С. Філософія права: навч. посіб. / за ред. П. Д. Біленчука. Київ: Атіка, 1999. С. 57.

³ Сміт А. Добробут націй: Дослідження про природу та причини добробуту націй / пер. з англ. О. Васильєва, М. Межевської, А. Малівського; наук. ред. Є. Литвин. Київ: Port-Royal, 2001. С. 11–15.

ко піддається раціональному удосконаленню. Тому саме поява модульної людини зробила можливим виникнення громадянського суспільства¹.

Разом із тим слід враховувати ту обставину, що ринок детермінує появу модульної людини, а сукупність модульних індивідів утворює громадянське суспільство. Звідси випливає характеристика співвідношення громадянського суспільства та ринкової системи: перше, як певне соціальне відображення ринкової системи, «перекодовує» імперативи ринку на формули свободи, а формули свободи – на соціальні імперативи демократії. Хоча у ринковому суспільстві панує значно жорсткіший детермінізм і необхідність, ніж у натуральному господарстві середньовіччя, але принципова відмінність ринку полягає у тому, що він дозволяє подолати сваволлю – особисту залежність людини від людини. Людські стосунки, суспільні відносини набувають безособового характеру. Певно, їх можна тлумачити як спотворені, відчужені форми людського буття, форми, в яких речі вивищуються над людьми і урядують ними, але не можна заперечити, що це врядування має раціонально-виражений характер².

У такому контексті цікавими є зауваження О. Пономаря щодо сутності стосунків між людьми у Західному (ринковому) суспільстві. Відправним моментом його розмірковувань є теза про те, що Захід є ринком, а людина з її якостями, навичками, уміннями і здібностями – товар. І їй, природно, доводиться постійно продавати себе. Навіть працюючи на гарній роботі, люди не зупиняються у своєму розвитку, продовжують навчатися, розсилають резюме, ходять на співбесіди. І якщо, скажімо, американцям десь запропонують кращу платню, то вони приймають пропозицію, ладні переїхати в інший район і навіть інше місто. З дитинства в них заохочують індивідуалізм, пошук себе, прагнення експериментувати, визначати, в чому ти кращий, бо це може стати в нагоді в майбутньому³. Отже тут фактично йдеться про типову поведінку «модульної» людини, але з погляду ринку, котрий, у свою чергу, є корелятом громадянського суспільства.

Водночас громадянське суспільство є не простим віддзеркаленням ринку, а, швидше, його «ізоморфним відображенням». Бо, як ринок являє собою систему розподілу праці, так і громадянське

¹ Геллер Э. Условия свободы. Гражданское общество и его исторические соперники. Москва: Моск. шк. полит. исслед., 2004. С. 118–120.

² Пасько І. Т., Пасько Я. І. Громадянське суспільство і національна ідея // Україна на тлі європейських процесів. Компаративні нариси. Донецьк: ЦГО НАН України, УКЦентр, 1999. С. 46.

³ Пономарь О. Витрина. Київ: Компанія ОСМА, 2015. С. 333.

суспільство постає як система розподілу (розділення) думок, ід та об'єднань; як на ринку панують вільні «ринкові» ціни, так і громадянському суспільстві вільно висловлюються думки, утворюються громадські об'єднання, непідлеглі державі; як ринок жив в умовах мінливих цін, так і в громадянському суспільстві спонтанно народжуються і вмирають ідеї, змінюється громадська думка, переформатуються об'єднання людей. Так само, як на ринку, так визначальним важелем узгодження розмаїття попиту і пропозицій, плюралізму поглядів та позицій, приведення їх у системну єдність (рівновагу) є злагода (суспільний договір, консенсус)¹.

Тому слушною здається думка, що таїна феномена громадянського суспільства полягає у тому, що саме тут відбувається усвідомлення ринкових детермінант. Механізми цього усвідомлення можуть бути самими різноманітними, але всі вони, перш за все, формують суспільний менталітет певної поваги до громадської системи. Ця система, незалежно від того, сподобається вона іншому індивідові чи іншій суспільній групі, починає сприйматися масовою свідомістю як об'єктивний порядок речей, як соціальна необхідність, а не тільки як соціальна даність свавільного панування дужчих над слабшими.

Оскільки відображення ринкових імперативів у громадянському суспільстві здійснюється усім спектром різноманітних соціальних груп через призму їхніх потреб та інтересів, тут стає неможливою монолітність суспільної свідомості і однастайність громадської думки. Натомість природним є плюралізм ідей, думок, розмаїття політичних, культурологічних, професійних та конфесійних об'єднань, які покликані виявляти і формувати ці ідеї та думки в межах ринкової парадигми. Вже не держава нав'язує свої ідеї суспільству, а навпаки, громадянське суспільство висловлює свої вимоги державі. Табу накладається лише на політичні програми, які закликають до насильницького руйнування самого суспільного ладу. Таким чином громадянське суспільство стає сферою духовної і соціальної свободи. Можна говорити про межі цієї свободи, але не підлягає сумніву, що громадянське суспільство створює атмосферу суб'єктивного відчуття наявності свободи у кожного індивіда, відчуття можливості вибору думок, об'єднань, спілок, форм діяльності².

У вітчизняній юриспруденції називають загальні основи (принципи) функціонування громадянського суспільства: економічна свобода, поліформія власності, ринковий характер розвитку еко-

¹ Пасько І. Т., Пасько Я. І. Громадянське суспільство і національна ідея // Україна на тлі європейських процесів. Компаративні нариси. Донецьк: ЦГО НАН України, УКЦентр, 1999. С. 48.

² Там само. С. 47–48.

номіки; безумовне визнання і захист природних прав людини і громадянина; легітимність і демократичний характер влади; рівність усіх перед законом і правосуддям, надійна юридична захищеність особистості; правова держава, побудована на принципі розподілу влади і взаємодії окремих її гілок; політичний та ідеологічний плюралізм, існування легальної опозиції; свобода слова, думок, незалежність ЗМІ, невтручання держави у приватне життя громадян, їхні взаємні права, обов'язки і відповідальність; класовий мир, партнерство і національна злагода; ефективна соціальна політика, котра забезпечує належний рівень життя людей¹.

Звісно, тут може йтися про «загальні основи/принципи функціонування громадянського суспільства». Але водночас останні можуть розглядатися як передумови існування громадянського суспільства та його ознаки.

Характеризуючи громадянське суспільство, вітчизняні науковці зазначають, що, по-перше, громадянське суспільство складається з вільних суверенних індивідів, тобто громадян, що означає: 1) свободу кожного члена суспільства як людини, 2) рівність його з кожним іншим в основних правах і обов'язках, 3) самостійність кожного члена суспільства (персоніфікована власність), 4) наявність плюралізму в усіх сферах матеріального і духовного життя, 5) свобода громадян у створенні об'єднань для реалізації своїх потреб, 6) наявність засобів, які підтримують свободу, рівність, самостійність індивідів – за допомогою моральних і правових регуляторів. По-друге, громадянське суспільство – це сукупність приватних економічних соціальних і духовних відносин між громадянами, які виникають для задоволення їхніх інтересів. Особисті мотиви є пануючими². По-третє, громадянське суспільство – це діяльність по задоволенню системи різносторонніх історично обумовлених потреб та інтересів самими громадянами. (Якщо інтереси не розвинуті, громадянське суспільство може й не виникнути).

Дискусійним є питання визначення взаємин між громадянським суспільством і державою. Значення його зумовлюється тим, що розмаїття інтересів створює суперечність між ними, конфлікти, з якими громадянське суспільство самотужки впоратися не може; подолання їх можливе лише за участі держави, котру громадянське суспільство формує шляхом встановлення правових зв'язків і відносин, що створюють керуючі структури, визначають процедуру їх

¹ Кузнецова Н. С. Развитие гражданского общества и современное частное право Украины // Вибрані праці / Н. С. Кузнецова. Київ: Юрид. практика, 2014. С. 235.

² Біленчук П. Д., Івездецький В. Д., Сливка С. С. Філософія права: навч. посіб. / за ред. П. Д. Біленчука. Київ: Атіка, 1999. С. 60–63.

діяльності та співпраці. Державна влада повинна створювати оптимальні умови для нормального функціонування громадянського суспільства, охороняти його, сприяти подоланню конфліктних ситуацій. Держава, яка слугує громадянському суспільству, є правовою державою. Громадянське суспільство і правова держава – це взаємопов'язані явища. Одне без іншого існувати не може¹.

Зауважимо, що останнє твердження викликає сумніви. Перше, тому, що уявити синхронне виникнення цих феноменів досить складно: щось усе ж таки з'явилося раніше, а щось – пізніше. Візьмемо, як приклад, дві історичні форми громадянського суспільства: поліс Стародавньої Греції (станове) та новоевропейське громадянське суспільство, яке виникло у добу Відродження, Реформації і формувалося до середини ХІХ ст. (відкрите суспільство), ставши наслідком нового погляду на людину і знаменуючи початок новоевропейської цивілізації². В обох випадках – і в добу античності, і в часи Відродження громадянське суспільство виникало і функціонувало поза правовою державою (чи незалежно від неї). Крім того, і у країнах посткомуністичної Європи згадана «синхронність» практично є неможливою. Очевидно, саме формування громадянського суспільства нерідко стає тим чинником, що зумовлює руйнування авторитарної (неправової) держави і формування нової держави правової, котра надалі співіснує з громадянським суспільством, забезпечуючи функціонування останнього. Логічно припустити, що саме на такому посиленні ґрунтується поширена зокрема у соцмережах, характеристика України: «Слабка держава, але сильне громадянське суспільство».

Можна погодитися з розумінням громадянського суспільства як цілісної сфери громадського життя, що є відносно самостійною від державних інституцій і механізму державної влади. Громадянське суспільство – це унікальна система взаємодії суспільних індивідів, соціальних груп, верств і прошарків, що збалансовує вектори своїх складових, виявляючи рівнодіючу безлічі індивідуальних і групових прагнень та сподівань. Не держава має визначати спільний знаменник суспільних аспірацій, бо вона принципово не здатна виконувати ці функції, а може лише імітувати цей процес, а, навпаки, громадський лад своїм функціонуванням об'єктивно відтворює суспільні імперативи політичній системі, одночасно зумовлюючи

¹ Біленчук П. Д., Гвоздецький В. Д., Сливка С. С. Філософія права: навч. посіб. / за ред. П. Д. Біленчука. Київ: Атіка, 1999. С. 63.

² Філософія права: навч. посіб. / О. О. Бандура, С. А. Бублик, М. Л. Заінчковський [та ін.]; за заг. ред. М. В. Костицького, Б. Ф. Чміля. Київ: Юрінком Інтер 2000. С. 187–188.

становлення таких державних форм, які були б спроможні адекватно реагувати на об'єктивні інтереси суспільства¹.

Втім зазначена концепція також потребує уточнення, пов'язаного з доцільністю відходу від спрощеного бінарного бачення взаємин: громадянське суспільство – держава. Більш обґрунтованою здається трискладова модель, у якій громадянське суспільство відокремлюється як від держави, так і від економічних структур, що дозволяє йому не лише відігравати опозиційну роль в умовах авторитарних режимів, але й відроджувати свій критичний потенціал в умовах ліберальної демократії². У такому разі зникає необхідність жорсткої «прив'язки» концептів «громадянське суспільство» та «держава» одне до одного, а відтак виникає можливість враховувати останню складову як перемінну, що сприяє чи перешкоджає розвитку громадянського суспільства.

Попри зауваження щодо окремих положень концепції громадянського суспільства, з викладеного вище впливає загальний висновок, що вичерпний перелік ознак згаданого феномена скласти, практично, неможливо. Втім у цьому нема й необхідності: достатньо обмежитись констатацією того, що громадянське суспільство є результатом узгодження інтересів та відносин, котрі формуються між приватними особами і створеними ними об'єднаннями, котрі діють в умовах ринку. Враховуємо також, що таке суспільство: 1) є результатом договору (консенсусу) між приватними особами, котрі відповідають уявленням про «модульну людину»; 2) виникає та існує на підґрунті лібералізму; 3) функціонує в умовах розвиненого цивілізованого ринку; 4) дотримується формули свободи, вираженої як соціальні імперативи демократії; 5) має основою взаємин між людьми активність демократичного і ліберального характеру; 6) розглядається, передусім, як феномен поведінковий та інституціональний (на відміну від, скажімо, «соціального капіталу»)³; 7) не є об'єктом державного управління, але претендує на забезпечення державою умов його функціонування та життєдіяльності, оскільки принцип пріоритетного функціонування громадянського суспільства стосовно державної влади стає все більш характерним для генеральної динаміки розвитку сучасної світової цивілізації⁴.

¹ Пасько І. Т., Пасько Я. І. Громадянське суспільство і національна ідея // Україна на тлі європейських процесів. Компаративні нариси. Донецьк: ЦГО НАН України, УКЦентр, 1999. С. 46.

² Джин Л. Козл, Ендрю Арато. Гражданское общество и политическая теория: пер. с англ. / общ. ред. И. И. Мюрберг. Москва: Весь мир, 2003. С. 7.

³ Ховард Марк М. Слабость гражданского общества в посткоммунистической Европе / пер. с англ. И. Е. Кокарева. Москва: Аспект Пресс, 2009. С. 57.

⁴ Оніщенко Н. До питання про пошук балансу у співвідношенні громадянського суспільства та держави: теоретико-методологічні аспекти // Право України.

У свою чергу, поміж названих ознак вирішальними є наявність ліберального підґрунтя та цивілізованого ринку. При цьому названі ознаки громадянського суспільства одночасно є також умовами його буття.

Розуміючи громадянське суспільство як систему взаємодії суспільних індивідів, соціальних груп, верств і прошарків, що збалансовує вектори своїх складових, виявляючи рівнодіючу безлічі індивідуальних і групових прагнень та сподівань, можна дійти висновку, що воно не може існувати без приватного права (деякими правознавцями формування цивілізованого громадянського суспільства розглядається як одна з тенденцій розвитку приватного права)¹. Приватне право є основою правового середовища громадянського суспільства, а також елементом громадянського суспільства, органічно властивим йому, що слугує регулятором внутрішніх відносин у ньому і засобом забезпечення інтересів його членів суспільства, що є суспільством. Крім того, воно є методологічною основою діяльності правової держави у галузі забезпечення прав людини (членів громадянського суспільства) та створення умов для функціонування громадянського суспільства.

Разом із тим громадянське суспільство в умовах цифрової доби має особливості, зумовлені тією важливою роллю, яку відіграють у ньому інформаційно-комунікаційні технології, котрі дозволяють збирати, обробляти, отримувати та передавати інформацію на локальному, загальнодержавному та міжнародному рівнях.

У контексті проблематики нашого дослідження варто згадати алгоритм розвитку Інтернету – всесвітньої телекомунікаційної мережі, яка основною метою має поширення інформації серед користувачів, обмін інформацією тощо. Він є унікальним засобом комунікації, що не знає часових і просторових меж, оскільки обмін інформацією відбувається блискавично і незалежно від відстані кордонів.

Протягом свого розвитку Всесвітня мережа пройшла розвиток від системи Web 1.0, функціональність якої була обмежена можливостями читати інформацію і купувати речі; через Web 2.0, котра дозволяла здійснювати в Інтернеті різноманітні дії; до соціальної мережі на основі нової платформи Facebook, завдяки якій люди отримують

2014. № 4. С. 55. Огляд та ґрунтовний перелік ознак громадянського суспільства див.: Колодій А. Громадянське суспільство: ознаки, структурні елементи, співвідношення із державою // Право України. 2014. № 4. С. 9–12.

¹ Баринов Н. А. Частное право и гражданское общество: проблемы соотношения и развития // Гражданское общество и развитие гражданского права: сб. ст. к юбилею д-ра юрид. наук, проф. Наталии Семеновны Кузнецовой / отв. ред. Р. А. Майданик и Е. В. Кохановская. Киев: Юрид. практика, 2014. С. 100.

римали можливість обговорювати і ділитися інформацією про дії¹. Водночас завдяки Інтернету відбувається соціальна інтеграція як процес утворення взаємозв'язків між індивідами, групами, яскравим прикладом чого є створення соціальних мереж, які набувають все більшого значення і охоплюють усе ширше коло учасників.

Соціальні мережі (social network) – це соціальні структури, що утворюються окремими особами або організаціями з метою обміну інформацією, спілкування, комунікацій. Таким чином, стрімкий розвиток сучасних інформаційно-комунікаційних технологій створює таку ознаку диференціації суспільства, як ознака комунікативна. За допомогою комунікації суспільство може визначити себе, інформувати себе про власні інтелектуальні комунікації, піддавати інформацію сумніву, відхиляти її, нормувати комунікації як допустимі чи неприпустимі тощо².

Наразі найбільш поширеними соціальними мережами є Facebook (заснована у 2004 році. Станом на липень 2016 року мала 1,7 млрд користувачів. У липні 2017 року кількість акаунтів в українському Facebook перевищила 10 млн. Займає перше місце серед аналогічних сервісів за кількістю часу, що витрачають на неї користувачі. Користувачем може бути кожна людина старша 13 років, яка має електронну пошту), Instagram (має метою забезпечити користувачам можливість робити фотографії, обмінюватися фотографіями, поширювати фото через свій сервіс та інші соціальні мережі. У квітні 2012 року Instagram був придбаний компанією Facebook за 1 млрд доларів), YouTube (відеогостінг, що надає користувачам послуги розміщення відеоматеріалів, їхнього перегляду і коментування. Заснований у 2005 році. Поступається за популярністю лише соціальній мережі Facebook. Був придбаний Google Inc. у 2006 році за 1,65 млрд доларів. Станом на серпень 2017 року є другим за відвідуваністю сайтом в Інтернеті); Google+ (існує з 2011 року. За перші три тижні набрала 20 млн користувачів. Примітною є не зовсім типова для соціальних мереж політика невизнання анонімних акаунтів, яку мотивує тим, що повідомлення свого справжнього імені у мережі необхідне для того, аби інші користувачі могли знаходити своїх друзів і знайомих)³.

Підстави та чинники створення соціальних мереж є різноманітними, вони об'єднують величезну кількість людей за інтересами,

¹ Шмідт Е., Розенберг Дж. Як працює Google / пер. з англ. Ю. Гордієнка. Київ: Вид. група КМ-БУКС, 2016. С. 274–275.

² Андрєєв Д. Засоби масової інформації як механізм інтелектуальної комунікації в процесі розвитку інформаційного суспільства // Теорія і практика інтелектуальної власності. 2015. № 5. С. 56.

³ Тут і далі, якщо не застережене інше, відомості про соціальні мережі з Вікіпедії.

соціальним становищем, професійною, гендерною, віковою ознакою, навіть за національним принципом (Druzi.org.ua, Ukrainc.org — неполітична благо-соціальна мережа «Ми-Українці!»). Останні з'явилися після подій Євромайдану 2013–2014 років, після анексії Криму і розв'язання Росією війни на Донбасі, внаслідок чого відбувся відтік україномовних користувачів з російськомовних соціальних мереж. На врахуванні професійних уподобань ґрунтується соціальна мережа Twitter, котра була створена як мережа мікроблогів і дає змогу користувачам надсилати короткі текстові повідомлення, використовуючи SMS, служби миттєвих повідомлень і сторінні програми-клієнти.

Важливою ознакою соціальних мереж є те, що на відміну від Інтернет-спільнот, де користувач не знаходиться в центрі системи; його стосунки з іншими учасниками спільноти знаходяться на другому плані, бо основна увага Інтернет-спільноти зосереджена на внеску користувача в досягнення спільних цілей, цінностей та спілкуванні, у соціальних мережах користувач знаходиться в центрі системи та може належати до декількох груп водночас¹.

Можливості, які надають соціальні мережі, створюють підґрунтя формування так званого «інтерактивного громадянського суспільства», котре можна визначити як систему взаємодії вільних громадян та їх добровільних об'єднань за допомогою Всесвітньої мережі (Інтернет), де інформація є головним чинником соціалізації з метою формування механізму реалізації та захисту основних прав і свобод людини, задоволення індивідуальних та групових прагнень і сподівань, впливу на владні державні інституції, напрямок державного розвитку в цілому.

Втім вираз «інтерактивне громадянське суспільство» наразі є не доконаним терміно-поняттям, а, швидше, концептом, що перебуває у процесі формування. Тому, мабуть, поки що доцільно вести мову про «громадянське суспільство цифрової доби», маючи на увазі, що зміст цього поняття залежить від ступеня долучення ІТ до функціонування спільноти, котра є людським субстратом громадянського суспільства.

Врахування згаданого ступеня долучення ІТ до функціонування громадянського суспільства дозволяє розрізняти кілька варіантів (рівнів).

Найпростішим варіантом (першим рівнем) є використання ІТ як засобу спілкування членів «звичайного» громадянського суспільства (домовленості про зустрічі, акції, громадські проекти тощо) повідомлення про заходи, події, що відбулися, тощо).

¹ Соціальна мережа (Інтернет). URL: [https://uk.wikipedia.org/wiki/Соціальна_мережа_\(Інтернет\)](https://uk.wikipedia.org/wiki/Соціальна_мережа_(Інтернет)).

Більш складним варіантом (другим рівнем) є підвищення (забезпечення) ефективності діяльності громадянського суспільства за рахунок використання можливостей інформаційних технологій. Прикладом такого способу діяльності громадянського суспільства може бути розширення соціальною мережею Facebook можливостей сервісу Safety Check, котрий автоматично активується у разі виникнення кризових ситуацій. У ньому стає доступна опція Community Help (допомога спільноти), яка сприятиме організації взаємодопомоги під час стихійного лиха.

Кожен користувач Facebook, який опинився у районі, де автоматично активується опція Safety Check (запускається у випадку, коли з одного місця надходить багато повідомлень про якесь лихо або жакливу подію), зможе запропонувати оточуючим замовити у них їжу, напої, дах над головою та можливість скористатися транспортним засобом. Для зручності відповідна сторінка Facebook містить категорії допомоги, а також її види (розділи «їжа для тварин», «дитячі речі», «одяг» тощо). Крім того, Community Help допоможе у пошуку людей у зоні лиха та забезпечить зв'язок з ними.

Спочатку Community Help буде працювати у тестовому режимі лише в умовах природних катастроф і лише у США, Канаді, Австралії, Новій Зеландії, Індії та Саудівській Аравії. Після тестового періоду та усунення недоліків система буде доступна для усіх країн та для використання в усіх кризових ситуаціях¹.

Найближчим до «повноцінного» концепту «інтерактивного громадянського суспільства» у розумінні, про яке йшлося вище (третім рівнем), є тип соціальних мереж, котрі мають цілі, властиві громадянському суспільству, зокрема, вплив на соціальні зв'язки, який справляють шляхом оприлюднення інформації та здійснення на такій основі діяльності вільно сформованою спільнотою «модульних людей».

Прикладом такої форми діяльності є соціальна мережа Авааз («голос» на фарсі)², котру іноді іменують «глобальною громадською організацією»³. Заснована у 2007 році 34-річним канадцем Рікеном Пателем для просування дій активістів з таких питань, як права людини, кліматичні зміни, збереження довкілля, релігійні конфлікти тощо. Активно займається збором підписів і розсиланням петицій по всьому світу. Вже у 2011 році Авааз називали «соціальною мережею номер один у світі» – якщо й не за кількістю користувачів,

¹ Facebook вводить функцію взаємодопомоги во время стихийных бедствий. URL: <https://ru.slovoidilo.ua/2017/02/09/novost/obshchestvo/facebook-vvodit-funkciyu-vzaimopomoshhi-vo-vremya-stixijnyx-bedstvij>.

² Avaaz. URL: <https://uk.wikipedia.org/wiki/Avaaz>.

³ Там само.

то за впливом¹. Найбільшою популярністю користується в Бразилії, США, Франції, Німеччині та Великобританії.

Ідеологію Авааз можна охарактеризувати як «практичний ідеалізм». У 2011 році Рікен Пателъ зазначив, що у Авааз «немає ідеології як такої. Наша місія полягає в тому, щоб подолати розрив між світом, в якому ми живемо, і світом, в якому хотіла б жити більшість людей. Ідеалісти всіх країн, єднайтеся!»

Рікен Пателъ об'єднав зусилля 10 організацій, а також окремих людей, які склали команду, що заснувала в 2007 році Авааз. Як стверджує The Guardian, «співтовариство Авааз не приймає ніяких внесків від фондів і корпорацій з 2009 року, а також внесків розміром більше 5000 доларів. Замість цього Авааз повністю складається на внески членів спільноти, які вже пожертвували понад 20 мільйонів доларів».

Глобальні компанії організовує команда фахівців, розташована більш ніж в 30 країнах світу, яка взаємодіє з членами спільноти за допомогою електронної пошти, використовуючи при цьому громадські онлайн-петиції, відеоролики та звернення до національних керівників і міжнародних організацій по електронній пошті. У деяких випадках Авааз також використовує рекламу і платні консалтингові консультації юристів для оптимізації проведення кампаній, а також використовує такі прийоми, як «сидячі демонстрації протесту», мітинги, дзвінки і телефонні переговори, що привертають увагу до публічних акцій.

Важливою особливістю діяльності Авааз, котра, як на нашу думку, підтверджує характеристику цієї соціальної мережі як інтерактивного громадянського суспільства, є те, що пропозиції в кампаніях також можуть вносити члени спільноти, яких консультує команда фахівців Авааз, що займаються відповідними питаннями. Якщо пропозиція розцінюється як потенційно перспективна, то певному числу випадково вибраних членів Авааз розсилається опитування по електронній пошті. Якщо на цей пробний лист відповідало достатня кількість членів, то Авааз розсилає його усім своїм прихильникам в регіоні, країні або світі (залежно від масштабу розглянутої проблеми).

У 2010 році автор статті в The Economist висловив припущення, що «методи, які використовуються Авааз, щоб об'єднати складні соціальні цілі різних груп людей, можуть бути дуже цінними для світу, в якому кампанії, наприклад, за расовими або класовими проблемами, все ще можуть роз'єднувати, а не примиряти людей».

¹ Наталі Шилд. Соціальна сеть номер один в мире — это Avaaz! URL: <http://freejojo.com/society/society-world/683-socialnaya-set-nomer-odin-v-mire-eto-avaaz.html>.

Удосконаленням форм діяльності інтерактивного громадянського суспільства можна вважати, на наш погляд, запуск у 2012 році спільнотою Авааз онлайн-платформи, що дозволяє кожному з мільйонів її членів швидко створювати власні петиції. Протягом кількох місяців після цього запрацював сайт громадських петицій, на якому за перші місяці роботи більше 8000 членів організували кампанії з найрізноманітніших питань: від захисту новозеландських дельфінів Мауї, що знаходяться на межі зникнення, до допомоги з повернення на батьківщину 100 індійських громадян, які з примусу працювали на будівельну компанію в Бахрейні. Зокрема, в Україні петиція, створена членом спільноти проти видобутку в Україні сланцевого газу із застосуванням екологічно небезпечної технології фрекінгу, отримала значну підтримку і була розширена до національного рівня¹.

Про ефективність діяльності цієї соціальної мережі свідчать результати її діяльності, про які регулярно повідомляється в Інтернеті.

Так, лише за один тиждень березня 2018 року: після того, як зроблені Авааз знімки з космосу підтвердили значний масштаб збезлісення в Колумбії, президент облетів проблемні ділянки і з'явилася надія на перемогу в цій кампанії; йшла боротьба за створення найбільшого морського заповідника в Атлантиці. Після ознайомлення з фінальною версією чернетки проекту міністр з охорони навколишнього середовища Бразилії попросив допомоги, щоб узяти гору з цього питання над іншими членами кабінету і президентом; чинилася активна протидія перемозі на виборах в Італії очолюваної фашистами коаліції. Команда Авааз зверталася до мільйонів виборців по електронній пошті, в Фейсбуці, в ЗМІ з проханням об'єднатися навколо розрізненої опозиції і проголосувати за кандидата, який має найбільше шансів перемогти ультраправих. Внаслідок цього коаліція ультраправих не отримала більшості; тривала протидія об'єднанню Монсанта та Байер у мегакорпорацію, і Авааз є єдиною організацією громадянського суспільства, яка отримала офіційний статус третьої особи в процесі ЄС по цій угоді. Попри не надто високі шанси на перемогу, боротьба триває; активно підтримувалася вимога посилення контролю над зброєю в США. Коли сталася стрілянина в школі, команда Авааз мобілізувалася протягом доби, щоб привернути увагу громадськості до найголовнішого одержувача коштів від збройових лобістів сенатора Марко Рубіо; африканські лідери підпишуть петицію Авааз за заборону торгівлі слоновою кісткою. Це дуже важливо, оскільки в ЄС

¹ *Avaaz*. URL: <https://uk.wikipedia.org/wiki/Avaaz>.

заявляли, що африканські лідери не хочуть таких заходів від Єросоюзу. Це величезний крок вперед у боротьбі за порятунок єнів від вимирання; нарощувалися зусилля у боротьбі за безстрокову заборону на пестициди, що вбивають бджіл в Європі, велися переговори з політиками ЄС і вченими з Німеччини, Бельгії та Ірландії, щоб організувати брифінг для осіб, відповідальних за прийняття рішень, а за минулі вихідні члени Авааз з Голландії чинили тиск на уряд, щоб він погодився з вимогами цієї кампанії. Тривали виступи на захист палестинських дітей, які знаходяться в ув'язненні після маршу з їх сім'ями; в результаті профінансованої Авааз таємних розслідувань було закрито дві бійні. Навіть Макарнах подав до суду на одну бійню після публікації відео, на якому були показані страждання корів; здійснювався тиск на уряди для ефективної боротьби з дезінформацією в ЗМІ. Була проведена зустріч з представниками урядів Франції та Бразилії, які готують законопроекти по боротьбі з масштабною загрозою демократії за допомогою неправдивих новин і дезінформуючих кампаній, що хвилює 85 % членів Авааз. Активісти Авааз поділилися результатами опитування учасників руху щодо можливих рішень проблеми і розіслали доповідні записки з найбільш популярними серед спільноти варіантами, які дозволяють вирішити проблему і уникнути навантаження на владу; був підготовлений і розісланий лист з порадами щодо подальших кроків 530 000 членів Авааз, які дали обіцянку щодо скорочення споживання м'яса. 94 % дотримуються даної обіцянки. Усе це, і не лише це, було зроблено за один досить звичайний робочий тиждень¹.

З погляду проблематики нашого дослідження тут важливим є те, що функціонування складної системи інтерактивного громадянського суспільства потребує відповідного законодавчого забезпечення.

Власне, усі відносини інтерактивного громадянського суспільства є правовим полем «ІТ-права» у широкому сенсі, включаючи як приватноправові, так і публічно-правові його складові.

Якщо ж беремо «ІТ-право» у вузькому сенсі, тобто регулятивні норми (переважно цивільно-правові), що забезпечують функціонування ІТ-відносин у цивільному (торговому) обігу, то тут, фактично, йдеться про цивільно-правове регулювання на засадах цивільного права з усіма завданнями, що постають перед цією галузю у громадянському суспільстві.

Разом із тим на нього покладаються додаткові завдання в порядкування відносин за участю модульної людини – забезпечення

¹ Семь дней из жизни Авааз. URL: <https://mail.google.com/mail/u/0/?pc=topn&about-ru#inbox/162036340871b3b4>.

можливості створення громадських організацій, їхньої діяльності та часті в них особи; гарантування здійснення права громадської активності тощо.

Що стосується «ІТ-права» у спеціальному сенсі, яким можна вважати сукупність норм та правил, що стосуються суто сфери ІТ-відносин, то у контексті буття громадянського суспільства воно виконує «службову» роль, впорядковуючи інформаційно-комунікаційні відносини; відносини створення та використання програмного забезпечення; інтернет-відносини тощо.

ПРАВОВЕ РЕГУЛЮВАННЯ ВІДНОСИН КОРИСТУВАННЯ СОЦІАЛЬНИМИ МЕРЕЖАМИ

Соціальні мережі вже не нове явище в сучасному світі. Відповідно до дослідження GlobalWebIndex у січні 2018 року соціальні мережами користується приблизно 3,196 млрд осіб, це складно близько 42 % від всього населення Землі (7,593 млрд осіб)¹.

Згідно з інформацією, наданою медійною платформою Українформ на травень 2018 року в Україні найпопулярнішою соціальною мережею є Facebook². А відповідно до даних сайту gs.statcounter.com близько 87 %³ користувачів соціальних мереж також використовують Facebook. Серед лідерів соціальних мереж слід назвати Instagram, Twitter, LinkedIn, Snapchat.

При реєстрації у будь-якій соціальній мережі в користувачів запитують згоду на умови використання конкретної соціальної мережі. Розглянемо детальніше такі умови на прикладі найпопулярнішої у світі соціальної мережі Facebook, кількість користувачів якої сягнула за відмітку в 2 млрд осіб⁴ у всьому світі.

Перш ніж зареєструватись у соціальній мережі, Facebook пропонує ознайомитись з умовами і правилами користування даною соціальною мережею. Перший розділ має назву «Умови надання послуг». У даному розділі визначено мету, з якою створено Facebook — надати користувачам можливість будувати спільноту, зблизити людей із різних куточків світу, а також перелік послуг, які надаються соціальною мережею. До них слід віднести:

- надання персоналізованого досвіду (з цією метою Facebook використовує інформацію стосовно переліку друзів, сторінок, які ви цікавитесь користувачі, події, які вони відвідують і т. д.);

¹ У 2018-му люди проведуть в мережі мільярд років, дослідження // Еспресо. 2018. URL: https://espresso.tv/news/2018/01/30/v_2018_lyudy_provedut_v_merezhi_milyard_rokiv_statystyka.

² ТОП-25 найпопулярніших в Україні сайтів // Українформ. 2018. URL: <https://www.ukrinform.ua/rubric-society/2455506-top25-najpopularnisih-v-ukraini-sajtiv.html>.

³ Найпопулярніші соціальні мережі в країнах СНД і світі // Marketer. 2017. URL: <https://marketer.ua/ua/top-social-media-2017>.

⁴ Facebook // Вікіпедія. 2018. URL: <https://uk.wikipedia.org/wiki/Facebook>.

– зв'язок із людьми та організаціями, які цікавлять користувача (для цього Facebook збирає інформацію щодо людей, організацій, подій, які цікавлять користувачів, та на основі зібраних даних надає рекомендації стосовно приєднання до конкретних груп, відвідування подій, додавання в розділ «Друзі» інших користувачів, які були підібрані на основі отриманої персоналізованої інформації);

– можливість самовиражатись та спілкуватись з іншими про те, що має значення для осіб, які зареєструвались в даній соціальній мережі;

– допомагає знайти контент, продукти та послуги, що можуть зацікавити користувачів;

– бореться з недобросовісною поведінкою, захищає та підтримує спільноту Facebook;

– використовує і розробляє передові технології для надання безпечних і багатофункціональних послуг для всіх споживачів (наприклад, створює Інтернет-мережі та комунікаційні технології для підключення до Інтернету більшої кількості людей);

– досліджує шляхи поліпшення послуг та сервісів Facebook;

– надає послідовний і бездоганний досвід використання продуктів компанії Facebook;

– надання глобального доступу до послуг Facebook¹.

Далі йде інформація стосовно політики використання персональних даних користувача та вибору рівня конфіденційності. Facebook пропонує ознайомитись з «Політикою використання персональних даних», з якою особа повинна обов'язково погодитись для отримання можливості користування послугами даної соціальної мережі.

Персональна інформація, яку збирає Facebook, ділиться на три частини: інформацію, яку надають користувачі та їх дії в соціальній мережі; інформація про пристрій; інформація від партнерів.

До першої частини входить інформація про контент, яку надає особа, наприклад: інформація, яка надається при створенні акаунту, повідомлення, спілкування з іншими користувачами Facebook, інформація про місцезнаходження, місце, де було зроблене фото, час коли воно було зроблено, доступ до камери пристрою, через який здійснюється користування даною соціальною мережею.

Досить цікавим є застереження про расове або етнічне походження, релігійну приналежність. При наданні такого роду інформації вона може бути об'єктом спеціального захисту відповідно до законодавства країни користувача.

¹ Terms of Service. URL: <https://en-gb.facebook.com/legal/terms>.

Погоджуючись з політикою використання персональних даних, особа погоджується, що Facebook збирає інформацію про людські сторінки, акаунти, хештеги, групи, з якими взаємодіє користувач, і спосіб, у який він це робить. Facebook збирає інформацію про контакти, які особа завантажує, синхронізує або імпортує з пристроєм (наприклад, адресну книгу або історію журналу викликів SMS).

Погоджуючись з «Політикою використання персональних даних», особа надає дозвіл на фіксування Facebook інформації про те, яким чином особа використовує продукти даної компанії, дані про використання, час активності в соціальній мережі. При здійсненні фінансових транзакцій Facebook зберігає платіжну інформацію, таку як номер кредитної або дебетової картки користувача, інформацію дані про картку, інформацію щодо автентифікації, а також платіжні реквізити, дані про відвантаження.

Дії та інформація, надані іншими користувачами стосовно конкретної особи, також є предметом збирання та аналізу соціальних мережі Facebook.

Наступним блоком, на який потрібно надавати свою згоду користувачу при реєстрації у Facebook, — інформація про пристрій. Facebook збирає інформацію про телефони, комп'ютери, телевізори та інші пристрої, які мають доступ до Інтернету і які користувач використовує для входу у соціальну мережу. Така інформація збирається та використовується, зокрема, для більш ефективного показу рекламної продукції та для фіксування реакції користувача на ті або інші оголошення. Інформація, яка збирається щодо пристрою, через який здійснюється вхід до мережі Facebook:

- операційна система, версії апаратних засобів і програмного забезпечення, рівень заряду акумулятора, потужність сигналу, місце, де знаходиться пристрій, тип браузера, додатки та імена файлів і їх типи, а також плагіни;

- рухи комп'ютерної мишки;

- унікальні ідентифікатори (наприклад, ігор, додатків), акаунти, які використовує особа, сімейні ідентифікатори особи, пов'язані з пристроєм або акаунтом;

- сигнали пристрою: сигнали Bluetooth, інформація про близькість до точки доступу Wi-Fi, маяки та вежі мобільного зв'язку;

- інформація, отримана через доступ до GPS, камери та фотоприладів при наданні користувачем дозволу на такий доступ;

- найменування оператора мобільного зв'язку або Інтернет-провайдерів, мова, часовий пояс, номер мобільного телефону, IP-адреса, швидкість з'єднання та, в деяких випадках, інформація про інші пристрої поблизу або у вашій мережі;

– дані файлів cookie, які зберігаються на пристрої користувача соціальної мережею, включаючи ідентифікатори файлів cookie та налаштування¹.

Останнім блоком у політиці використання персональних даних, на який дає згоду користувач, є інформація від партнерів. Рекламодавці, розробники додатків та видавці можуть надсилати інформацію соціальній мережі Facebook. Такі партнери надають інформацію про діяльність поза мережею Facebook, наприклад, інформацію про пристрій, яким користується особа, веб-сайти, які вона відвідує, покупки, які здійснює, рекламу, яку переглядає особа незалежно від того, чи є у особи обліковий запис Facebook або чи увійшла вона в акаунт Facebook. Таким чином, Facebook отримує дані про активність не тільки всередині соціальної мережі, а і поза нею.

Крім того, такі партнери отримують й інформацію про користувача, коли ви відвідуєте або використовуєте їхні послуги навіть через третіх сторін, з якими вони співпрацюють. Facebook вимагає від кожного такого партнера наявності законного права збирати, використовувати та передавати ваші дані, щоб надавати ці дані їм.

Третій пункт «Умов надання послуг» визначає обов'язки користувачів перед Facebook:

- використовувати те ім'я, яким особа користується в повсякденному житті;
- особа повинна надавати достовірну інформацію про себе;
- створювати тільки один акаунт і користуватись життєписом в особистих цілях;
- не розкривати пароль, не надавати доступ до акаунту іншим особам або передавати акаунт (без згоди Facebook).

Не можуть користуватись Facebook особи, які не досягли 13 років (або іншого мінімального віку, з якого особа має право користуватись продуктами Facebook у країні реєстрації). Також не можуть користуватись Facebook особи, які вчинили протиправні дії сексуального характеру, та особи, акаунт яких був вимкнений через порушення умов та правил користування Facebook. Особи не можуть користуватись Facebook, якщо за чинним законодавством країни таким особам заборонено отримувати продукти, послуги та програмне забезпечення Facebook.

Використовуючи Facebook, особа не може ділитись нічим, що порушує умови використання Facebook, що є незаконним, оманливим, дискримінаційним або шахрайськими, а також розповсюджувати дані, що порушують права інших користувачів.

¹ Data Policy. URL: <https://en-gb.facebook.com/about/privacy/update>.

Користувачам Facebook забороняється завантажувати віруси, шкідливий код або вчиняти щось, що може спричинити відключення, перевантаження або погіршення належної роботи або зовнішнього вигляду продуктів Facebook. Користувачі Facebook не можуть отримувати доступ до даних стосовно продуктів Facebook, збирати такі дані за допомогою автоматичних засобів (без наявності попередньо оформленого належного дозволу Facebook) або намагатися отримати доступ до даних, стосовно яких у користувача немає дозволу на доступ.

Контент, який порушує вище перелічені вимоги, може бути видалений командою Facebook, більш того Facebook залишає за собою право вчиняти певні дії, якщо вони є доцільними, стосовно акаунту такого користувача, який порушив вищезгадані умови. Якщо особа неодноразово порушує права інтелектуальної власності інших користувачів, то Facebook може відключити такий акаунт.

Для того щоб Facebook мав змогу надавати свої послуги безплатно середньо споживачам, такий одержувач послуг повинен надати Facebook наступні дозволи:

- дозвіл на використання контенту, який створив користувач, яким він ділиться (тобто потрібно розуміти, що коли особа поширює, публікує або завантажує інформацією, яка підпадає під охорону правом інтелектуальної власності (наприклад: фото або відео), використовуючи при цьому продукти Facebook, то така особа надає Facebook невиключну, з правом передачі та субліцензування, без виплати роялті, глобальну ліцензію на розміщення, використання, розповсюдження, переробку, виконання, відтворення, публічне виконання або показ, переклад і використання для створення подібних творів вашого контенту. Більш того, слід пам'ятати, що користувач може припинити таке ліцензування в будь-який час шляхом видалення такого контенту або акаунту);

- дозвіл на використання імені користувача, фотографію профілю та інформації про дії такого користувача відносно реклами та спонсорського контенту;

- дозвіл на оновлення програмного забезпечення, яке використовує або завантажує користувач.

Погоджуючись із «Умовами надання послуг», особа також погоджується з тим, що при використанні контенту, який підпадає під захист права інтелектуальної власності, яким володіє Facebook та всі його продукти, Facebook зберігає всі права на такий контент. Особа може використовувати такі об'єкти авторського права (знаки для товарів і послуг (або будь-які аналогічні знаки) тільки таким способом, передбачений «Правилами використання бренду Facebook».

або при наявності у такої особи попереднього письмового дозволу від компанії Facebook.

Додаткові положення до «Умов надання послуг» містять інформацію стосовно оновлення продукції Facebook. Також в даному блоці прописана політика Facebook стосовно призупинення або припинення дії акаунту (при виявленні Facebook порушення з боку користувача Facebook має право призупинити доступ до акаунту або заблокувати доступ до нього (за власною ініціативою або на вимогу законодавства).

Facebook не контролює та не скеровує дії та висловлювання користувачів Facebook, не несе відповідальності за дії та поведінку користувачів онлайн чи оффлайн, за будь-який контент, який вони поширюють (образливий, неналежний, нецензурний, незаконний та інший неприйнятний контент).

Варто звернути увагу на порядок вирішення спорів з Facebook та на законодавство, яке буде застосовуватись при вирішенні такого спору. При вирішенні спору, який виник з «Умов надання послуг» Facebook або при використанні іншої продукції Facebook, клієнт Facebook має можливість звертатись до будь-якого компетентного суду країни свого проживання. В усіх інших випадках особа погоджується на те, що претензія повинна бути вирішена виключно в Окружному суді Північного округу Каліфорнії (США) або суді штату, розташованому в окрузі Сан-Матео.

Важливо запам'ятати, що користувач без згоди компанії Facebook не може передавати права та обов'язки, зазначені в «Умовах надання послуг».

Певною новелою у даних «Умовах надання послуг» є поява припису, в якому зазначено, що користувач може призначити особу (котра буде називатись спадкоємцем), яка зможе мати можливість керувати акаунтом такого користувача у разі його смерті, після увічнення акаунту. Тільки така особа або особа, яку користувач зазначив у дійсному заповіті або документі, що до нього прирівнюється і закріплює чітку згоду на розкриття контенту після смерті або визнання такої особи недієздатною, зможе запросити розкриття акаунту після увічнення даного акаунту.

В «Умовах надання послуг» також зазначено, що Facebook може сам змінити ім'я користувача при наявності скарги стосовно імені користувача та з'ясування інформації про те, що особа не користується вказаним ім'ям в реальному житті.

На сьогодні, на жаль, в Україні не закріплено на нормативному рівні регулювання відносин, які виникають в соціальних мережах, оскільки законодавча база України значною мірою не встигає за стрімкою зміною реальності.

Найбільш розвинутою у цьому плані вбачається законодавча база Сполучених Штатів Америки. Тому пропонується ознайомитись з аналізом нормативно-правової бази, яка наразі є чинною кожному штаті окремо.

Так, двома найбільш важливими законодавчими положеннями на які слід звернути увагу при обговоренні юридичних зобов'язань на сайтах соціальних мереж, є розділ 512 Закону «Про захист авторських прав у цифрову епоху» та розділ 230 Закону «Про прихильність до комунікації»¹.

Розділ 512 знімає відповідальність за порушення авторських прав із веб-сайтів, які дозволяють користувачам публікувати контент, якщо на сайті є механізм, за допомогою якого власник авторських прав може вимагати видалення контенту, що порушує права. Сайт також не повинен отримувати фінансову вигоду, безпосередньо пов'язану з протиправною діяльністю.

Це створює цікаву проблему для більшості сайтів, які дозволяють користувачам публікувати музику, фотографії або відео. Наприклад, кілька власників вмісту, включаючи медіа-гіганта Viacom, подали до суду на YouTube за порушення авторських прав, а YouTube, захищаючись, послався на розділ 512 Закону «Про захист авторських прав у цифрову епоху». Оскільки YouTube є дочірньою компанією Google, то її майбутній бізнес-план передбачає розміщення реклами відповідно до типу відео, які користувачі переглядають або шукають. Таким чином, якщо сайт передбачає це, він може мати фінансову вигоду, безпосередньо пов'язану з обміном матеріалами захищеними авторським правом.

Ці випадки в даний час розглядаються у федеральних окружних судах США, і їх вирішення буде мати значний вплив на послуги, які пропонують соціальні мережі, а також їх бізнес-моделі.

Розділ 230 Закону «Про прихильність до комунікації» захищає веб-сайт від певної відповідальності, що впливає з публікації інформації, наданої іншою стороною даному сайту. Як правило, такий захист виникає в контексті дискредитації, конфіденційності, недбалості та інших претензій до сайту. Однак це не стосується кримінальної відповідальності, порушення авторських прав та інших претензій щодо прав інтелектуальної власності.

Таким чином, якщо користувач публікує наклепницький чи іший протизаконний вміст, розділ 230 захищає соціальну мережу від певної відповідальності, яка виникає внаслідок публікації. З іншого боку, веб-сайти, які повністю або частково створюють чи розробляють

¹ Thomson Reuters. Understanding the Legal Issues for Social Networking Sites and Their Users. URL: <https://technology.findlaw.com/modern-law-practice/understanding-the-legal-issues-for-social-networking-sites-and.html>.

ють спірну інформацію, вважаються «контент-провайдерами», які не користуються захистом розділу 230.

Користувачі соціальних мереж не мають імунітету, наданого сайтам соціальних мереж відповідно до закону, тому вони повинні бути обережними, щоб завжди діяти належним чином, публікуючи повідомлення або файли на сайтах.

Основні сфери, де користувачі можуть потрапити у неприємність, – це публікування наклепницького контенту чи вмісту, який порушує права інтелектуальної власності.

Оскільки для захисту користувачів немає імунітетів, наданих певним законом, застосовуються стандартні норми, що стосуються наклепу та порушень.

Окрім того, слід вказати і на те, що хоча кожен розділ державного законодавства США щодо соціальних мереж застерігає роботодавців від запитування у співробітників або заявників їхні імена користувачів і паролі від соціальних мереж, близько 11 законопроектів також містять положення, що забороняють роботодавцям вимагати від працівників або заявників доступ до своїх особистих соціальних мереж у присутності біля працівника у цей момент роботодавця. Така практика, відома як «позаплечовий серфінг», дозволяє роботодавцю переглянути контент, який співробітник або заявник опублікував на Facebook або в іншому соціальному ЗМІ, не запитуючи прямо у співробітника його ім'я користувача або пароль. Хоча «позаплечовий серфінг» може виглядати менш нав'язливим, ніж вимагати пароль для соціальних мереж, та вже чотири штати – Каліфорнія, Іллінойс, штат Орегон і Вашингтон – вже зробили таку практику незаконною. Каліфорнія та Вашингтон не дозволяють роботодавцю навіть просити, щоб працівник або заявник заходив до соціальних мереж у присутності роботодавця¹.

Також слід звернути увагу на законодавчі новели, що впроваджуються у Сполученому Королівстві Великобританії. Воно вважає за доцільне сформулювати нове законодавство, яке буде більш детально регулювати соціальні медіа. Міністр культури та цифрового простору Метт Ханкок заявив, що нові закони будуть запроваджені «в найближчі пару років». Вони будуть спрямовані на подолання ряду юридичних та незаконних Інтернет-«посягань», «кібербулінгу» (залякування в Інтернеті) та сексуальної експлуатації дітей у цифровому просторі².

¹ T. Quackenboss R. Lesser-Known Social Media Legislation. 2013. URL: <https://www.huntonak.com/images/content/3/7/v3/3720/Lesser-Known-Social-Media-Legislation.pdf>.

² Vincent J. The UK wants to police social media with new 'online safety' laws. 2018.

Дане законодавство буде останньою спробою консервативного уряду Великобританії здійснювати більший контроль над Інтернет-простором. Слід також зазначити, що у 2016 році партія провадила нові закони про нагляд, закріпивши (серед іншого), що інтернет-провайдери зберігають запис історії веб-браузера кожного громадянина.

Доволі цікавим та оригінальним є також підхід до питань захисту даних, який застосовується у Німеччині. Уповноважені з питань захисту даних у цій країні вимагають, щоб налаштування у соціальній мережі Facebook за замовчуванням базувались на принципі згоди – тобто за замовчуванням в налаштуваннях програмних продуктів має бути зазначено те, що дані користувача не збираються соціальною мережею¹.

Отже, провівши аналіз законотворчої практики різних країн світу та дослідивши «Умови надання послуг» соціальної мережі Facebook (однієї з найбільших у світі), можна дійти висновку, що відносини, які склалися між соціальними мережами та їх користувачами, найчастіше оточені досить жорсткими рамками відносно користувачів. Соціальні медіа доволі суворо регламентують свої положення та власні можливості щодо збору та розповсюдження персональних та цифрових даних користувачів, проте наразі несуть значно менше ризиків, ніж їхні користувачі, незважаючи на спроби таких провідних держав, як Великобританія, США та Німеччина, врегулювати й збалансувати такі відносини належним чином шляхом правового регулювання та захисту прав безпосередньо самих користувачів соціальних мереж.

URL: <https://www.theverge.com/2018/5/21/17375450/uk-social-media-online-safety-legislation-matt-hancock>.

¹ Legal Aspects of the Use of Social Media. 2013. URL: https://www.haerting.de/sites/default/files/downloads/handout_legal_aspects_of_social_media_2013.pdf.

ПРАВОЧИНИ В СОЦІАЛЬНІЙ МЕРЕЖІ

Розвиток ринкової економіки та науково-технічний прогрес привели до того, що правочини, які вчиняються з використанням електронних засобів зв'язку, є повсякденним явищем у нашому житті. Переваги у вчиненні правочинів за допомогою електронних засобів зв'язку очевидні: швидкий, оперативний обмін інформацією, зручність зберігання, оброблення, відправлення документів.

Враховуючи інформатизацію суспільства та формування цифрового середовища, в якому передбачається взаємодія всіх суб'єктів правовідносин, зокрема і цивільних, можна говорити про існування двох паралельних підходів: традиційного та нового (інформаційного). Наразі ми є свідками формування інформаційного, цифрового суспільства нового зразка (якості). Це стосується і правочинів: сьогодні є можливість укласти правочини як традиційним способом, так і більш оновленим, електронним, що офіційно регулюється законодавством (умови вчинення, сторони, наслідки невиконання умов тощо).

В рамках інформатизації суспільства популярності набули і соціальні мережі, які мали на меті забезпечити можливість користувачам обмінюватися різного роду інформацією, здійснювати її пошук, як, наприклад, знаходити старих і нових друзів, однокласників, однокурсників і т.п. Наразі соціальні мережі сприймаються більшістю користувачів як засіб розваги і спілкування, обміну інформацією. Також постійно збільшується значення використання соціальних мереж в економічній сфері, при організації різного роду 3D конференцій, міжнародних презентацій, наукових відеочатів тощо.

Зазначене зумовлює і збільшення інтересу бізнесу до соціальних мереж, використання їх можливостей для вчинення різного роду правочинів. Цим пояснюється постійне збільшення реклами, в тому числі і в соціальних мережах. Найпопулярнішими нині є такі соціальні мережі, як Facebook, Twitter та Instagram, які широко використовуються і для ведення бізнесу, а не лише спілкування.

Платформа, яка б дозволяла безпосередньо заробляти у соцмехах, відсутня, однак в Україні діє велика кількість агентств, які дають свої послуги компаніям, що прагнуть популяризувати бренд через соціальні мережі. Зокрема, досить високі прибутки можуть мати SMMщики (від SocialMediaMarketing), оптимізатори контенту тощо.

Digital-агентства – це організації, які займається розробкою, просуванням інтернет-ресурсів в медіа-просторі, в тому числі соціальних мереж. Працівники таких агентств створюють сайти й організують їх оптимальну роботу, просувають їх за допомогою цифрових медіа та в онлайн-спільнотах (паблік у соціальних мережах, форуми, матичні майданчики) тощо.

Правочин є одним з найбільш поширених юридичних фактів у сфері приватного права, будучи головною підставою виникнення цивільних регулятивних правовідносин. Як правова категорія, правочин характеризується сукупністю ознак, що дають можливість відмежовувати їх від інших юридичних фактів, зокрема, правочин завжди є вольовим актом; є дією, спеціально спрямованою на досягнення певного правового результату; є дією суб'єктів цивільного (приватного) права; завжди є правомірною дією. Названі ознаки є загальними для усіх типів правочинів, а тому стосуються й правочинів, які укладаються в ІТ-сфері, зокрема, і в соціальних мережах.

«Традиційними» можна вважати правочини, правове регулювання яких відбувається відповідно до засад, встановлених у чинному цивільному законодавстві (ЦК України), зокрема, чітко встановлені умови дійсності, основи тлумачення, наслідки недійсності тощо. Стосовно правочинів такого роду існує цивілістична традиція, сформована стала судова практика.

Умовами дійсності правочинів є вимоги щодо: 1) змісту правочину, 2) наявності правочиностдатності суб'єктів правочину, 3) повідності волевиявлення внутрішній волі суб'єкта (суб'єктів) правочину, 4) форми правочину, 5) реальності правочину, 6) дотримання спеціальних умов, встановлених законом для даного виду правочину. Правочини, які можуть бути здійснені в соціальній мережі, також мають відповідати встановленим чинним законодавством умовам дійсності. На жаль, окремо така категорія правочинів законодавчо не регулюється (хоч останнім часом законодавець намагається узгодити діючі норми з реаліями, що, зокрема, виражається у закріпленні понять електронного правочину, електронного договору, електронної комерції тощо) і такі правочини мають свої особливості вчинення, процедури виконання тощо. Проаналізувавши більш детально зазначені умови.

Відповідно до ч. 1 ст. 203 ЦК України, зміст правочину не може суперечити актам цивільного законодавства, а також інтересам держави і суспільства, його моральним засадам, тобто фізичні та юридичні особи повинні враховувати вимоги щодо здійснення цивільних прав, встановлених у ст. ст. 12, 13 ЦК України та інших актах цивільного законодавства. Дана умова дійсності правочину має ути «абсолютною» для всіх видів правочинів, які вчиняються міжчасниками цивільних правовідносин. Не є виключенням і соціальні мережі, особливо враховуючи те, що активними користувачами соціальних мереж у своїй більшості є молодь, особи, які внаслідок своєї недосвідченості можуть бути чутливі до так званої «забороненої» інформації (як, наприклад, антиморальної, антисоціальної тощо). Враховуючи специфіку онлайн середовища, вважаємо, що можливість укладення правочинів, які б суперечили актам цивільного законодавства, інтересам держави і суспільства, його моральним засадам, повинні «передбачувати», «блокувати» тощо провайдери та нести відповідальність за свою бездіяльність.

Важливою вимогою до чинності правочину є те, що його можуть вчиняти лише суб'єкти, які мають необхідний обсяг правосуб'єктності (ч. 2 ст. 203, ст. ст. 30–32, 34–39, 41, 42, 92 ЦК України). Діюче цивільне законодавство чітко визначає вимоги до осіб, які наділені цивільною правосуб'єктністю. Зокрема, зміст дієздатності фізичної особи залежить від віку особи і від стану її психіки, з урахуванням чого виділяється повна, часткова дієздатність або недієздатність. Самостійне вчинення правочинів є одним із найважливіших елементів дієздатності. Враховуючи те, що в різних країнах вік осіб, які можуть стати користувачами соціальних мереж, є різним, однак, він, як правило, нижчий за вік повної дієздатності особи, важливо розуміти, які саме правочини в соціальній мережі може здійснювати зареєстрована особа. Також є можливість не вказувати свій вік (або ж вказати вигаданий), що може надати можливість отримати доступ до інформації, сервісів тощо, які фактично були б недоступні малолітньому. В даному випадку мова йде про введення в оману, що може бути складно виявити. Відповідно до діючого законодавства України за протиправні дії малолітніх і неповнолітніх (частково) несуть відповідальність батьки (які могли взагалі не знати про дії своїх дітей у соціальних мережах). Якщо ж мова йде про осіб, які мають опікунів чи піклувальників, то їх дії також повинні відповідати чинному законодавству.

Наступну умову, необхідну для чинності правочину, ЦК України визначає, як вчинення у формі, встановленій законом. Виділяють наступні форми зовнішнього виразу волі при вчиненні правочину: конклюдентні дії; мовчання; усна; письмова; письмова з нота-

ріальним посвідченням; письмова з дотриманням спеціальних мог (державна реєстрація тощо). Враховуючи те, що більшість «тудиційних» правочинів передбачено вчиняти у письмовій формі, бимо висновок про важливість вимоги щодо дотримання форми.

Розглядаючи можливі форми укладення правочинів у соціальних мережах, можна дійти висновку, що переважна більшість правочинів вчиняється у формі надання згоди на запропоновані умови без можливості змінити умови правочину, що фактично можна порівняти з усним правочином. Також правочини, які вчиняються у соціальній мережі, можуть мати і письмову форму, як, наприклад, правочини з адміністраторами, провайдерами тощо.

Після аналізу форми вчинення правочину як умови його дійсності не можна не звернути увагу на зазначену вище умову щодо реальності правочину, яка також є необхідною для визнання правочину дійсним. Тобто правочин має бути спрямований на реальне настання правових наслідків, що ним обумовлені. Вчинення правочинів через соціальні мережі мають деякий ступінь ризику, адже є можливість того, що товари, послуги тощо, які пропонуються через соціальні мережі, не відповідають характеристикам цих товарів у реальному житті (інші якісні характеристики або ж взагалі відсутність такого товару, тобто фактично це обман). Розглянемо декілька прикладів.

Яскравим прикладом впливу соціальних мереж на формування враження від пропозицій в Інтернеті є експеримент У. Батлера з Лондона, який рекламував неіснуючий насправді ресторан, оформивши відповідним чином сайт, розміщуючи велику кількість позитивних коментарів. У результаті активної роботи над сайтом ресторан «Theshedatdulwich» зайняв перше місце в рейтингу, бажаючих його відвідати було досить багато¹. В даному випадку експеримент не мав на меті реально щось продавати (адже фактично не існувало ані приміщення, ані співробітників) чи купувати (хоча і надходили пропозиції від постачальників товарів тощо), а лише довести «силу Інтернету», а саме відгуків у соціальних мережах, які і сформували ажіотаж і велику кількість бажаючих відвідати новий ресторан.

Ведучи мову про реальність правочину необхідно зазначити, що купуючи будь-який товар через соціальні мережі, користувач мережі не може бути впевнений у тому, що описані якісні характеристики відповідають дійсності, що немає пошкоджень товару тощо. Може здатися, що покупка через спеціалізований інтернет-магазин має більше гарантій якості та відповідальності з боку продавця.

¹ URL: https://macos.livejournal.com/1638607.html?utm_source=fbsharing&utm_medium=social.

аніж покупка у фізичної особи через соціальні мережі. Що не завжди відповідає дійсності. Також гарантією якості та відповідальності продавця вважається наявність позитивних відгуків інших покупців, які демонструють вже куплений товар, розмішують його фото тощо. Так, частково це може зорієнтувати особу у виборі товару, однак попередній приклад говорить про можливість розміщення несправжніх відгуків, які будуть лише дезорієнтувати.

На практиці можуть бути і відверто обманні дії, коли створений сайт працює деякий час, розмішуючи фейкові позитивні відгуки, пропонуючи купити товар та оплатити його відразу, а покупка взагалі не приходить. З часом сайт перестає існувати і повернути свої кошти вже не видається можливим.

Тому більш реальною гарантією виконання продавцем своїх обов'язків є пропозиція оплатити товар після отримання його покупцем (наприклад, при отриманні посилки на пошті або кур'єру при доставці). Нині цей спосіб оплати набрав популярності і досить часто використовується.

Разом з тим перспективним способом гарантувати виконання зобов'язань укладеного договору за допомогою соціальних мереж є гарант-сервіси (захищений правочин). Такі сервіси передбачають, що гроші за послуги або товари не надходять безпосередньо від покупця до продавця, а кладуться на банківський рахунок, який так само недоступний для обох сторін правочину, що, у свою чергу, є гарантією дотримання інтересів всіх учасників правовідносин.

Захищений правочин вигідний для всіх сторін-учасниць: продавець гарантовано отримує оплату, покупець мінімізує ризики в разі скасування правочину або шахрайства, а агент отримує фіксований відсоток.

Головна перевага захищеного правочину полягає в присутності третьої сторони – компанії-посередника, гаранта, яка збереже гроші покупця, якщо продавець поставить неякісний товар або порушить умови правочину, що дає можливість робити безпечні покупки на будь-яку суму, як з офіційним рітейлером, так і з індивідуальним продавцем.

Фактично ризик шахрайства зникає: гроші поступають продавцеві з рахунку компанії-посередника лише після того, як товар буде доставлений і покупець підтвердить, що все гаразд. Послуга може активно використовуватися й учасниками соціальної мережі, де завжди велика ймовірність отримати товар, який не відповідає заявленій якості, навіть незважаючи на наявність позитивних відгуків.

Останнім часом особливою популярністю користуються спільні покупки товарів закордоном, коли кілька користувачів ко-

оперуються і створюють єдине замовлення в закордонному інтернет-магазині, яке потім доставляють однією посилкою. Таким чином всі учасники економлять на миті і комісійних зборах, іноді отримують знижку. У подібних ситуаціях спеціальний сервіс може захистити всю групу, а комісію розподілити між усіма учасниками.

Спочатку послуга «захищений правочин» використовувалася при укладенні правочинів з нерухомістю. У Великобританії і США широко поширена практика передачі грошових коштів юристам для виконання всіх умов обома сторонами¹. В Україні цей інструмент ще мало відомий, але позитивні тенденції вже з'являються в різних сферах.

Всі сервіси захищених правочинів працюють за схожим принципом, незалежно від типу покупки. Так, щоб придбати старий автомобіль або заробити на цікавому проєкті, не відходячи від комп'ютера, досить пройти кілька простих етапів. Спочатку слід вибрати відповідний сервіс. Далі обговорити з продавцем (замовником) умови, при виконанні яких грошові кошти надійдуть виконавцю. Правочин буде вважатися вчиненим. Внести всі нюанси (особливі умови) в спеціальну онлайн-форму і далі перевести необхідну суму компанії-гаранту (гроші «заморожуються» на банківській карті або зберігаються на рахунку агента). Агент, у свою чергу, інформує продавця про те, що гроші отримані. Покупець перевіряє отриманий товар на відповідність обговореним заздалегідь вимогам та підтверджує це, що дає можливість перевести гроші продавцю. Аналогічним чином завершується «правочин із замовником»: особа отримує кошти, виконавши своє завдання у відповідності із зафіксованими умовами.

У разі ж виявлення дефектів товару при укладенні «захищеного правочину» вирішити ситуацію допоможе онлайн-сервіс врегулювання суперечок (який є у більшості компаній-посередників), який можна скористатися, якщо попередньо не вдалося вирішити конфлікт самостійно.

Залежно від суми правочину компанія-гарант утримує фіксовану комісію, але при цьому користувачі можуть самі вирішувати, хто буде її сплачувати: продавець чи покупець. Є можливість розділити комісійний платіж на двох, а якщо в правочині зацікавлено більше двох осіб – рівномірно між учасниками.

Якщо правочин виявився спірним, гроші будуть передані продавцю лише після того, як сторони домовляться між собою і претензія буде відсутня.

¹ URL: <https://rb.ru/longread/escrow>.

Правочини в інтернет-співтоваристві можуть вчинятися і щодо електронного товару. З урахуванням сервісу «захищеного правочину» правочин вважається вчиненим, коли покупець отримав електронний товар, а продавець отримав грошові кошти¹.

Деякі маркетплейси користуються альтернативними методами підвищення безпеки платежів на своїх платформах. Одним з таких інструментів є «рейтинг продавців», який активно використовується AliExpress, Ebay й іншими великими торговельними майданчиками і інтернет-аукціонами.

У країнах Європи поряд з власними системами врегулювання конфліктів на інтернет-майданчиках компаній діє єдина платформа, де конфлікти між споживачами і онлайн-продавцями розглядаються незалежною комісією.

Варто відзначити, що раціонально було б запустити і в Україні подібний сервіс досудового оскарження спорів, спираючись на успішний закордонний досвід впровадження таких систем.

Аналогів сервісу безпечних правочинів на ринку України поки не існує, проте є дуже близькі, схожі сайти, які орієнтовані на роботу тільки в рамках свого проекту, це, зокрема:

1. Bigl.ua (колишній aukro.ua) – найбільший в Україні On-line-маркет з товарами перевірених продавців, проєкт групи компаній EVO. На цей майданчик потрапляють тільки ті продавці, у яких більше 90% позитивних відгуків, весь асортимент товарів у наявності, а також незмінно висока якість обслуговування.

2. Kloomba.com і kidstaff.com.ua – батьківська дошка оголошень, на якій можна розмістити приватні оголошення, запропонувати продаж різних товарів, як для дітей, так і для дорослих, речі (одяг), взуття, іграшки та інші товари. Є свій особистий рейтинг продавців, і так само можна залишити відгук про покупця.

3. «Захищений платіж» від Приватбанку. Сервіс представлений в травні 2015 року для послуг і товарів, придбаних в Інтернет-магазинах або у приватних осіб.

4. Prom.ua – всеукраїнський торговий центр в Інтернеті, найбільший майданчик України з великим асортиментом від продавців зі всієї країни.

5. OLX.ua – компанія, що надає On-line-майданчик для оголошень про продаж вживаних товарів, таких як меблі, музичні інструменти, спортивні товари, автомобілі, дитячі товари, мотоцикли, фотоапарати, мобільні телефони та багато іншого.

¹ URL: <http://garant.pro/telegram>.

В цьому напрямку варто згадати про стартап PavelStavratii, який пропонує запустити сервіс безпечних On-line правочинів, основними перевагами роботи якого будуть:

- реальні відгуки і репутація про кожного користувача;
- повний захист коштів і посилок від шахрайства;
- швидко і вигідно продати / купувати протягом доби;
- вирішення спірних правочинів через арбітраж сервісу безпечних On-line правочинів;
- більше не потрібно переплачувати комісію за накладення платеж (післяоплату);
- кошти надходять на карту протягом 15 хвилин після отримання посилок.

Дохідна частина проекту (стартапу) – це фіксована комісія сервісу у вигляді відсотків від суми товару за кожну успішну операцію. При ціні за товар до 1000 грн комісія буде складати фіксовану суму 10 грн, а понад 1000 грн безпосередньо 1 % від суми товару. Проект знаходиться на етапі повністю готового робочого прототипу, і автор запрошує до співпраці потенційних інвесторів¹.

Враховуючи різноманітність напрямів вирішення спорів у соціальних мережах, досить цікавою є думка відеоблогера і адміністратора дискорду Alex. Дискорд (Discord) – це безкоштовний месенджер з підтримкою VoIP і відеоконференцій, орієнтований на користувачів комп'ютерних ігор. В даній мережі також вчиняють правочини, трапляються суперечки, відбувається спілкування.

Як заявляє Alex, найбільша помилка – це асоціювати інтернет-діяльність з реальністю, адже в Інтернеті не мають значення статус досягнення особи (як в реальному житті), основами спілкування є недосяжність, анонімність, безкарність. Тому, розглядаючи модератора чи адміністратора як аналог армії і поліції інтернет-простору, які в теорії мають цілу систему законів, але не мають влади її застосовувати, пропонується спростити саму систему. Модератор і адміністратор покликані захищати інтереси спільноти, і вони, який не поліцейський або суддя, вони аналог «вибивали» в клубі, а отже вони можуть (не вникаючи в суть конфлікту) просто уникнути інцидент за умови, що ситуація шкодить каналу (соціальній інтернет-спільноті). Наприклад, якщо два учасники посварились в загальному чаті – mute (заборона на спілкування) обох без роз'яснення причин і наслідків. Тому що, на відміну від псевдоавторитету управлінців дискорду, ban (забороняти) і mute (різнорічний бан) – реальний інструмент².

¹ URL: <https://startup.ua/startups/348426.html>.

² URL: https://youtu.be/qsFyjQD_VCk.

Така позиція вирішення спорів превалює в інтернет-спільноті, особливо активно використовується адміністраторами гральних соціальних мереж при вирішуванні конфліктів сторін-учасників, які активно купують та продають ігрові атрибути.

Укладення правочинів за допомогою засобів електронного зв'язку регулюється, зокрема, такими нормативно-правовими актами, як: закони України «Про електронні документи та електронний документообіг», «Про електронний цифровий підпис», «Про захист прав споживачів», «Про електронну комерцію». Дані закони дають визначення таким поняттям, як: договір, укладений на відстані, електронний договір, електронний правочин, електронна торгівля тощо.

Так, під електронною торгівлею розуміється господарська діяльність у сфері електронної купівлі-продажу, реалізації товарів дистанційним способом покупцю шляхом вчинення електронних правочинів із використанням інформаційно-телекомунікаційних систем; під електронним правочином – дія особи, спрямована на набуття, зміну або припинення цивільних прав та обов'язків, здійснена з використанням інформаційно-телекомунікаційних систем; під електронним договором – домовленість двох або більше сторін, спрямована на встановлення, зміну або припинення цивільних прав і обов'язків та оформлена в електронній формі.

Електронну комерцію визначають як систему правовідносин у сфері вчинення правочинів за допомогою використання мереж електрозв'язку, що ґрунтується на електронній обробці та передачі даних і охоплює різноманітні види діяльності щодо продажу товарів, надання послуг та виконання робіт.

На сьогодні виділяють такі основні форми здійснення електронної комерції: електронний обмін інформацією (ElectronicDataInterchange, EDI); електронний рух капіталу (ElectronicFundsTransfer, EFS); електронна торгівля (E-Trade); електронні гроші (E-Cash); електронний маркетинг (E-Marketing); електронний банкінг (E-Banking); електронні страхові послуги (E-Insurance); електронні брокерські послуги (інтернет-трейдинг); електронні аукціони; електронна пошта; електронні бюро; дистанційне навчання¹.

Великою перевагою використання електронних договорів у цивільному праві є економія часу, що одночасно дозволяє скоротити витрати і розширити число потенційних контрагентів. Стаття 207 ЦК України прирівнює до вчинених у письмовій формі правочинів правочини, зміст яких зафіксований у кількох документах (зокрема листах), а також правочини, воля сторін яких виражена за допо-

¹ Блажівська Н. Є. Електронні правочини в цивільному праві України. URL: http://pidruchniki.com/68105/pravo/visnovki_rozdilu_elektronniypravochin.

могою електронного або іншого технічного засобу зв'язку. Законом України «Про електронну комерцію» визначає електронний договір як домовленість двох або більше сторін, спрямовану на встановлення, зміну або припинення цивільних прав і обов'язків, оформлену в електронній формі.

Виділяють два види договорів, що укладаються через Інтернет: 1) через Web-сайт (продаж товарів за допомогою інтернет-магазинів, надання послуг); 2) по e-mail. Такі договори можуть укладатися між організацією і фізичною особою (так званим кінцевим споживачем), а також між юридичними особами. І так само, як і при укладенні традиційного договору, клієнт і продавець мають дотримуватися порядку укладення договору, а саме – наявність оферти і акцепту. З розвитком торговельної діяльності через інтернет-ресурси стало поширеним укладення договору через мережі за допомогою здійснення певних конклюдентних дій: click-wrap agreement (угода, яка укладається шляхом натискання мишею) і browse-wrap agreement (угода, яка укладається шляхом використання веб-сайта).

Отже, особливістю електронного договору є те, що він вкладається в електронній формі. ЦК України передбачає можливість вчинення договорів в усній та письмовій формах. Також пам'ятаємо про ст. 639 ЦК України, яка передбачає можливість укладення договору у будь-якій формі, якщо вимоги щодо форми договору не встановлені законом. При цьому електронна форма договору не передбачається як одна із його можливих і правомірних форм. Абзац другий ч. 2 ст. 639 ЦК України передбачає, що договір, який укладений за допомогою інформаційно-телекомунікаційних систем, вважається укладеним у письмовій формі. Однак, враховуючи специфіку укладення електронних договорів, можна сказати, що він швидше прирівнюється до письмового договору, аніж є таким.

Сам по собі продаж товарів з використанням соціальних мереж не є неправомірним (за винятком зброї, наркотиків та інших товарів, обіг яких заборонено). В діючому законодавстві немає нормативного акта, який би забороняв продаж товарів через соціальні мережі. Разом з тим існують реальні порушення діючого законодавства при здійсненні продажу товарів через соціальні мережі. Розглянемо основні з них.

1. Продаж товарів через соціальні мережі може тлумачитися згідно з законодавством як продаж товарів на замовлення позаофісного торговельного приміщення, що передбачає відповідне оформлення. Відсутність оформлення такої діяльності (продаж товарів через соціальні мережі) є порушенням, а це, у свою чергу, порушує Закон України «Про захист прав споживачів».

2. Самостійний, регулярний продаж через соціальні мережі з метою отримання прибутку підпадає під визначення підприємницької діяльності і має здійснюватися суб'єктом підприємницької діяльності фізичною або юридичною особою, зареєстрованою у встановленому Законі України «Про державну реєстрацію юридичних осіб, фізичних осіб – підприємців та громадських формувань». У більшості випадків продавці в соціальних мережах своєю діяльністю ніяк не оформляють, що є прямим порушенням діючого законодавства.

3. Відповідно до Податкового кодексу України всі особи, які займаються підприємницькою діяльністю, повинні сплачувати податки. Однак користувачі соціальних мереж, які вчиняють правочини з метою отримання прибутку, в основному не виконують дану вимогу, чим прямо порушують чинне законодавство України.

Разом з тим стрімкий розвиток інформаційних технологій, можливості Мережі, в тому числі розвиток та глобальне використання соціальних мереж, свідчать про необхідність врахування особливостей таких видів правочинів (як договорів, так і односторонніх правочинів), які стосуються суб'єктного складу, об'єктів, наслідків виконання або ж невиконання (чи неналежного виконання), можливості визнання таких правочинів недійсними (враховуючи специфіку інтернет-середовища, застосування наслідків такої недійсності тощо).

Особливостями укладених правочинів у цифровій (електронній) площині є засоби ідентифікації, як інструмент встановлення особи, яка її вчиняє (можуть бути використані наступні засоби ідентифікації: електронний підпис, електронний цифровий підпис, паспорт громадянина України у формі карти з безконтактним електронним носієм (та електронним цифровим підписом), Bank ID, підпис одноразовим ідентифікатором та аналог власноручного підпису), та форма його вчинення, дотримання якої є однією із загальних вимог, необхідних для забезпечення його чинності.

Однак якщо мова йде про укладення правочинів у соціальні мережі, то засобами ідентифікації в основному є більш «прості» способи, як, наприклад, підпис одноразовим ідентифікатором, електронний підпис. Саме простота їх використання є головною перевагою при виборі варіанта засобу ідентифікації. Разом з тим вони є більш ризикованими внаслідок простоти підробки, адже отримуючи підтвердження з номера телефону продавець не може бути впевнений, що це не викрадений телефон і що особа дійсно бажає здійснити покупку. Також немає впевненості в тому, що особа вчиняє правочин у межах своєї дієздатності. Враховуючи те, що користувачами соціальних мереж офіційно можуть бути особи

з неповною дієздатністю, виникає питання про можливість укладення ними правочинів лише в межах своєї дієздатності. Контроль у даному випадку не видається можливим. З одного боку, за дії малолітніх і неповнолітніх осіб несуть відповідальність батьки; з іншого боку, продавець не має права реалізовувати певні товари неповнолітнім (як, наприклад, алкогольні, тютюнові вироби, зброя тощо), однак натиск позиції «Він є 18 років» не гарантує достовірності такої інформації. Також на практиці можуть виникнути проблеми при вчиненні правочинів неповнолітніми недієздатними та обмежено дієздатними особами.

Отже, правочини, вчинені в соціальній мережі, як будь-які правочини, повинні відповідати умовам дійсності, перерахованим вище. Якщо ж правочин вчинено з порушенням даних умов (а хоча б однієї з них) — він не може вважатися дійсним.

Розвиток інформаційного суспільства та активне використання Інтернету, і соціальних мереж, зокрема при вчиненні правочинів, дає можливість говорити не просто про «правочини», а про правочини нового типу, які сутнісно пов'язані з використанням інформаційних технологій, внаслідок чого можуть мати таку назву: «ІТ-правочини» і визначатися як дії суб'єкта цивільного права, що вчиняються у сфері застосування та /або за допомогою інформаційних технологій, спрямовані на встановлення, зміну, припинення цивільних прав та обов'язків.

АКАУНТ У СОЦІАЛЬНІЙ МЕРЕЖІ ЯК ОБ'ЄКТ ЦИВІЛЬНИХ ПРАВОВІДНОСИН

Життя кожного з нас сьогодні настільки тісно пов'язане з Інтернетом, що ми вже не звертаємо уваги на рівень нашої онлайн активності, не завжди пам'ятаємо, які дії вчиняємо онлайн, не замислюємося над тим, якою кількістю акаунтів володіємо, оскільки про деякі забуваємо невдовзі після того, як створили. Між тим, за даними додатку Dachlane, середній користувач цього додатку має близько 90 акаунтів, і це привід замислитись. Адже сьогодні на законодавчому рівні не визначено ані поняття, ані правової природи, ані особливостей правового регулювання акаунтів, в той час як деякі з них містять важливу інформацію та мають не абияку цінність для своїх володільців. Іноді акаунти у соціальних мережах можуть приносити реальний прибуток, наприклад, шляхом монетизації відео, як це має місце в YouTube, або завдяки кількості підписників, що дає можливість володільцям акаунтів розміщувати рекламу та отримувати від цього дохід. Такі можливості заробляти на власних акаунтах поступово перетворюють їх на важливі об'єкти цивільного обігу, разом із тим питання щодо можливостей відчуження або передачі в аренду чи інших способів використання акаунтів з комерційною метою, проблеми їх захисту, долі їх після смерті володільця залишаються відкритими.

Перш за все, необхідно визначитись, що ми маємо розуміти під поняттям «акаунт». Акаунт (від англ. account) є записом, який містить набір певних відомостей, що передаються користувачем який-небудь комп'ютерній системі. Акаунти призначені для ідентифікації користувача, який входить у певну комп'ютерну систему, обліку його дій та збору статистики його поведінки в системі. Основними даними про користувача, що містяться в акаунті, є логін, e-mail, пароль або інший спосіб аутентифікації¹.

За загальним правилом, акаунтом (обліковим записом, профілем) у соціальній мережі вважається особиста сторінка, на якій ко-

¹ Акаунт. URL: <https://wiki.rookee.ru/akkaunt>.

ристувач розміщує особисту інформацію, викладає відео-, аудіо- та інші матеріали, за допомогою якої веде листування з іншими користувачами та управління якою можливе лише після процедури авторизації шляхом введення відповідного логіну та пароля. Таким чином фактично під акаунтом маються на увазі кілька складових: по-перше, це інформація для авторизації користувача (яка необхідна для ідентифікації його провайдером та включає в себе ім'я користувача та пароль, що являють собою рядки символів), по-друге, акаунт в'язаний із базою даних на сервері провайдера, у якій зберігається інформація з цього акаунту. Ця база даних зв'язує користувача з інформацією в соціальній мережі. Як зазначає Пржемыслав Палка, це своєрідний кіберпростір у рамках кіберпростору – чиясь особисте місце в рамках більш широкого контексту. З цієї точки зору він пропонує вважати акаунти цифровими об'єктами, які також виконують певні функції сервісу. До цього слід додати, що платформами він розглядає як сервіси (послуги), але не в традиційному розумінні цього поняття, він вважає їх скоріше кіберпростором, у якому люди «присутні в цифровому вигляді» та набувають ліцензії на користування ним¹.

Зазначимо, що з урахуванням потреб цивільного обігу видається доцільним розрізнити в деяких випадках ці складові акаунту – імені користувача та інформаційного наповнення веб-сторінки, пов'язана з акаунтом. Такий підхід може бути пояснений тим, що в деяких випадках особу може зацікавити придбання саме імені користувача, оскільки, наприклад, раніше зареєстрований обліковий запис збігається з назвою, скажімо, знов створеної фірми, яка може бути цікавлена мати саме цей запис у якості свого акаунту. Особа ж, яка зареєструвала свій акаунт раніше, цілком може бути згодна віддати цей запис, попередньо видаливши всю інформацію профілю, яка не цікавить покупця. Разом із тим у деяких випадках покупець може цікавити весь профіль користувача з метою, скажімо, отримання інформаційними/рекламними повідомленнями його друзів чи писників або з іншою метою. В такому випадку об'єктом відношення буде весь акаунт, а не його окремий елемент. Крім того, варто зазначити, що акаунт може бути як об'єктом договірних (у випадку його продажу, передачі в користування тощо), так і об'єктом ліквідації правовідносин (у випадку його незаконного захоплення або зламу).

Отже, акаунт у таких соціальних мережах, як Facebook, YouTube, Instagram, Google тощо, по суті є веб-сторінкою (веб-сторінка – інформаційний ресурс, доступний в мережі World Wide Web (В

¹ Przemysław Palka. Virtual property: towards a general theory. URL: http://cad.eui.eu/bitstream/handle/1814/49664/Palka_2017.pdf?sequence=1&isAllowed=y.

вітня павутина), який можна переглянути у веб-браузері¹), відповідно власник веб-сторінки розміщує на ній інформацію незалежно від власника веб-сайта (яким є сама та чи інша соціальна мережа) та самостійно управляє нею. Це породжує питання про відповідальність власників акаунтів за дії, які вони вчиняють у соціальній мережі.

Визначення поняття веб-сторінки міститься у Законі України «Про авторське право та суміжні права», відповідно до якого веб-сторінка — це складова частина веб-сайта, що може містити дані, електронну (цифрову) інформацію, інші об'єкти авторського права і (або) суміжних прав тощо. Отже, перш за все у питаннях, пов'язаних із використанням акаунтів у соціальних мережах, слід керуватися вже існуючими правилами щодо правового регулювання веб-сторінок. Наприклад, це стосується питань відповідальності за інформацію, розміщену на веб-сторінці, зокрема щодо порушення авторських прав. Так, якщо донедавна ще було дискусійним питання щодо того, хто є належним відповідачем у справі про захист авторського права², і навіть існує позиція Пленуму ВГС України «Про деякі питання практики вирішення спорів, пов'язаних із захистом прав інтелектуальної власності» від 17 жовтня 2012 року щодо того, що власники сайта, на якому було розміщено твори без надання дозволів згідно з законом, визнаються порушниками авторського права³, сьогодні ситуація змінилася. Останнім часом вже визнається той факт, що існують різні види веб-сайтів, деякі з них, як, наприклад, соціальні мережі, надають користувачам можливість самостійно розмішувати інформацію на своїх веб-сторінках, а тому саме останні є відповідальними за порушення прав інтелектуальної власності. Зазначимо, що саме така позиція вже знайшла своє відображення у судовій практиці. Так, нещодавно Верховний Суд України постановив залишити в силі рішення господарського суду Рівненської області від 24 травня 2017 року про стягнення з відповідача 64 000 грн на користь позивачів за розміщення та публічну демонстрацію на Інтернет-сторінці у соціальній мережі Facebook за гіперпосиланням твір, виключні майнові права на який належали позивачам⁴.

¹ Веб-сторінка. URL: <https://uk.wikipedia.org/wiki/%D0%92%D0%B5%D0%B1-%D1%81%D1%82%D0%BE%D1%80%D1%96%D0%BD%D0%BA%D0%B0>.

² Нєкім К. І. Веб-сайт як комплексний об'єкт цивільних прав // Часопис цивілістики. Спецвип. ІТ-право. 2017. № 26. С. 69–74.

³ Про деякі питання практики вирішення спорів, пов'язаних із захистом прав інтелектуальної власності: постанова Пленуму ВГС України від 17 жовт. 2012 р. URL: <http://zakon3.rada.gov.ua/laws/show/v0012600-12>.

⁴ Постанова Верховного Суду України: від 13 берез. 2018 р. у справі № 918/186/17. URL: <http://www.reyestr.court.gov.ua/Review/72763168>.

Однак не всі акаунти у соціальних мережах по'язані із веб-ринками. Наприклад, акаунти у таких соціальних мережах, як Watsapp, Telegram та інших, які прив'язуються до телефонного номера, існують в рамках мобільних додатків та не відкриваються веб-сторінки. Вони також надають користувачам інші можливості, призначені для виконання інших функцій, тобто мають свою ідентифікацію, яка має бути врахована і при розробці особливостей правового регулювання пов'язаних із ними відносин. Наприклад, годні є поширеними об'яви щодо продажу акаунтів у соціальних мережах – як у Фейсбуці, так і у Вайбері, але якщо припустити можливість їх продажу (яку ми розглянемо далі), то оформлення відносин купівлі-продажу того чи іншого акаунту буде мати особливості.

Таким чином, акаунти в соціальних мережах мають складну та відмінну один від одного структуру, яка залежить від можливостей, що надаються тією чи іншою платформою. Спробуємо визначити, які елементи можна виділити в структурі акаунту в певній соціальній мережі, як, наприклад, Facebook. Перш за все, як зазначалось, ім'я та пароль як спосіб авторизації користувача; по-друге, це інформація, яка розміщується на своїй особистій сторінці користувачем. Це можуть бути як чужі твори, тоді при їх використанні користувач зобов'язаний не порушувати авторських прав, так і власні твори користувача, тоді вони підпадають під охорону авторським правом. Щоправда, для користувачів деяких соціальних мереж, зокрема і Facebook, їх розробники встановлюють певні внутрішні правила, які надають їм права користування всіма творами, що розміщується користувачами. Говорячи про такі неосяжні можливості, розробників соціальних мереж, які дозволяють їм, в тому числі, блокувати чи видалити акаунт, в контексті прав користування на їхні акаунти як цифрові об'єкти та відповідно об'єкти віртуальної власності, Пржемыслав Палка зазначає про так звану «цифрову силу» (digital force)¹. Це своєрідне встановлене внутрішніми правилами користування соціальними мережами право їх розробників, яке надає їм повноваження контролю та навіть розпоряджатися акаунтами користувачів і яке, слід вказати, останнім часом широко критикується, особливо в контексті можливостей деяких компаній видалити акаунти у випадку їх тривалого невикористання або смерті користувача. Ще одним елементом, який можна виділити в структурі акаунту, є листування, яке ведеться користувачем та, очевидно, має підпадати під загальні правила про таємницю листування, закріплені у ст. 31 Конституції України, ст. 163 ЦК України.

¹ Przemyslaw Palka. Virtual property: towards a general theory. URL: http://cad.eui.eu/bitstream/handle/1814/49664/Palka_2017.pdf?sequence=1&isAllowed=y.

тощо. Крім того, акаунт нерозривно пов'язаний із особистими даними користувача, які ним вказуються, а тут вже виникає питання захисту персональних даних. До таких відповідно до ст. 2 Закону України «Про захист персональних даних» відносяться відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Деталізацію того, які саме відомості щодо фізичної особи сьогодні підпадають під особливий захист, можна знайти у нещодавно прийнятому, але дуже резонансному акті – General Data Protection Regulation (GDPR)¹, в якому визначено, що до таких відомостей слід, зокрема, відносити ім'я, електронну адресу, місцезнаходження людини, стать, професію та інші (значну частину з них більшість людей вказує під час реєстрації в соціальних мережах).

Таким чином, у правовому регулюванні відносин, пов'язаних із акаунтами, перетинаються норми договірного права (правила користування акаунтами, розроблені соціальною мережею), права інтелектуальної власності, положення про захист приватності особи, майнові права. З урахуванням вказаного, пропонуємо розрізняти правовий режим окремих елементів акаунту та спробуємо визначити правовий режим акаунту у цілому, відповідаючи на питання, чи може він бути розглянутий як об'єкт особливого різновиду права власності (права віртуальної власності) та бути об'єктом правочинів, спрямованих на його відчуження/ передачу в користування третім особам.

Перш за все, увагу привертають ті самі персональні дані, які вказуються володільцем акаунту, з точки зору можливостей їх продажу (у складі акаунту чи окремо). Сьогодні в Європі це питання широко дискутується. Прийняття GDPR з визначенням у цьому акті деяких повноважень володільців персональних даних, зокрема можливості отримувати копії своїх даних, передавати дані від одного контролера до іншого, вимагати їх знищення тощо (ст. ст. 17, 20, 26 GDPR), дало підстави деяким дослідникам вважати, що тим самим підтверджується той факт, що персональні дані можна визначати різновидом власності, оскільки вказані повноваження аналогічні повноваженням власника з користування, розпорядження, отримання доходів від належного їм нематеріального блага².

¹ Regulation EU 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 45/46/EC (General Data Protection Regulation). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>.

² My data are mine. Why we should have ownership rights on our personal data: report. URL: <https://www.generationlibre.eu/wp-content/uploads/2018/01/Rapport-Data-2018-EN-v2.pdf>.

Проте така позиція, відповідно до якої персональні дані розглядаються як різновид власності, піддається критиці. Так, французький юрист Ліонел Маурел у своєму блозі зазначає, що у вказаному дослідженні деякі повноваження, що надаються користувачам, помилково прирівнюються до форми приватної власності. Між тим цей термін не використовується у Регламенті, у якому дані захищаються як атрибут особи, а не різновид майна. Разом із тим формулювання GDPR породжують питання про можливість продажу персональних даних третій особі і про те, чи можна вважати такі правочини дійсними. Автор пропонує проаналізувати ситуацію, коли людина хоче продати свої особисті дані третій особі, що, на його думку, є можливим на підставі ст. 6 GDPR, згідно з якою «обробка законна лише в тому випадку, якщо суб'єкт погодився на обробку своїх персональних даних», відповідно, цікавлений у такій обробці суб'єкт може бути готовим сплачувати кошти за надання згоди на обробку. Однак у зазначеній статті вказано, що згода дається «для однієї або кількох певних цілей». Отже, на відміну від продажу товару, що припускає реальну передачу права власності, компанія, яка збирає персональні дані, буде зобов'язана вказувати цілі, з якими вони передаються. Таким чином, на думку автора, така ситуація вже скоріше нагадує не півлю-продаж, а надання певної ліцензії, схожої з наданням ліцензії зволу у питаннях, пов'язаних із авторськими правами, але таке порівняння теж не зовсім актуальне, оскільки цесія прав третій особі є неможливою з точки зору особистих даних. Крім того, згідно з GDPR, користувач може відізвати свою згоду в будь-який час, що є неможливим у випадку передачі авторських прав. Отже, не відбувалася б не купівля чи поступка, а скоріше оренда, причому дуже ненадійна, оскільки вона може бути в будь-який момент відізнана. Такі обмеження ускладнюють для покупця і перепродаж третім особам, навіть якщо дані були передані з цією метою, оскільки треті особи повинні знову ж таки фіксувати цілі передачі даних і отримувати згоду користувача, повертаючись до нього. Такий логічний отримання згоди для перепродажу в цілому не є неможливим, але його складно забезпечити з точки зору забезпечення безпеки операцій. Тому в США, наприклад, вже існують компанії, які позиціонують себе як «брокери персональних даних» та виступають посередниками між особами, які довіряють їм свої дані, та третіми особами, які бажають їх придбати. Така модель не є неможливою в рамках GDPR, однак посередник повинен буде кожного разу отримувати згоду фізичної особи на кожну транзакцію, вказуючи його точні цілі, для досягнення яких третя особа бажає отримати його дані. Однак якщо врахувати концепцію «вільної згоди», у трак

ванні якої є тенденція розуміти згоду як «безумовну», а отже, не пов'язану ані з застосуванням санкцій, ані з виплатою винагороди, то можна дійти висновку, що у випадку, якщо таке трактування буде офіційно прийняте, навіть за наявності згоди особи на використання третьою особою її персональних даних, вона не зможе їх передати за винагороду, такий правочин буде вважатися недійсним. Отже, такий підхід буде рівнозначним твердженню, що персональні дані знаходяться «поза торгівлею» та не можуть бути перетворені на товари¹.

Зазначимо, що питання, чи може бути право власності на персональні дані в українських реаліях, відсилає до давньої дискусії про право власності на інформацію (оскільки персональні дані є різновидом інформації). На сьогодні відповідь на це питання негативна, інформація розглядається як окремий об'єкт цивільних прав, і на відносини щодо інформації не поширюються норми про право власності.

Проти розуміння інформації як різновиду власності виступають й англійські дослідники. Так, колишній суддя апеляційного суду Дж. Маммері у своїй роботі «Property in the Information Age», аналізуючи справу *Fairstar Heavy Transport NV v Adkins* щодо можливості заявляти вимоги власника на зміст електронних ділових листів, які зберігалися в комп'ютері відповідача, та низку інших справ стосовно інформації, доходить висновку про неможливість вважати інформацію різновидом власності. Він не виключає можливість поширення правового режиму власності на інформацію в майбутньому, але на сьогодні не бачить для цього підстав. (У якості єдиного виключення наводиться справа *Tiscows v Renner*, де предметом судового розгляду було недобросовісне використання доменного імені. Справу було вирішено на користь позивача, при цьому було зазначено, що доменне ім'я є особистою власністю, частиною нематеріальних активів (*intangible property*) позивача і більше, ніж просто інформація². Цей висновок є важливим у контексті нашого дослідження, тому вважаємо за необхідне відзначити його).

Проміжну позицію у питанні співвідношення власності та інформації займає П. Палка. Він висловлює слушну думку про необхідність розрізняти інформацію (*data*) як форму та інформацію як зміст. Автор підкреслює відмінності між цифровою формою (як електронна книга замість реальної (*tangible*) книги) та інформації-

¹ Le RGPD interdit-il aux individus de «vendre» leurs données personnelles? URL: <https://scinfolex.com/2018/05/12/le-rgpd-interdit-il-aux-individus-de-vendre-leurs-donnees-personnelles>.

² John Mummery. *Property in Information Age* in Barr (ed) // *Modern studies in Property Law*. Bloomsbury, 2015. Vol. 8.

єю як знанням, яке може зберігатися у матеріальній формі, наприклад на папері. Аналізуючи в такому світлі роботу Дж. Мамме П. Палка зазначає, що якщо припустити, що наведена справа про витребування інформації, що містилася в електронних листах, має місце років 30 тому, то в ній ішлося б не про витребування інформації, а про витребування паперових листів, тобто матеріальних предметів, які знаходяться у чужому володінні, а питання про інформацію, яка є змістом цих паперових листів, взагалі б не піднімалося. Проблема виникає тому, що електронні листи одночасно вміщують інформацію, і самі по собі є інформацією у тому сенсі, що складаються з бітів, тобто існують як інформація, але в сенсі «інформаційної технології», а не «інформаційної асиметрії»¹. (Інформаційна асиметрія – це ситуація, при якій одна з груп учасників ринку володіє необхідною для ведення своїх справ інформацією, а інша не володіє)². Отже, інформація сьогодні має подвійну природу і може розглядатися і як зміст, і як носій, тобто форма. І якщо питання про «право власності» на інформацію як знання (тобто персональні дані) сьогодні ще є об'єктом дискусій, яким чином це питання не було вирішено, слід розрізняти власність на інформацію як знання та власність на цифрові об'єкти, які тільки за своєю формою є інформацією.

Керуючись зазначеним підходом, візьмемо на себе сміливість дійти висновку про можливість розглядати акаунти як форму зберігання інформації, таку саму, як паперову. Тут можна провести також аналогію між письмовою та електронною формою документів, письмовою та електронною формою правочинів. Так, певний час існувала невизначеність у розумінні правової природи електронного правочину, але сьогодні електронна форма правочину прирівняна до письмової (ст. 205 ЦК України). Поняття електронного документа сьогодні також є достатньо поширеним та досить детально врегульовується на нормативному рівні. Зокрема, відповідно до ст. 5 Закону України «Про електронні документи та електронний документообіг», електронний документ – це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа. При цьому, відповідно до ст. 1 Закону України «Про інформацію», документ – це матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі. З цих визначень випливає, що електронний документ сьогодні визнається різновидом документу.

¹ *Przemyslaw Palka*. Virtual property: towards a general theory. URL: http://cadmus.eui.eu/bitstream/handle/1814/49664/Palka_2017.pdf?sequence=1&isAllowed=y.

² *Информационная асимметрия*. URL: <http://www.economicportal.ru/ponyatiya-informaconnaya-assimetriya.html>.

тобто також є матеріальним носієм інформації, з тією лише різницею, що інформація в електронному документі зафіксована у вигляді електронних даних.

Так само і акаунт можна розглядати як цифровий об'єкт, особливий об'єкт права власності (можливо, особливого різновиду права власності — права віртуальної власності) за аналогією з матеріальними носіями інформації. На користь такого висновку слугує й розуміння правової природи доменних імен, яке сьогодні сформувалося у світовій практиці (див. вказану вище позицію англійських судів щодо розуміння доменного імені як різновиду майна, справу *Kremen v. Cohen*, яка демонструє розуміння доменного імені як особистої власності у судовій практиці США, справу *Raeffgen GmbH v. Germany*, розглянуту ЄСПЛ, яка ілюструє можливість розуміння доменного імені як об'єкта права власності в значенні ст. 1 Протоколу №1 до Конвенції про захист прав людини і основних свобод)¹. Якщо визнати за акаунтом економічну цінність (а вона існує, оскільки якщо існує попит на акаунти, то існує й корисність товару) та, відповідно, об'єктом права власності у значенні ст. 1 Протоколу № 1 до Конвенції про захист прав людини і основних свобод, це дозволить володільцям акаунтів укладати правочини, спрямовані на відчуження/передачу в користування особистих акаунтів. Щоправда, тут виникає проблема визначення долі таких його елементів, як персональні дані та листування. На сьогодні відчуження персональних даних видається неможливим, тому при передачі акаунту персональні дані, листування та інша інформація особистого характеру підлягатимуть видаленню. Та й взагалі при укладенні договору, спрямованого на відчуження акаунту, з урахуванням його комплексного характеру, варто вказувати долю всіх його окремих елементів (що саме передається у складі акаунту) за аналогією з відчуженням веб-сайтів.

Слід зазначити, що сьогодні спори, пов'язані із правами на акаунти в соціальних мережах, є досить поширеними у судовій практиці США. Більшість з них пов'язані із так званими бізнес-акаунтами, тобто профілями компаній, які створюються та ведуться їхніми найманими працівниками, відповідно, у випадках звільнення останніх виникає питання, кому належить акаунт. Наприклад, справа *Phonedog v. Kravitz* пов'язана із тим, що після того, як відповідач, який займався SMM компанії був звільнений, він залишив за собою акаунт компанії в Twitter із 17 тис. підписників, просто

¹ *Некім К. Г.* Доменне ім'я як об'єкт цивільних прав // Часопис цивілістики. 2017. № 23. С. 40–45; *Правовий статус криптовалют в Україні та у світі* // Юридичний науковий електронний журнал. 2018. № 1. С. 40–42. URL: http://lscj.org.ua/1_2018/12.pdf.

змінивши назву акаунту, додавши своє ім'я. У справі *Eagle v. Morgan* предметом судового розгляду стали вимоги, пов'язані з використанням профілю позивача в *LinkedIn*. Суть справи зводиться до того, що, будучи власником компанії, позивачка створила акаунт в *LinkedIn* для професійних та особистих цілей. Пізніше її компанія була викуплена іншою, а позивачка заміненa іншим менеджером. При цьому нові власники компанії отримали доступ до профілю позивачки, змінили пароль та замінили її фото та ім'я даними нового менеджера. Але при цьому в профілі залишилася деяка професійна інформація позивачки, включаючи контакти. На цій підставі позивачка звернулася до суду із 11 вимогами, серед яких викрадення особистості (*identity theft*). У справі *Ardis Health, LLC v. Nankivell* проблема була пов'язана із тим, що відповідач, який займався SMM позивача, після залишення компанії відмовлявся надати доступ до акаунтів компанії. Але суд примусив його зробити це, оскільки відповідачем було підписано угоду про те, що інформація з акаунтів належить позивачеві.

Таким чином, у ситуаціях, коли може виникнути спір між компанією і найманими працівниками щодо акаунтів компаній, варто письмово прописувати, кому належать права на окремі елементи акаунту в соціальній мережі – щодо профілю, доступу, змісту, підписників¹. Можна також дати пораду компаніям розробляти власну політику щодо соціальних мереж із передбаченням всіх можливих наслідків, пов'язаних із правами на акаунти компанії в соціальних мережах.

Щодо сучасних українських реалій, то сьогодні ми можемо зустріти кину пропозицій купити/продати акаунт у соціальній мережі, а також і рекомендацій, як це зробити, але тут важко говорити про правове регулювання.

Наприклад, здійснювати купівлю каналу в Телеграмі (продаж яких сьогодні набуває все більшого поширення, а вартість може бути досить високою) рекомендують за участі посередника (гаранта). Схема передачі прав на акаунт при цьому виглядає наступним чином: сторони обирають гаранта, якому обидві довіряють, володільць каналу видає всі особисті дані, контакти та листування, покупець переводить оплату на рахунок гаранта, продавець після зарахування оплати гаранту переносить доступ до акаунту на номер нового володільця, покупець перевіряє активні сесії, після підтвердження покупцем доступу до облікового запису гарант відправ

¹ *David Lizerbram*. A Legal Perspective: Who Owns Social Media Profiles? URL: <https://blog.marketo.com/2012/08/a-legal-perspective-who-owns-social-media-profiles.html>.

ляє гроші продавцеві¹. Тут важливо пам'ятати, що Телеграм-канали (як і акаунти у Вайбері тощо) прив'язані до телефонних номерів та SIM-карт, тому передача каналу тягне передачу SIM-карти, при цьому для надійності рекомендують здійснювати і фізичну передачу самої SIM-карти покупцеві акаунту. В цьому полягає ключова відмінність продажу акаунтів у соціальних мережах типу Facebook та Instagram від акаунтів, привязаних до телефонних номерів.

Слід також зазначити, що такі схеми важко піддаються правовій кваліфікації, що невід'ємно потягне проблеми, якщо справа дійде до суду. Як зазначає Д. Гадомський, у випадку продажу Телеграм-каналу немає сенсу укладати звичайний договір купівлі-продажу, оскільки важко ідентифікувати володільця каналу, а це позбавляє справу будь-яких судових перспектив. Тим не менш юрист рекомендує у таких випадках укладати тристоронній договір із залученням ескроу-агента, в якому описати процедуру заміни SIM-карти, ризик надто швидкої втрати підписників, гарантії на випадок втрати контролю над каналом з причини зловмисних дій продавця тощо. Крім того, рекомендується передбачити умову про персональні дані, оскільки продавцю можуть бути відомі номери телефонів підписників, а іноді їх імена².

Вказані зауваження видаються слушними з точки зору тимчасового вирішення проблеми, але очевидно є необхідність визначення правової природи акаунтів як різновиду майна, цифрових об'єктів, об'єктів права власності/віртуальної власності, що зробить можливим їх офіційне введення у цивільний обіг з можливістю судового захисту правочинів, що з ними проводяться.

Ще одним нагальним питанням сьогодення, пов'язаним із акаунтами у соціальних мережах, є питання про визначення їх долі після смерті користувача.

Потреба вирішення цього питання призвела до того, що внутрішніми правилами користування багатьох пошукових систем або соціальних мереж було визначено порядок дій з акаунтами на випадок смерті їх володільців, де наслідки визначаються самими користувачами або системою (наприклад, Yahoo! передбачає видалення акаунту у випадку смерті користувача, тоді як Facebook надає користувачам можливість розпорядитися своїм акаунтом на випадок смерті).

Але відомі вже й випадки втручання держави у правове регулювання спадкування акаунтів. Першим прецедентом стало прийнят-

¹ Інструкція: как продать и купить канал в Телеграмме. URL: <https://ru.telegram-store.com/blog/kak-prodat-i-kupit-kanal-v-telegramme>.

² Санитон М. Хочу завести Telegram-канал. С чего начать? URL: <https://ain.ua/2018/03/15/ya-reshil-zavesti-telegram-kanal>.

тя в 2014 році в штаті Делавер закону щодо фідучіарного доступу до цифрового майна (digital assets) та цифрових акаунтів. Вказаний акт під цифровим акаунтом розуміє електронну систему для створення, генерування, відправлення, поширення, спілкування, отримання, зберігання, відображення, обробки інформації, який надає доступ до цифрового майна, що існує або може існувати, який зберігається на будь-якому цифровому пристрої незалежно від власності на такий цифровий пристрій, на якому цифрове майно зберігається, у тому числі, e-mail акаунти, акаунти в соціальних мережах, страхові, фінансові, податкові та інші акаунти. Цифрове майно цей акт визначає як інформацію, тексти, електронні листи, документи, аудіо, відео, зображення, контент соціальних мереж, записи про стан здоров'я, про страхування, комп'ютерні програми, ліцензії, бази даних, у тому числі імена користувачів та паролі, що створені, згенеровані, відіслані, отримані, поширені або збережені за допомогою електронних засобів або цифрових пристроїв. Закон дозволяє призначити фідучіарія (особистого представника, передбаченого заповітом), який контролюватиме акаунти померлого та його цифрове майно та може передати доступ до них визначеному члену сім'ї померлого¹.

Пізніше, у 2015 році, у більшості штатів США було введено дію аналогічний акт – щодо фідучіарного доступу до цифрових акаунтів. Вказаний акт дозволяє визначити у заповіті, що виконавець заповіту може мати доступ до електронної пошти та акаунтів у соціальних мережах померлого. Закон не визначає, і ще не складалася судова практика з цього питання, як саме має відбуватися цей доступ. Тому на сьогодні ситуація складається таким чином: виконавець повинен зв'язатися з компаніями по кожній цифровій платформі, щоб визначити, як отримати доступ до акаунту померлого. По суті закон використовує конструкцію трасту на випадки розпорядження цифровим майном померлого. Так, відповідно до закону, виконавцем волі померлого щодо цифрового майна є траст – фідучіарій, що має легальний титул на майно згідно з угодою або декларацією³. «Цифровим виконавцем» може бути особа відмінна від виконавця щодо реального майна⁴.

¹ An Act to Amend Title 12 of the Delaware Code Relating to Fiduciary Access to Digital Assets and Digital Accounts. URL: <https://legiscan.com/DE/text/HB345/id/102350>.

² Estate planning for your digital assets. URL: <https://theconversation.com/estate-planning-for-your-digital-assets-90613>.

³ Revised Uniform Fiduciary Access to Digital Assets Act. URL: http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2015_RUFAA_Final%20Act_2016mar8.pdf.

⁴ How to deal with your online accounts before you die. URL: <https://www.cnn.com/how-to/5-steps-to-settle-your-digital-affairs>.

У таких штатах, в яких закон не прийнято, компанії самі вирішують, чи надавати родичам доступ до цифрових акаунтів померлого члена сім'ї. Наприклад, Yahoo, як зазначалось, наполягає на закритті акаунтів у випадку смерті користувачів із заборобою подальшого доступу до них. Така ситуація породила судовий спір у штаті Масачусетс (в якому не прийнято закон про цифрові акаунти), і в жовтні 2017 року Верховний суд штату Масачусетс постановив, що все ж таки виконавець повинен мати доступ до акаунтів померлого, чийм майном він управляє. Справа була повернута до суду першої інстанції для уточнення кількох питань, у тому числі чи можливим є доступ виконавця до акаунту померлого, незважаючи на умови угоди користувачів Yahoo¹. Критика цих умов (які між тим визнаються формою контракту, який зв'язує сторони зобов'язанням) зводиться до того, що є несправедливою встановлена умовами можливість платформи видаляти електронні листи, які знаходяться в її володінні, але належать користувачеві (тим самим не прямо визнається факт, що користувач є власником електронних листів, а платформа їх володільцем).

Практика визнання можливості спадкування акаунтів складається на сьогодні і в Європі. Так, нещодавно Верховний Суд Німеччини дозволив передавати у спадок акаунти в Facebook. Згідно з рішенням суду, усі дані акаунтів у соціальних мережах, у тому числі медіафайли та особисте листування, слід прирівнювати до щоденників та листів, передача у спадок яких прописана у німецькому законодавстві. Суд зазначив у своєму рішенні, що акаунт користувача в соціальній мережі передається спадкоємцям власника акаунту, а спадкоємці можуть зажадати від оператора мережі надати їм доступ до акаунту, в тому числі до даних, що стосуються спілкування користувача в соціальній мережі. До цього рішення Facebook надавав рідним померлого можливість повністю видалити акаунт або перетворити акаунт у цифровий меморіал, що дає можливість користувачам залишати співчуття. Доступу до листування померлого соціальна мережа не надавала².

¹ Marianne Ajemian, coadministrator and others v Yahoo!, inc. URL: <https://www.mass.gov/files/documents/2017/10/16/12237.pdf>.

² Верховний суд Німеччини дозволив передавати у спадок акаунти у Facebook. URL: https://medium.com/@jur_blog/%D0%B2%D0%B5%D1%80%D1%85%D0%BE%D0%B2%D0%BD%D0%B8%D0%B9-%D1%81%D1%83%D0%B4-%D0%BD%D1%96%D0%BC%D0%B5%D1%87%D1%87%D0%B8%D0%BD%D0%B8-%D0%B4%D0%BE%D0%B7%D0%B2%D0%BE%D0%BB%D0%B8%D0%B2-%D0%B%D0%B5%D1%80%D0%B5%D0%B4%D0%B0%D0%B2%D0%B0%D1%82%D0%B8-%D1%83%D1%81%D0%BF%D0%B0%D0%B4%D0%BE%D0%BA-%D0%B0%D0%BA%D0%B0%D1%83%D0%BD%D1%82%D0%B8-%D0%B2-facebook-5a4f72f14946.

Отже, ситуація аналогічна тій, що існує на сьогодні в США – родичі повинні звертатися до операторів соціальних мереж з вимогою надати доступ до акаунту померлого члена сім'ї, і соціальні мережі повинні надавати такий доступ. Зазначимо також, що описані ситуації стосуються в основному лише такого елемента акаунтів, як листування, і не вирішують проблеми введення акаунтів у цивільний обіг як окремих самотійних об'єктів.

Сьогодні вже зустрічаються і істотні теоретичні дослідження проблеми можливості спадкування цифрового майна, у яких піднімається низка важливих питань. Так, англійські дослідники Х. Конвей та Ш. Греттен, аналізуючи проблеми дій з цифровим майном на випадок смерті, зазначають, що основною проблемою при спадкуванні цифрового майна є відсутність визначення поняття цифрове майно. Відомі тільки об'єкти, які за загальним правилом відносять до цифрового майна, і ці об'єкти є дуже різнорідними – це електронні листи і електронні скриньки, блоги, акаунти та профілі у соціальних мережах, цифрова музика, репозитарії цифрових фото та відео, банківські акаунти та інші фінансові інструменти, а також онлайн підписки на журнали, акаунти на Amazon, профілі продавців на eBay, доменні імена тощо. По суті будь-які файли, що зберігаються або створюються на цифрових пристроях, є цифровим майном. Проблеми, пов'язані з цим, зводяться до того, що, по-перше, це практично нескінченний перелік речей, що можуть складати цифрове майно; по-друге, цінність кожного виду цифрового майна буде істотно відрізнятися від іншого: деякі з них, як банківські акаунти та фінансові інструменти, доменні імена, будуть мати очевидну грошову цінність, тоді як інші, такі як фотографії, електронні листи, листування у соціальних мережах, будуть мати лише емоційну або сентиментальну цінність для родичів померлого користувача. Це породжує проблему необхідності категоризації об'єктів, які вважаються цифровим майном. У якості найбільш фундаментального критерію класифікації видів цифрового майна автори пропонують використовувати критерій, чи є таке майно власністю, чи ні, оскільки очевидно, що не все цифрове майно є власністю у традиційному розумінні. Чи буде виступати цифрове майно об'єктом власності, на думку дослідників, залежатиме ще й від умов угоди користувача, яка може розглядати цифрове майно як окремий об'єкт власності, який може передаватися, або відносини можуть будуватися як суто ліцензійна угода, яка закінчується у зв'язку зі смертю користувача. Отже, цифрове майно відрізняє від традиційного майна те, що володілець акаунту (особа, яку ми можемо кваліфікувати як власника) не обов'язково контролює кінцеву долю цього майна. Спроби заповідати таке май-

но (або авторизувати доступ) ігноруватимуть приватну угоду з провайдером, яка може забороняти це¹. Таким чином, доля цифрового майна напряду залежить від умов угоди користувача, яка може залишати за оператором соціальної мережі право розпорядитися цим майном. І це не суперечить загальним принципам договірних прав, оскільки користувачі погоджуються на ці умови, підписуючи угоду. Проте автори у своїй статті зазначають, що ще не відомим є ставлення суду до цього, і, як ми можемо бачити з останніх справ, що мали місце у судах США та Німеччини, суди все ж таки схиляються до надання переваги захисту зацікавлених осіб, тому можемо припустити, що у майбутньому деякі положення угод користувачів, що забороняють передачу доступу до акаунтів або надають можливість розпорядження ними самим операторам соціальних мереж, будуть визнані дискримінаційними та заборонені.

У доктрині сьогодні висловлюється думка, що стосовно цифрового майна закон має надавати ті самі права та свободи, що й стосовно інших форм власності, що індивідуум повинен мати право визначати долю свого цифрового майна, однак тут слід враховувати той факт, що не всі об'єкти цифрового майна можуть бути прирівняні до власності, крім того, деякі з них, навіть за умови визнання їх власністю, не можуть бути передані². Проте, незважаючи на велику кількість питань, що потребують відповідей у цій сфері, дослідники пропонують подбати про долю свого цифрового майна за життя шляхом включення положень про визначення його долі у заповіт, з урахуванням, однак, положень угоди користувача та в її межах. Пропонується також призначити окремо «цифрового виконавця», який буде, крім іншого, освіченим у сфері комп'ютерних технологій³.

Зазначимо, що сьогодні Європейським інститутом права спільно з дослідниками із США створено робочу групу щодо вивчення можливості використання американського закону про фідуціарний доступ до цифрового майна як моделі для європейського законодавства⁴. Вказане свідчить про необхідність врахування останніх тенденцій і в Україні. З цією метою цілком допустимо звернутися до інституту довірчої власності, який існує в нашій країні вже досить тривалий час, та передбачити можливість призначення довірчого власника виконавцем заповідальних розпоряджень щодо

¹ Heather Conway and Sheena Grattan. The «New» New Property: Dealing with Digital Assets on Death in Barr (ed) // Modern studies in Property Law. Bloomsbury, 2017. Vol. 9. P. 100–103.

² Там само. P. 104.

³ Там само. P. 111.

⁴ Там само. P. 113.

цифрового майна, зокрема акаунтів та їх контенту. Актуальність використання моделі саме довірчої власності, а не призначення виконавця заповіту згідно з нормами спадкового права пояснюється, по-перше, тим, що такий підхід є більш близьким до світової практики, по-друге, тим, що в рамках інституту довірчої власності краще прописується відповідальність довірчого власника перед бенефіціаріями, але це вже може бути предметом окремої дискусії.

ПРАВОВИЙ СТАТУС РЕКЛАМИ В СОЦІАЛЬНИХ МЕРЕЖАХ

Розвиток Інтернету в найближчому майбутньому перетворить мережу в стандартний канал соціальних комунікацій, за яким будуть здійснюватися переважна кількість роздрібних торгових операцій, переказ грошових коштів, будуть виконуватися всі функції зв'язку і мовлення засобів масової інформації. Виникнуть нові соціальні групи, нова ідеологія, сформується новий психологічний образ жителя планети ХХІ століття¹.

Як відомо, під твердженням «Інтернет не має кордонів» більшість користувачів Мережі мають на увазі неможливість визначення, законодавству якої держави підпорядковується Всесвітня комп'ютерна мережа, проте це, насправді, далеко не так. У дійсності Інтернет знає, що таке «кордони», які при цьому досить чіткі.

Канал соціальних комунікацій зараз можна використовувати і як ресурс для розвитку, і як засіб для здійснення антисоціальних дій. При відсутності норм, що регулюють дії користувачів, організацій і держав, в Інтернеті виникає і міцно закріплюється у свідомості подвійний стандарт: закони повинні дотримуватися, але тільки не в мережі.

Одна з причин, яка може призвести до небезпечних тенденцій, – права.

До правомірних причин відносяться вже раніше відома недостатність правового регулювання, а також концептуальна складність забезпечення доказів у мережі. Нині, наприклад, з точки зору кримінального законодавства, будь-який український сегмент в Інтернеті є конгломератом кримінально караних діянь у формі наклепу і образ, що зустрічаються всюди і скрізь на просторах Інтернету, завідомо неправдивої реклами, у вигляді поширення пор-

¹ Інформаційні технології як фактор суспільних перетворень в Україні: зб. аналіт. доп. / М. А. Ожеван, С. Л. Гнатюк, Т. О. Ісакова; за заг. ред. Д. В. Дубова. Київ: НІСД, 2011. 96 с.

нографічних матеріалів, порушення прав на об'єкти інтелектуальної власності.

У сучасному світі інформаційних технологій Інтернет-простір стає основним полем битви за клієнта, а найактивніші дії ведуться на фронтах соціальних мереж. Тому не дивно, що питання, пов'язані з проведенням рекламних кампаній у Facebook, Twitter і LinkedIn, набувають все більшої актуальності.

Чи є конкретне повідомлення рекламою або ж чимось іншим – одине з принципових питань для рекламодавців, особливо для тих, хто просуває свої товари або послуги в Інтернеті, оскільки вимоги Закону України «Про рекламу» застосовуються тільки до такої інформації, яка відповідають визначенню «реклами».

Реклама в Інтернеті на сьогоднішній день є одним з найбільш ефективних способів поширення інформації та її доведення до споживача. Однак використовуючи цей засіб, компаніям необхідно пам'ятати про те, що сфера дії Закону України «Про рекламу» в повній мірі поширюється і на інтернет-рекламу.

Відповідно до ст. 1 Закону України «Про рекламу», «реклама – інформація про особу чи товар, розповсюджена в будь-якій формі та в будь-який спосіб і призначена сформулювати або підтримати обізнаність споживачів реклами та їх інтерес щодо таких особи чи товару». Як впливає з наведеного вище визначення, інформаційне повідомлення буде рекламою за умови відповідності трьом ознаками:

- 1) інформація про особу чи товар;
- 2) розповсюджена в будь-якій формі та в будь-який спосіб;
- 3) призначена сформулювати або підтримати обізнаність споживачів реклами.

Формальна невідповідність одній з цих ознак має виключати можливість кваліфікації повідомлення в якості реклами.

Іноді маркетологи цікавляться: якщо не можна рекламувати, наприклад, алкоголь, чи можна просувати сам бренд напою? На практиці така діяльність з просування самого бренда без прив'язки до конкретного товару (або послуги) називається «брендингом». З точки зору Закону України «Про рекламу», в разі брендингу об'єктом рекламування буде не конкретний товар, а засіб індивідуалізації (товарний знак, фірмове найменування тощо).

Як відомо, однією з найбільш ефективних і одночасно складних методик маркетингу є сарафанне радіо або word-of-mouth marketing. Йдеться про передачу інформації про товар одним задоволеним споживачем іншому. Така передача може здійснюватися як в рамках живого спілкування, так і за допомогою Інтернету. В останньому випадку мова йде про призначений для користувача контент (user-generated content).

У першу чергу варто відзначити, що українське законодавство не містить спеціальних норм, що регулюють цей вид реклами. Тому щодо такої реклами будуть застосовуватися загальні принципи, сформульовані в Законі України «Про рекламу», а також норми цивільного законодавства. Найбільш вірогідним сценарієм несумлінної поведінки в контексті сарафанного радіо може бути спроба поширювати позитивні відгуки про товар від імені нібито неупереджених і незалежних споживачів, які насправді є «агентами» виробника.

Іншою поширеною практикою в області сарафанного радіо є замовлення позитивних публікацій про продукт у відомих авторів в Інтернеті (блогерів). У США на таких блогерів покладається обов'язок розкрити факт наявності відносин з особами, які замовлять публікацію. В українському законодавстві такої вимоги немає, хоча воно і може бути виведено із загальних принципів про добросовісну і достовірну рекламу.

У разі визнання конкретного інформаційного повідомлення рекламою виникає закономірне питання про те, хто повинен нести відповідальність за можливі порушення. Згідно зі ст. 27 Закон України «Про рекламу» пропонується три можливих суб'єкта відповідальності:

1) рекламодавці, винні:

- у замовленні реклами продукції, виробництво та/або обіг якої заборонено законом;
- у наданні недостовірної інформації виробнику реклами, необхідної для виробництва реклами;
- у замовленні розповсюдження реклами, забороненої законом;
- у недотриманні встановлених законом вимог щодо змісту реклами;
- у порушенні порядку розповсюдження реклами, якщо реклама розповсюджується ними самостійно;

2) виробники реклами, винні в порушенні прав третіх осіб при виготовленні реклами;

3) розповсюджувачі реклами, винні в порушенні встановленого законодавством порядку розповсюдження та розміщення реклами.

За ст. 1 Закону України «Про рекламу»:

«Рекламодавець – особа, яка є замовником реклами для її виробництва та/або розповсюдження».

«Виробник реклами – особа, яка повністю або частково здійснює виробництво реклами».

«Розповсюджувач реклами – особа, яка здійснює розповсюдження реклами».

Конкретний склад правопорушень, за які несуть відповідальність зазначені вище суб'єкти, визначені в ст. 27 Закону України «Про рекламу». Існують відмінності в режимах відповідальності рекламодавця і розповсюджувача реклами (хоча вони і перетинаються в більшості випадків). Виробник реклами несе відповідальність за будь-які правопорушення, якщо буде доведено, що порушення відбулося з його вини. Суб'єкти можуть залучатися до відповідальності як окремо, так і спільно за одне правопорушення.

З метою захисту інтересів суспільства, держави, споживачів реклами і учасників рекламного ринку державні органи, зазначені у ст. 26 Закону України «Про рекламу», можуть звертатися до суду з позовами про заборону відповідної реклами та її публічне спростування.

Центральний орган виконавчої влади, що реалізує державну політику у сфері державного контролю за дотриманням законодавства про захист прав споживачів, за поданням державних органів, зазначених у ст. 26 Закону України «Про рекламу», або самостійно у випадках, передбачених цією статтею, крім тих, які віднесено виключно до компетенції Антимонопольного комітету України та які регулюються законодавством з питань авторського права та суміжних прав, накладає штрафи у порядку, встановленому Кабінетом Міністрів України, на:

- рекламодавців за вчинення дій, передбачених п. 1 ч. 2 ст. 27 Закону України «Про рекламу», – у розмірі п'ятикратної вартості розповсюдженої реклами;

- виробників реклами за вчинення дій, передбачених п. 2 ч. 2 ст. 27 Закону України «Про рекламу», – у розмірі п'ятикратної вартості виготовлення реклами;

- розповсюджувачів реклами за вчинення дій, передбачених п. 3 ч. 2 ст. 27 Закону України «Про рекламу», – у розмірі п'ятикратної вартості розповсюдження реклами.

Повторне вчинення перелічених порушень протягом року тягне за собою накладення штрафу у подвійному від передбаченого за ці порушення розмірі.

Кожному учаснику ринку реклами варто чітко розуміти свій статус і відповідний такому статусу режим відповідальності. Наприклад, у разі розміщення контекстної і таргетованої реклами в соціальних мережах рекламодавцем буде виробник товару, в той час як соціальна мережа буде розповсюджувачем реклами. Через те, що соціальні мережі несуть самостійну відповідальність, рекламні повідомлення майже завжди проходять перевірку (модерацію) перед тим, як опинитися на просторах мережі¹.

¹ *Kuna O. O.* Правопорушення в мережі Інтернет // Часопис Київського університету права. 2010. № 4. С. 346–350.

Ринок social media marketing в Україні безумовно буде продовжувати зростати, а використовувані методики будуть удосконалюватися. У свою чергу законодавець буде все частіше звертати увагу на цей сегмент реклами. Учасникам ринку варто стежити за розвитком практики і адаптувати свої рекламні кампанії з урахуванням вимог законодавства.

Не є рекламою в Інтернеті:

1. Інформація про виготовлення і реалізацію товарів, розміщена на сайті виробника або продавця товарів або на сторінках в соціальних мережах, якщо зазначені відомості призначені для інформування відвідувачів сайта або сторінки в соціальній мережі про реалізовані товари, асортимент, правила користування (алкогольні компанії можуть зітхнути спокійно – на своїх сайтах їм можна публікувати асортимент і іншу інформацію).

Приклади: компанія, що реалізує побутові товари, розміщує у себе на сайті каталог, фото товарів, їх опис і ціну – Закон України «Про рекламу» на цю інформацію не поширюється; ця ж компанія розміщує свій банер на іншому сайті – Закон «Про рекламу» поширюється і на рекламодавця, і на розповсюджувача реклами.

2. Інформація про знижки або акції, розміщена на сайтах-агрегаторах (на сайтах, де акумулюються і пропонуються різні купони або квитки, що дозволяють придбати товар зі знижкою). Приклади: сайти знижок, Покупон. Дана позиція достатньо спірна: за такою логікою, слід виводити з-під дії Закону України про рекламу і спеціалізовані рекламні офлайн-видання.

Швидше за все, комісія, отримавши скаргу щодо порушення законодавства в представлений на такому сайті рекламі все-таки буде розглядати її по суті, виявляючи конкретного рекламодавця і притягуючи до відповідальності саме його.

3. Результати пошукової видачі не є рекламою і не регулюються законодавством про рекламу, тому що така інформація є результатом обробки пошукового запиту користувача і не спрямована на формування і підтримку інтересу до якого-небудь товару.

Є рекламою в Інтернеті: інформація на сайті рекламодавця або в його групі в соціальній мережі, спрямована на привертання особливої уваги до конкретного товару і його виділення серед однорідних товарів (наприклад, спливає банер); контекстна реклама (Яндекс.Директ і аналогічні).

Стосовно правового регулювання відеореклами в соціальній мережі, то українське законодавство не дає легального визначення відеореклами в Інтернеті¹.

¹ Єфремова К. В. До перспектив правового регулювання інтернет-правовідно-

Однак, з практичної точки зору, відеорекламою в Інтернеті є показ рекламного відеоролика зацікавленої аудиторії на різних інтернет-сайтах, що на сьогоднішній день стало реальною альтернативою телевізійній рекламі¹.

На сьогоднішній день видом реклами, що найактивніше розвивається, є саме та реклама, що розміщується у Всесвітній павутині. Швидкий стрибок розвитку мережі, а також практично відсутні накладні витрати на утримання медіаносіїв – безсумнівний плюс.

А ціна, як відомо, найкращий інструмент переконання на сьогодні. Нарешті, Інтернет об'єднав в собі всі звичні форми спілкування зі споживачами, починаючи від друкованого слова і закінчуючи відеороликами. Інтернет-відеореклама активізувала свій стрімкий розвиток в 2007 році в зарубіжному Інтернеті, коли компанія Google купила Youtube.

Саме тоді величезну популярність отримало онлайн-відео, яке рекламодавці незабаром змогли використати для розміщення відеореклами. В Україні інтернет-відеореклама почала розвиватися трохи пізніше, але темпи настільки ж швидкі, як і за кордоном.

До 2020 року, за прогнозами аналітиків, український ринок інтернет-відеореклами зросте, як мінімум, у 20 разів. Основний сайт, що займається розміщенням відеореклами, – це youtube.com.

Як зазначалось раніше, українське законодавство не дає легального визначення відеореклами в Інтернеті, проте, з практичної точки зору, відеореклама в Інтернеті є показом рекламного відеоролика зацікавленій аудиторії на різних інтернет-сайтах, що на сьогоднішній день стало реальною альтернативою телевізійній рекламі.

Відносини, що виникають в процесі виробництва, розміщення та розповсюдження реклами на ринку товарів, робіт, послуг України, включаючи ринки банківських, страхових та інших послуг, пов'язаних з користуванням грошовими коштами громадян (фізичних осіб) і юридичних осіб, а також ринки цінних паперів, також регулюються Законом України «Про рекламу».

Цілями зазначеного Закону є захист від недобросовісної конкуренції в галузі реклами, запобігання і припинення неналежної реклами, здатної ввести споживачів реклами в оману або завдати шкоди здоров'ю громадян, майну громадян або юридичних осіб, навколишньому середовищу або честі, гідності або діловій репутації зазначених осіб, а також такої реклами, що зазіхає на суспільні інтереси, принципи гуманності і моралі. Закон встановлює:

син: господарсько-правовий аспект // Право та інноваційне суспільство. 2014. № 1. С. 5–11.

¹ Котенко Е. С. Авторские права на мультимедийный продукт: монография. Москва: Прспект, 2013. 123 с.

- загальні та спеціальні вимоги до реклами;
- права та обов'язки рекламодавців, виробників реклами та розповсюджувачів реклами;

- державний контроль і саморегулювання в галузі реклами;
- відповідальність за порушення законодавства про рекламу.

Найбільш важливі загальні вимоги до реклами наступні:

- вона повинна бути доступною для людини без спеціальних знань та без застосування технічних засобів;

- не повинна спонукати громадян до насильства, агресії, на-рошувати паніку, а також спонукати до небезпечних дій, які здатні завдати шкоди здоров'ю фізичних осіб або які загрожують їхній безпеці;

- не повинна спонукати до дій, які порушують природоохоронне законодавство.

Закон вводить поняття «недобросовісна реклама» – реклама, яка вводить або може ввести в оману споживачів реклами, завдати шкоди особам, державі чи суспільству внаслідок неточності, недостовірності, двозначності, перебільшення, замовчування, порушення вимог щодо часу, місця і способу розповсюдження. Недобросовісна реклама забороняється (ч. 1 ст. 10 Закону України «Про рекламу»).

Характеристика недобросовісної реклами:

а) недобросовісною є реклама, яка:

- дискредитує юридичних і фізичних осіб, які не користуються рекламованими товарами;

- містить некоректне порівняння рекламованого товару з товаром (товарами) інших юридичних або фізичних осіб, а також містить висловлювання, образи, що ганьблять честь, гідність чи ділову репутацію конкурента (конкурентів);

- вводить споживачів в оману щодо рекламованого товару за допомогою імітації (копіювання або наслідування) загального проєкту, тексту, рекламних формул, зображень, музичних або звукових ефектів, використовуваних в рекламі інших товарів, або за допомогою зловживання довірою фізичних осіб або браком у них досвіду, знань, в тому числі у зв'язку з відсутністю в рекламі частини істотної інформації;

б) недостовірною є реклама, в якій присутні відомості, що не відповідають дійсності щодо:

- таких характеристик товару, як природа, склад, спосіб і дата виготовлення, призначення, споживчі властивості, умови застосування, наявність сертифіката відповідності, сертифікаційних знаків і знаків відповідності державним стандартам, кількість, місце походження;

- наявності товару на ринку, можливості його придбання в зазначеному обсязі, періоді часу і місці;
- вартості (ціни) товару на момент поширення реклами;
- додаткових умов оплати;
- доставки, обміну, повернення, ремонту і обслуговування товару;
- гарантійних зобов'язань, термінів служби, термінів придатності;
- інформації про самого рекламодавця та інше;

в) неетичною є реклама, яка:

- містить текстову, зорову, звукову інформацію, що порушує загальноприйняті норми гуманності та моралі шляхом вживання образливих слів, порівнянь, образів щодо раси, національності, професії, соціальної категорії, вікової групи, статі, мови, релігійних, філософських, політичних та інших переконань фізичних осіб;

– порочить об'єкти мистецтва, які є національним чи світовим культурним надбанням;

– порочить державні символи (прапори, герби, гімни), національну валюту України чи іншої держави, релігійні символи і ін.;

г) завідомо помилковою є реклама, за допомогою якої рекламодавець (виробник реклами, розповсюджувач реклами) навмисне вводить в оману споживача реклами.

Відповідальність за недобросовісну рекламу несе винна особа (ч. 2 ст. 10 Закону України «Про рекламу»).

Рішення щодо визнання реклами недобросовісною приймають державні органи, визначені у ст. 26 цього Закону України «Про рекламу», а саме:

– центральний орган виконавчої влади, що реалізує державну політику у сфері державного контролю за додержанням законодавства про захист прав споживачів, – щодо захисту прав споживачів реклами;

– Антимонопольний комітет України – щодо дотримання законодавства про захист економічної конкуренції;

– Національна рада України з питань телебачення і радіомовлення – щодо телерадіоорганізацій усіх форм власності;

– центральний орган виконавчої влади, що реалізує державну фінансову політику, – щодо реклами державних цінних паперів;

– Національна комісія з цінних паперів та фондового ринку – щодо реклами на фондовому ринку;

– центральний орган виконавчої влади, що реалізує державну політику у сферах будівництва, архітектури, – щодо спорудження житлового будинку;

– центральний орган виконавчої влади, що реалізує державну політику з питань державного нагляду та контролю за дотриманням

законодавства про зайнятість населення, – щодо реклами про вакансії (прийом на роботу).

Порівняльна реклама – реклама, яка містить порівняння з іншими особами та/або товарами іншої особи.

Відносини, які виникають у зв'язку з порівняльною рекламою, регулюються законодавством України про захист від недобросовісної конкуренції (ч. 1 ст. 11 Закону України «Про рекламу»).

Відповідальність за неправомірне порівняння в рекламі несе рекламодавець.

Рішення щодо визнання порівняння в рекламі неправомірним приймають державні органи, визначені у ст. 26 Закону України «Про рекламу».

Закonom України «Про рекламу» також передбачено і поняття соціальної реклами, під якою розуміється інформація будь-якого виду, розповсюджена в будь-якій формі, яка спрямована на досягнення суспільно корисних цілей, популяризацію загальнолюдських цінностей і розповсюдження якої не має на меті отримання прибутку.

Рекламодавцем соціальної реклами в соціальній мережі може бути будь-яка особа.

Соціальна реклама не повинна містити посилань на конкретний товар та/або його виробника, на рекламодавця (крім випадків, коли рекламодавцем є громадське об'єднання чи благодійна організація), на об'єкти права інтелектуальної власності, що належать виробнику товару або рекламодавцю соціальної реклами, крім реклами національних фільмів.

Реклама національних фільмів прирівнюється до соціальної реклами та може розміщуватися і розповсюджуватися за умови дотримання вимог, встановлених абзацом дванадцятим ч. 1 ст. 8 Закону України «Про рекламу».

На осіб, які безоплатно виробляють і розповсюджують соціальну рекламу, та на осіб, які передають свої майно і кошти іншим особам для виробництва і розповсюдження соціальної реклами, поширюються пільги, передбачені законодавством України для благодійної діяльності.

Засоби масової інформації – розповсюджувачі реклами, діяльність яких повністю або частково фінансується з державного або місцевих бюджетів, зобов'язані розміщувати соціальну рекламу державних органів та органів місцевого самоврядування, громадських організацій безкоштовно в обсязі не менше 5 % ефірного часу, друкованої площі, відведених для реклами, також зобов'язані надавати пільги при розміщенні соціальної реклами, замовником якої є заклади освіти, культури, охорони здоров'я, які утримуються за рахунок державного або місцевих бюджетів, а також благодійні організації.

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ПРАВОВОЇ ОХОРОНИ ЗОБРАЖЕННЯ ЛЮДИНИ У СОЦІАЛЬНИХ МЕРЕЖАХ

З поширенням популярності мережі Інтернет у всьому світі, зі збільшенням кола користувачів отримала своє розповсюдження нова форма спілкування – спілкування у соціальних мережах. Соціальні мережі об'єднують користувачів за спільними інтересами, напрямками діяльності, колом друзів, знайомих тощо. Широкі можливості дозволяють не тільки обмінюватися повідомленнями, але й розмішувати численні об'єкти інтелектуальної власності: фотографії, листівки та інші художні твори, аудіо- та відеозаписи, приватні щоденники тощо. Одним з актуальних питань, що потребує вирішення при вдосконаленні правового регулювання відносин у мережі Інтернет, зокрема у соціальних мережах, є визначення правових засад використання розміщених у мережі персональних даних фізичних осіб, імені та зображення. Ускладнення способів використання зображень фізичної особи завдяки новітнім технологіям створює можливість швидкого та безперешкодного поширення та використання зображення завдяки репосту, хештегу, встановлення відмітки на фотографії про конкретну зображену особу з активним посиланням на її сторінку у соціальній мережі тощо. Зі збільшенням популярності соціальних мереж збільшується кількість й правопорушень в мережі, що у свою чергу потребує вироблення нових дієвих механізмів захисту у віртуальному просторі.

Зображення фізичної особи – це нематеріальне благо, яке виступає безпосередньо чи опосередковано об'єктом особистого права фізичної особи на власне зображення. Поняття «зображення фізичної особи» можна розглядати у двох значеннях. По-перше, як безпосереднє зображення фізичної особи, втілене у людині (її зовнішній вигляд), що доступне для сприйняття оточуючими. По-друге, як зображення зовнішнього обліку фізичної особи, зафіксованого у фотографічному чи іншому художньому творі.

У першому значенні зовнішній вигляд фізичної особи виступає результатом реалізації права на власну індивідуальність (ст. 300 ЦК України) та є особистим немайновим благом фізичної особи. Зазначене благо за своїм характером є немайновим, невідчужуваним, індивідуалізуючим, спрямованим на забезпечення особистої фізичної недоторканності, схильним до якісних змін. На формування зовнішнього вигляду фізичної особи впливають як суб'єктивні, так і об'єктивні фактори, зокрема: родинно-сімейний фактор (генетичне походження, традиційні родинні цінності тощо); особистісно-вольовий (власні прагнення, зусилля тощо); соціальний (визначені стереотипи краси, нормативно-визначені стандарти зовнішнього вигляду, медико-хірургічні можливості щодо зміни зовнішнього вигляду тощо). Змістом права на власний вигляд є право самостійно визначати власний зовнішній вигляд; змінювати його самостійно чи за допомогою третіх осіб; перешкоджати його зміні за визначенням випадків, встановлених законом.

У другому значенні зображення зовнішнього вигляду людини, зафіксоване у фотографічному чи іншому художньому творі, може виступати об'єктом права фізичної особи на власне зображення. Змістом права фізичної особи на власне зображення є право дозволяти створювати твори з власним зображенням (за виключенням випадків, передбачених законом), право зазначати власне ім'я як зображеної особи, право вимагати автентичності власного зображення; право на недоторканність власного зображення. При створенні примірника твору з зображенням людини виникають права, супутні авторським: право на використання матеріального носія твору з власним зображенням; право дозволяти його використання іншим особам та перешкоджати неправомірному використанню. Питання про належність прав, супутніх авторським, вирішується на етапі створення твору. В іншому випадку спори про належність прав, супутніх авторським, вирішуються відповідно до норм чинного законодавства (ст. 308 ЦК України).

Вільне поширення фотографічних та інших художніх творів з зображенням людини відбувається у суспільних інтересах з метою захисту інтересів зображеної особи чи інших осіб, зокрема у випадках: поширення творів з зображенням «публічних» фізичних осіб; творів, виконаних не за замовленням, за умови, що зображення фізичної особи не є основним об'єктом використання; з метою здійснення правосуддя чи суспільної безпеки у випадках, визначених законом або за згодою родичів зображеної особи; при створенні карикатур, пародій та інших творів саркастичного характеру; з інформаційною, культурною або особистою метою. При вільному поширенні творів повинні бути дотримані норми суспільної моралі

(ч. 3 ст. 13, ч. 2 ст. 319 ЦК України); право фізичної особи на конфіденційність інформації (ст. ст. 301, 442 ЦК України), право на честь, гідність, ділову репутацію при поширенні фотографічних та інших художніх творів з зображенням фізичної особи (ст. ст. 297, 299, 442 ЦК України) тощо.

Саме у другому значенні терміна «зображення фізичної особи» здійснюється його захист від неправомірного поширення у мереж Інтернет.

Соціальні мережі створюють можливості як для вільного, так і для обмеженого доступу до зображень особи на її соціальній сторінці, залежно від встановленого нею режиму доступу. Зазначені режими дозволяють визначити ступінь доступу людини до інформації про її особисте життя, окремі як значимі, так і маловажні події. Більшість з соціальних мереж дозволяє встановлювати доступ до певної інформації навіть для обмеженого кола друзів, що створює належні умови для належного захисту інформації від її неправомірного оголошення.

Людина самостійно визначає міру доступу до інформації про своє особисте життя, наприклад, інформуванням про це в соціальних мережах. Проте, як звертає увагу С. П. Гришаєв, слід враховувати, що таке особисте волевиявлення людини може поширюватися тільки на інформацію, що стосується її особисто, і не може поширюватися на інших осіб, навіть якщо вони були причетні до цієї ж події¹.

З появою соціальних мереж з'явилася можливість поширення форми об'єктивізації зображення людини завдяки пошуку за хештегом, встановлення відмітки на фотографії про конкретну зображену особу з активним посиланням на її сторінку в соціальній мережі тощо. На жаль, на сьогодні не існує єдиної виробленої позиції з правомірності використання таких позначень, але матеріали судової практики свідчать про необхідність врегулювання відносин у цій сфері. Як приклад можна навести таку суперечку. Фотограф із США опублікував у Facebook серію знімків із людиною в костюмі Санта-Клауса. Відмічаючи його на фото, він вибрав профіль реального жителя Аляски з таким ім'ям, після чого отримав від обуреного порушенням своїх прав чоловіка лист із вимогою видалити теги. Як повідомляє PetaPixel, через погрози фотографові довелося відредагувати відмітки на зображеннях. Як заявив Санта Клаус в електронному листі, відмітивши його на зображеннях, фотограф тим самим дав посилання на сторінку Клауса у Facebook, ввівши

¹ *Гришаев С. П.* Право на неприкосновенность частной жизни // Гражданин и право. 2012. № 12. С. 11–29.

користувачів в оману. Насправді на зображеннях був не він, а інший чоловік у костюмі Санти¹.

У соціальних мережах також удосконалюються можливості пошуку зображення людини. Наприклад, компанія Facebook уже розробила програмне забезпечення DeerFace для розпізнавання осіб, яка зможе автоматично знаходити і відмічати на завантажених фотографіях інших людей. Програмному забезпеченню DeerFace під силу виконувати процедуру верифікації особи (воно визнає, що на двох фотографіях зображена одна і та ж особа), а не розпізнавання особи (автоматичний пошук особи по фотографії особи). Тепер людину з реального життя можна ідентифікувати в мережі по особистому аватару². У будь-якому разі людині слід пам'ятати про параметри безпеки, зокрема про можливість відмовитися від публічних списків пошуку, про можливість встановлення обмежень, підвищення конфіденційності³. Ця сфера відносин у своєму розвитку набагато випереджає правове регулювання цих відносин, але питання автоматичного позначення людини за її зображенням потребує правового осмислення.

У соціальних мережах закріплюються правила щодо списку контенту, забороненого для публікації на сторінках користувачів, та намагаються видаляти його у разі появи. Компанія Facebook розробляє програму, що дозволить завадити користувачам соцмереж публікувати на сторінці фото в стані алкогольного сп'яніння. У майбутньому планується, що нова програма також зможе відстежувати публікації інших користувачів чужих фотографій без дозволу⁴. Безперечно, розроблення таких програм є важливим для ефективної охорони цивільних прав та інтересів фізичних осіб, але на практиці можуть виникнути певні питання щодо ефективності такої програми та результативності її показників.

Відповідно до позиції Суду Європейського Союзу, інтернет-користувачі повинні мати можливість вільно ділитися посиланнями на матеріали, наприклад, фотографії або відео, якщо матеріал був опублікований вільно онлайн з дозволу правовласника. Право ділитися посиланнями проте не заходить так далеко, що дозволяє ко-

¹ Степанов В. Настоящий Санта-Клаус запретил отмечать себя на фото в Facebook. URL: <https://tjournal.ru/p/never-tag-santa> [29.12.2014; 20:39].

² Adrian A. If I am the Author of my Online Persona, How can I protect it? URL: https://www.academia.edu/7928102/If_I_am_the_Author_of_my_Online_Persona_How_can_I_protect_it [25.07.2014].

³ Lowe I., Waite C. Soul stealers. What control do you have over your online images? // Copyright World. 2009. N 192. P. 24–26.

⁴ Facebook хоче завадити юзерам публікувати селфі «під мухою». URL: <http://tsn.ua/bbc/facebook-hoche-zavaditi-yuzeram-publikuvati-selfi-pid-muhoyu-397062.html> [12.12.2014; 12:37].

ристувачам обмінюватися посиланнями, які розроблені, щоб обійти платний доступ або інші підписки¹. Разом з цим неприпустимо комерційне використання фотографій у вільному доступі, навіть на умовах ліцензії Creative Commons².

Розміщення зображень на ресурсах з можливістю репосту запропоновано вважати виявленням згоди на їх наступне використання. У правозастосовній практиці деяких країн³ обнародуванням запропоновано вважати дії, які вперше роблять дане зображення доступним для загального доступу завдяки його опублікуванню, публічного показу чи іншим способом, у тому числі його розміщенням в мережі Інтернет.

Як звертає увагу М. Труханова, обставини розміщення фізичною особою власного зображення у мережі Інтернет можуть свідчити про висловлення такою особою згоди про наступне використання зображення, наприклад, якщо таке передбачено умовами користування сайтом, де особою розміщено зображення⁴. Аналогічну позицію підтримує А. Пичугіна, яка на підставі аналізу матеріалів судової практики робить висновок, що фізична особа при розміщенні власних фотографій на сайті у мережі Інтернет (у відкритому для невизначеного кола осіб доступі) своїми діями висловлює свою згоду на обнародування власного зображення, його обговорення та користувачам сайта надається можливість представлення оцінок⁵.

Аналогічна позиція простежується й у вітчизняній правозастосовній практиці. При вирішенні спору суд врахував, що фотографії, які стали приводом для конфлікту між сторонами, були розміщені особисто позивачем на власній сторінці в соціальній мережі «ВКонтакте» та були відкриті для загального доступу, що давало можливість безперешкодного їх огляду та обговорення сторонніми особами. В задоволенні позову про захист честі, гідності та стяг-

¹ Copyright notice: digital images, photographs and the Internet. Copyright Notice Number: 1/2014 Updated: March 2014. URL: <http://www.bipp.com/Portals/0/PDF/IPOCopyrightNoticeMarch2014.pdf>.

² Steven James. Picture use does not sit pretty. Copyright World Issue N 175, November 2007. P. 9–10; Sylvia Waycot. Turning common thinking on its head. Copyright World Issue N 175, November 2007. P. 5.

³ О применении судами некоторых положений раздела I части первой Гражданского кодекса Российской Федерации: постановление Пленума Верховного Суда Российской Федерации от 23 июня 2015 г. № 25. URL: http://www.supcourt.ru/Show_pdf.php?Id=10121. П. 43.

⁴ Труханова М. Верховный суд признал фотографии с возможностью репоста «общими». URL: http://online.zakon.kz/Document/?doc_id=38190551.

⁵ Пичугина А. Социальные сети и публичные люди // Корпоративный юрист. 2014. № 6. С. 38.

нення моральної шкоди було відмовлено. Апеляційна скарга по цій справі була відхилена¹.

Викладене свідчить про визнання можливості репосту розміщеного зображення у мережі Інтернет підставою для вільного використання зображення без комерційної мети. Потребують дослідження й інші технічні можливості пошуку та отримання доступу до зображень фізичної особи у мережі Інтернет з метою вироблення єдиної позиції у правозастосовній практиці при вирішенні спорів щодо правомірності використання зображення фізичної особи.

Характеризуючи порушення права на зображення, слід відзначити, що неправомірне використання фотографічних творів із зображенням фізичної особи може супроводжуватися різноманітними цілями, серед яких можна відзначити наступні:

- неправомірне використання фотографічних творів з комерційною метою (прикладом є вимоги мешканки штату Огайо Шеннон Стовалл, пред'явлені до Yahoo! у розмірі двадцять мільйонів доларів за використання її фотографії в рекламних цілях. Також жінка розраховує на частину прибутку від реклами з використанням її приватної власності (тобто особи), яку отримала Yahoo! та оплату судових витрат і витрат на послуги адвокатів з трьох фірм)²;

- неправомірне використання з метою пошуку та привернення уваги злочинців. Прикладом є справа за позовом мешканки Удмуртії, яка вимагала компенсацію в розмірі 5 млн рублів у судових приставів, які виманювали боржників, використовуючи її фотографії, розміщені на сайтах «Однокласники» і «ВКонтакте». Про те, як використовують її знімки, Яна Коновалова дізналася випадково з випуску новин. Пристави створювали сторінки вигаданої дівчини Елі Ковалевської, копіювали фото Яни Коновалової і під таким видом знайомилися з боржниками і призначали їм побачення. Відповідно до законодавства РФ, співробітники служби судових приставів не наділені правом вести оперативно-розшукову діяльність. Крім цього, вони порушили право людини на охорону її зображення (ст. 152.1 ЦК РФ)³;

- незаконне використання фотографічних творів у особистих цілях з порушенням права на приватні дані. Слід відзначити, що

¹ Рішення Василівського районного суду Запорізької області від 13.08.2013 р. по справі № 311/2168/13-ц. URL: <http://reyestr.court.gov.ua/Review/33024330>; Ухвала Апеляційного суду Запорізької області від 18.09.2013 р. по справі № 22-ц/778/4763/13. URL: <http://www.reyestr.court.gov.ua/Review/33589373>.

² Американка потребує с Yahoo! 20 миллионов за свою фотографию, 02.03.2007 г. Источник: Лента.Ру. URL: <http://www.yurpractika.com/news.php?id=0011014>.

³ «Приманка» судебных приставов в «Одноклассниках» требует в суде компенсацию, 23.11.2009 г. Источник: Украина Криминальная. URL: <http://www.yurpractika.com/news.php?id=0019294>.

у певних випадках розміщення фотографічних творів з зазначенням імен осіб, які на них зображені, визнають порушенням права на приватні дані. Користувачам польської соціальної мережі Nasza-Klasa (аналог «Однокласників»), схоже, доведеться якось обходитися без викладання фотографій у загальний доступ. Варшавський адміністративний суд задовольнив претензії позивача, який визнав, що поява у зазначеній мережі його старих шкільних фотографій та прізвища в ряду знімків учнів його класу є порушенням закону про захист особистих даних. У Nasza-Klasa він не зареєстрований і, відповідно, сам свою стару фотографію викласти в Мережу не міг. Це зробив хтось із його колишніх однокласників без відома позивача. Знімок був у загальному доступі близько року, перш ніж Томаш про це дізнався. Спершу Томаш хотів вирішити проблему полюбовно, зажадавши у адміністрації Nasza-Klasa прибрати його фотографію і прізвище з веб-сторінки, проте отримав відмову. Позицію сервісу розділив Генеральний інспектор із захисту особистих даних Міха Сежіцкі (Michał Serzycki). На його думку, зображення далекого минулого – а в школу Томаш ходив 30 років тому – не підпадають під визначення особистих даних, оскільки, щоб зв'язати їх з конкретно людиною, потрібно докласти значних зусиль. Однак варшавський суддя вирішив інакше, вважаючи, що строк давності в питаннях захисту приватних даних не має значення. Втім рішення суду ще може бути опротестоване, і не виключено, що пан Сежіцкі подасть апеляцію, тим більше що в одній із статей закону про захист особистих даних обумовлюється якраз можливість визначення особистості «без надмірних зусиль»¹;

– неправомірне використання з метою порнопомсти. «Revenge porn» (порно помста) як новий вид порушення особистих прав фізичної особи з'явився близько п'ятнадцяти років тому внаслідок конфліктів між знаменитими особами та їх колишніми коханими та бажанню покинутих коханих помститися за розлучення. Сутність таких дій полягає у неправомірному розміщенні фотографічних та інших художніх творів (як контенту Інтернет-сайтів) з зображенням колишніх близьких осіб в оголеному вигляді чи під час моментів особистого характеру. При цьому не виключається розголошення інформації персонального характеру поряд з такими творами.

Прикладом перших з таких дій було розміщення Томмі Лі в Інтернеті «гарячого відео» їх з Памелою Андерсон першої шлюбної ночі. Потім у мережі з'явилися відео Періс Хілтон («Одна ніч з Періс»), Камерон Діас і Брітні Спірс. Сьогодні ідея розміщувати

¹ Суд обязал польскую социальную сеть удалить с сайта старую школьную фотографию по иску одного из одноклассников, 06.03.2009 г. Источник: Новостей. COM. URL: <http://www.yurpractika.com/news.php?id=0017011>.

в мережі порнофото або відео зі своїм колишнім шанувальником або прихильницею – так звана «порно вендета» – набирає значних масштабів¹. У США навіть створені спеціальні сервіси, на яких розміщуються тільки фотографії фізичних осіб в оголеному вигляді. Вони супроводжуються інформацією про персональні дані зображеної особи, зокрема містять її прізвище та ім'я, вказівку на місце навчання чи роботи, посилання на сторінки у соціальних мережах, номери телефонів чи домашні адреси та інші дані. Крім цього, на сервісі існує можливість коментування розміщених фотографій.

Після розповсюдження «revenge porn» й у інших країнах на зріла необхідність боротьби з такими діями на законодавчому рівні. У Пенсільванії 14 січня 2014 року було прийнято законопроект № 1167, який забезпечує захист прав фізичної особи від злочину, пов'язаного з переслідуванням сексуального партнера. Розділ 18 (злочинів та правопорушень) консолідованого уставу Пенсільванії доповнено § 2709,2 – домагання інтимного партнера. Такий злочин здійснюється шляхом розміщення (обнародування) фотографії, кіно-, відеозапису чи аналогічного запису зображень інтимного партнера в оголеному вигляді чи в інтимні моменти їх особистого життя (при цьому якість запису дозволяє ідентифікувати особу) без будь-якої законної мети з наміром переслідування, залякування, збентеження чи хвилювання особи. Не є злочином дії, які вчинено за згодою зображеної особи.

До моменту прийняття відповідних змін у законодавство у США постраждалі особи намагалися власними зусиллями розробити механізм захисту прав фізичних осіб, які постраждали від «revenge porn». На жаль, дієвий захист здійснювався тільки щодо selfy-фотографій (створених самою особою) на підставі норм законодавства про авторське право.

Дії особи, яка постраждала внаслідок «revenge porn» та бажає захистити власні права, полягають у наступному. По-перше, необхідно забезпечити можливість підтвердження авторства для фотографій чи інших художніх творів і наявність відповідних прав. По-друге, направити повідомлення про блокування доступу найбільшим пошуковикам (в рамках DMCA), а також ініціювати блокування, згідно з антипіратським законом, щодо сервісу. По-третє, збільшити свою присутність у мережі шляхом реєстрації на популярних сервісах (соціальних мережах), що дозволить «відсунути» індексацію сайту з фотографіями на другу сторінку і далі. Спробувати об'єднатися з іншими жертвами і, зібравши важкий томик

¹ *Казати Д.* Месть реализуется через порно любительское порно. URL: aktiv.com.ua [29.04.2009, 16:44].

матеріалів, звернутися до правоохоронних органів¹. При виконанні даних рекомендацій у часті випадків є можливість обґрунтувати вимоги про видалення небажаного контенту зі сторінок Інтернет-сайтів.

В Україні у судовій практиці також трапляються справи про захист порушених особистих прав фізичної особи, порушених внаслідок розміщення фотографій інтимного характеру у соціальних мережах. До відповідальності за «revenge porn», в залежності від обставин справи, за законодавством України можна притягнути особу внаслідок:

- порушення права на персональні дані фізичної особи (Закон України «Про захист персональних даних»);
- порушення авторських прав – у випадку доведення авторства на фотографії чи інші художні твори (ЦК України, Закон України «Про авторське право і суміжні права»);
- порушення права на зображення (ст. ст. 307, 308 ЦК України);
- порушення норм суспільної моралі (Закон України «Про захист суспільної моралі») тощо.

У законодавстві нашої країни, на жаль, досить не існує дієвих механізмів захисту прав та інтересів у мережі Інтернет. Доцільно впровадити відповідні норми щодо можливості захисту прав шляхом зобов'язання видалити з сайту інформацію (контент), що порушує права та інтереси фізичних осіб. Слід вдосконалити порядок визначення винної у розміщенні контенту особи (користувача Інтернету) та притягнення її до відповідальності за порушення прав та інтересів фізичних осіб, з врахуванням специфіки Інтернет-середовища.

У соціальних мережах досить розповсюджені випадки неправомірної реєстрації акаунту, тобто під іменем особи, але без її відома та, відповідно, без отримання її згоди на це. Прикладом є пред'явлений бразильським полухакером донецького футбольного клубу «Шахтар» Жадсоном позов проти соціальної мережі orkut, створеної компанією Google. Незадоволення Жадсона викликав підроблений профіль в orkut, нібито належний футболісту. Гравець має намір заблокувати неправомірне використання свого образу в соціальній мережі, а також вимагати компенсацію за використання підробленого профілю. У соціальній мережі orkut є профіль користувача під іменем Жадсон Родрігес. У розділі «про себе» зазна-

¹ *Laws Ch. I've Been Called the «Erin Brockovich» of Revenge Porn, and For the First Time Ever, Here is My Entire Uncensored Story of Death Threats, Anonymous and the FBI.* URL: <http://www.xojane.com/it-happened-to-me/charlotte-laws-hunter-moore-erin-brockovich-revenge-porn>.

чено, що профіль належить футболісту «Шахтаря». Коло інтересів користувача обмежується футболом. Користувач доволі активний у мережі, має 135 друзів. Крім того, він регулярно поновлює розділ «фотографії». Також у мережі огіут є товариство, присвячене Жадсону¹. Іншим прикладом є справа про притягнення до відповідальності мешканки Мурманська за порушення недоторканності приватного життя, ч. 1 ст. 137 КК РФ. Після розриву стосунків зі своїм співмешканцем жінка знайшла в квартирі відеофайли еротичного змісту за участю колишнього друга, створила на сайті «ВКонтакте» сторінку з його ім'ям і розмістила на ній наявну в її розпорядженні інформацію².

При неправомірному публічному поширенні фотографічних чи інших художніх творів з використанням зображення чи інших персональних даних фізичних осіб, крім вимоги про стягнення компенсації моральних страждань (у випадку наявності таких), одним з способів захисту прав виступає вимога припинення публічного показу фотографічного твору чи видалення його з певних ресурсів (наприклад, Інтернет-сайта). При цьому, якщо порушник буде нести певні збитки внаслідок знищення примірників твору, у якому неправомірно відтворений фотографічний твір, всі збитки покладаються лише на нього. Ця вимога заснована на положенні ч. 2 с. 278 ЦК України, відповідно до якої, якщо особисте немайнове право фізичної особи порушено у газеті, книзі, кінофільмі, телепередачі тощо, які випущені у світ, суд може заборонити (припинити) їх розповсюдження до усунення цього порушення, а якщо усунення порушення неможливе, — вилучити тираж газети, книги тощо з метою його знищення.

Закріплення на законодавчому рівні права пред'являти вимоги не тільки про вилучення зображень фізичних осіб у мережі Інтернет, а також про припинення або заборону наступного їх розповсюдження, права вимагати знищення примірників екземплярів матеріальних носіїв, які містять інформацію про приватне життя, отриману з порушенням закону (у тому числі й фотографічні та інші художні твори з зображенням людини), є особливо актуальним в епоху розвитку інформаційних технологій та поширення випадків порушення прав та інтересів фізичних осіб у соціальних мережах, в мережі Інтернет.

¹ Футболіст «Шахтера» подал в суд на социальную сеть 14/08/09, Источник: Украина Криминальная. URL: <http://www.yurpractika.com/news.php?id=0018287>.

² За эротическое видео с бывшим мужем «ВКонтакте» женщина ответит в суде, 08.04.2010 г. Источник: Pravo.ru. URL: <http://yurpractika.com/news.php?id=0020816>.

В Україні законодавство про охорону права фізичної особи на власне зображення потребує удосконалення в частині закріплення категорії «зображення фізичної особи», розмежування на законодавчому рівні зображення особи як її немайнового блага (зовнішнього вигляду) та як відтворення образу на матеріальному примірнику, впровадження додаткових способів захисту прав та інтересів фізичної особи з урахуванням поширення порушення права фізичної особи на власне зображення у мережі Інтернет. Поява нових засобів зв'язків вимагає вдосконалення системи захисту прав та інтересів фізичних осіб, вироблення нових способів визначення порушників у мережі, визначення та фіксації системи доказів, адже зі спливом часу може відбуватися зміна фотографії аканту, прізвища та імені користувача мережі.

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У СОЦІАЛЬНІЙ МЕРЕЖІ

Соціальна мережа як феномен інформаційних технологій в ході свого існування та розвитку поставила досить важливе та логічне завдання перед суспільством – забезпечити дієвий захист персональних даних її користувачів.

Право на захист персональних даних особи є похідним від права недопущення втручання в особисте життя та права на заборону збирання, зберігання, використання та поширення конфіденційної інформації про особу, що закріплені у ст. 32 Конституції України¹.

Право на захист персональних даних особи є необхідним елементом людського життя в інформаційному суспільстві, воно є фундаментальним правом людини, і у разі його порушення під загрозою перебувають безпека особи, її честь, гідність тощо.

Захист фізичних осіб під час обробки персональних даних за законодавством ЄС є фундаментальним правом. Зокрема, ст. 8 (1) Хартії фундаментальних прав Європейського Союзу встановлено, що кожна особа має право на захист своїх персональних даних².

Особливо гостро проблема захисту персональних даних у соціальній мережі постала на початку 2018 року. Компанія Facebook була знову викрита у витоку персональних даних у 2016–2017 роках. Це був найбільший за всю історію людства витік – було вилучено персональні дані 50 млн користувачів соцмережі через сторонню програму опитування користувачів.

Вважається, що це результат протиправної діяльності приватної компанії Cambridge Analytica, яка займається аналізом даних соціальних мереж для розробки ефективної стратегії в ході виборчих кампаній в Інтернеті (політичний консалтинг). Вказана компанія збирала персональні дані користувачів Facebook для здійснення ма-

¹ Конституція України: Закон України від 28 черв. 1996 р. № 254к/96-ВР // Відомості Верховної Ради України. 1996. № 30. Ст. 141.

² Хартія основних прав Європейського Союзу. URL: http://zakon3.rada.gov.ua/laws/show/994_524.

ніпуляцій суспільною думкою. Cambridge Analytica створила алгоритм на основі отриманих персональних даних, за допомогою якого здійснювала адресну рекламну розсилку¹.

В результаті чого висувається теза, що діяльність компанії Cambridge Analytica суттєво вплинула на результати президентських виборів 2017 року у США та на результати референдуму 2016 року у Великобританії щодо виходу з Європейського Союзу².

З цього можемо зробити маленький висновок, що захист персональних даних у соціальній мережі потрібен не тільки для конкретного користувача, а й для всього суспільства загалом, оскільки наслідки витоку персональних даних можуть бути невідворотними.

В Україні основним нормативно-правовим актом, який регулює відносини, що виникають у зв'язку із захистом персональних даних у соціальній мережі, є Закон України «Про захист персональних даних» від 1 червня 2010 року. Закон врегульовує правові відносини щодо захисту та обробки персональних даних, він також спрямований на захист фундаментальних прав і свобод людини і громадянина, включно з правом на невтручання в особисте життя у зв'язку з обробкою персональних даних³.

Поряд з цим варто зазначити, що 25 травня 2018 року набрав чинності Загальний регламент про захист даних Європейського Союзу (EU General Data Protection Regulation) від 27 квітня 2016 року (далі – Правила GDPR)⁴, який почав регулювати відносини щодо захисту персональних даних не тільки в ЄС, а частково і в Україні.

Хоча Україна на даний момент не входить до списку членів ЄС, однак через закріплені ст. 3 Правил GDPR принцип екстериторіальності Правил GDPR застосовуються у випадках, коли:

1. Контролер або оператор персональних даних знаходяться на території Європейського Союзу, незалежно від місця обробки персональних даних.

2. Контролер або оператор персональних даних перебувають за межами території ЄС, а власники персональних даних (суб'єкти да-

¹ Ковальчук О. Я., Гайда Т. Ю., Жонца С. Я. Технології Big Data в інноваційному маркетингу // Український журнал прикладної економіки. 2018. Т. 3, № 1. С. 36–52. ISSN 2415-8453.

² David D. Kirkpatrick. Using Digital Firm, Brexit Campaigners Skirted Spending Laws, Ex-Employee Says // The New York Times. URL: <https://www.nytimes.com/2018/03/24/world/europe/uk-brexite-vote-leave-shahmir-sanni.html>.

³ Про захист персональних даних: Закон України від 1 черв. 2010 р. № 2297-VI. URL: <http://zakon2.rada.gov.ua/laws/show/2297-17>.

⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: <http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf>.

них) перебувають на території ЄС: (а) при оплатному чи безоплатному постачанні товарів чи наданні послуг таким особам у межах ЄС або (б) при моніторингу поведінки власників персональних даних у межах ЄС.

3. Контролер або оператор персональних даних знаходяться за межами ЄС, але в місці, де застосовується законодавство держави-члена в силу публічного міжнародного права¹.

Крім цього, відповідно до Угоди про асоціацію від 27 червня 2014 року Україна має узгодити внутрішнє законодавство згідно з Правилами GDPR².

У зв'язку з цим українські фізичні та юридичні особи можуть за певних обставин підпадати під дію Правил GDPR. Наприклад, ІТ-компанія, що розробила певну соціальну мережу, у випадку наявності користувача, що знаходиться на території ЄС, зобов'язана обробляти його персональні дані відповідно до Правил GDPR. Також під дію цього документа підпадатиме фізична особа, що знаходиться в Україні, але користується соціальною мережею, яку обслуговує ІТ-компанія, що перебуває у ЄС.

Саме тому виникає нагальна потреба у дослідженні Правил GDPR.

Згідно зі ст. 4 Правил GDPR персональними даними є будь-яка інформація, що відноситься до фізичної особи, яку ідентифіковано чи можна ідентифікувати («суб'єкт даних»); фізична особа, яку можна ідентифікувати, є такою особою, яку можна ідентифікувати, прямо чи опосередковано, зокрема, за такими ідентифікаторами, як ім'я, ідентифікаційний номер, дані про місцезнаходження, онлайн-ідентифікатор або за одним чи декількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи.

Закон України «Про захист персональних даних» персональними даними визначає відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована³. Закон загалом відображає визначення поняття «персональні дані», що надане у Директиві Європейського парламенту

¹ Офіційний переклад Регламенту Європейського Союзу 2016/679 від 27 квітня 2016 року Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) / Урядовий офіс координації європейської та євроатлантичної інтеграції Секретаріату Кабінету Міністрів України. URL: <https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf>.

² Угода про асоціацію між Україною та Європейським Союзом, Європейським співтовариством з атомної енергії та їхніми державами-членами сторони: від 27 черв. 2018 р. URL: http://zakon3.rada.gov.ua/laws/show/984_011.

³ Про захист персональних даних: Закон України від 1 черв. 2010 р. № 2297-VI. URL: <http://zakon2.rada.gov.ua/laws/show/2297-17>.

і Ради ЄС № 95/46/ЄС про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних, яку Правила GDPR скасували. Тому цілком логічним є те, що зовсім скоро законодавство України у сфері захисту персональних даних буде змінено у відповідності з Правилами GDPR.

Згадані вище визначення «контролера» та «оператора» персональних даних майже ідентичні вітчизняним визначенням «володільця персональних даних» та «розпорядника персональних даних».

Контролером є фізична чи юридична особа, орган публічної влади, агентство чи інший орган, який самостійно чи спільно з іншими визначає цілі та засоби опрацювання персональних даних. Оператором є фізична чи юридична особа, орган публічної влади, агентство чи інший орган, який опрацьовує персональні дані від імені контролера¹.

На прикладі буде краще зрозуміти, як українська юридична особа підпадає під дію Правил GDPR. Припустимо, що в Україні зробили уявну соціальну мережу під назвою «LSN» («Lawyer Social Network»), яка набула популярності не тільки в Україні, а й у Європі, як наслідок, особи, що перебувають у ЄС, почали активно реєструватись у цій соціальній мережі.

У такому випадку Правила GDPR прямо поширюються на соціальну мережу «LSN». Українська компанія – власник «LSN» Lawyer Social Network Inc. буде контролером персональних даних, а Amazon Web Services, Inc. (AWS) буде оператором персональних даних, оскільки остання надає послуги хостингу для обробки та зберігання персональних даних користувачів соціальної мережі на серверах AWS.

Правила GDPR також містять поняття «профайлінг», яке означає будь-яку форму автоматизованого опрацювання персональних даних, що складається із використання персональних даних для оцінювання окремих персональних аспектів, що стосуються фізичної особи, зокрема, для аналізу або прогнозування аспектів, що стосуються продуктивності суб'єкта даних на роботі, економічної ситуації, здоров'я, особистих переваг, інтересів, надійності, поведінки, місцезнаходження або пересування.

Після процедури профайлінгу персональні дані перетворюються на вторинну інформацію, за допомогою якої можливе автома-

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: <http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf>.

тизоване прийняття рішень на основі первинної інформації. Прикладом може бути реклама у соціальній мережі Facebook, з якою майже кожен з нас не раз стикався, залежно від статі, віку, місця знаходження тощо.

Відповідно до ст. 22 Правил GDPR у суб'єкта персональних даних є право на заборону прийняття контролером будь-якого рішення, яке засноване виключно на автоматичній обробці, включно з профілюванням, якщо такі рішення мають юридичні наслідки.

Правила GDPR у главі III визначають значний перелік прав суб'єктів персональних даних. До них відносяться права:

- на надання згоди щодо обробки персональних даних;
- на зрозумілу та прозору інформацію;
- на доступ до інформації;
- на виправлення;
- на стирання («бути забутим»);
- на обмеження опрацювання;
- на мобільність даних;
- на заперечення;
- заборони використання автоматизованих рішень, заснованих на профайлінгу;
- отримувати інформацію про порушення правил безпеки зберігання даних.

Особливої уваги серед них потребують право на стирання, право на мобільність, а також право на надання згоди щодо обробки персональних даних.

Правом на мобільність даних є право, за яким суб'єкт даних може вимагати від контролера надання власних персональних даних, наданих у процесі користування соціальною мережею, в структурованому, загальноприйнятому форматі, що легко зчитується машиною, та право на передачу цих даних іншому контролеру без перешкод від первинного контролера. У свою чергу, право на стирання персональних даних надає можливість суб'єкту персональних даних «бути забутим», тобто вимагати стирання всіх персональних даних, в такому випадку контролер без будь-якої необґрунтованої затримки має видалити ці дані. Але це дуже складна дія з технічної точки зору тому, що навіть після видалення персональних даних деякі з них все одно зберігаються на магнітних носіях інформації. Тому для повної відповідності Правилам GDPR контролери можуть такі дані користувачів соціальних мереж шифрувати, а потім видаляти тільки ключ шифрування. Такий метод перетворює дані в повністю і назавжди нечитабельний масив інформації¹.

¹ Пужний В. Нові вимоги ЄС до захисту персональних даних з травня 2018

Варто сказати, що реалізація права на надання згоди щодо обробки персональних даних чітко регламентована нормами Правил GDPR. Суб'єкт персональних даних – користувач соціальної мережі повинен надати однозначну та чітко виражена згоду на опрацювання персональних даних. Тобто загальноприйняте на практиці проставлення кліку про ознайомлення з документом у вигляді так званих «плюсика» чи «галочки» не відповідає вимогам Правил GDPR. Саме тому більшість соціальних мереж на даний момент отримують згоду своїх користувачів саме через спливаюче вікно з короткою інформацією про опрацювання персональних даних та позначкою згоди на таку дію.

Правила GDPR висувають вимогу до обсягу повідомлення про політику приватності, яка має бути простою, чіткою та зрозумілою. На практиці стало популярним використовувати два документи: Privacy Policy – загальна політика конфіденційності соціальної мережі, а також Privacy Notice – окрема частина Privacy Policy, в якій повідомляється про обсяг та мету опрацювання персональних даних¹.

Важливим моментом крім отримання згоди є також управління вже отриманими згодами. Для прикладу, Information Commissioner's Office (ICO) зазначає у власних рекомендаціях щодо управління згодами, які отримуються в ході виконання Правил GDPR:

- запит на отримання згоди варто робити виразним, стислим, відокремленим від інших умов і простим для розуміння;
- варто включити назву організації та будь-яких контролерів – третіх сторін, які будуть спиратися на згоду, пояснити, навіщо потрібна інформація, які дії будуть проводитись з інформацією, і наявність у суб'єкта персональних даних права на відкликання згоди;
- згода має бути надана в активній формі (без авто-заповнених полів анкет чи за замовчуванням);
- за можливості варто надавати можливість детального вибору умов згоди для різних цілей різних видів обробки;
- варто зберігати підтвердження факту надання згоди – суб'єкт, який надав згоду, час надання, спосіб та що було повідомлено суб'єкту перед наданням такої згоди;
- варто робити простою можливість відкликати надану згоду та розглянути можливість використання інструменту вибору переваг;

поку. URL: <http://channel4it.com/publications/Nov-vimogi-S-do-zahistu-personalnih-danih-z-travnya-2018-roku-30154.html>.

¹ Тарасюк А. В. Вплив загального регулювання захисту даних на контролерів та процесорів персональних даних – резидентів України // Інформація і право. 2018. № 1 (24). URL: http://ippi.org.ua/sites/default/files/5_8.pdf.

– варто тримати отримані згоди під контролем та оновлювати їх у випадку змін, а також зробити це частиною власних бізнес-процесів¹.

У свою чергу, Закон України «Про захист персональних даних» має як схожі, так і відмінні риси з Правилами GDPR.

Для прикладу, за діючим законом персональні дані обробляються відкрито і прозоро. Така дія виконується виключно з метою досягнення конкретних і законних цілей, які мають бути підтверджені чіткою згодою суб'єкта персональних даних, або прямо передбачена законодавство України. Мета процесу обробки персональних даних обов'язково має бути визначена у внутрішніх документах, якими врегульовується діяльність володільця персональних даних, а також має відповідати чинному законодавству України про захист персональних даних. Загальний перелік та зміст персональних даних повинні адекватно та не надмірно відповідати меті їх обробки.

Персональні дані потрібно оформлювати досить точно та достовірно, а також проводити їх регулярні оновлення у разі потреби, яка визначена метою обробки.

Оброблення персональних даних проводиться із залученням засобів та у спосіб, що суворо відповідають меті та цілям такого оброблення. У випадку несумісності попередньої та нової мети суб'єкт персональних даних має дати нову згоду на обробку його персональних даних згідно з новою метою².

Правила GDPR також закріплюють принцип захисту персональних даних за замовчуванням. Він означає впровадження технічних та організаційних заходів захисту персональних даних контролерами та операторами ще до того, як дані потрапляють до них. До технічних заходів можна віднести застосування мережевого захисту від несанкціонованого доступу до бази персональних даних, використання методів шифрування даних та їх анонімізації, фізичний та онлайн-контроль доступу до даних, впровадження процедур багатоступеневої авторизації працівників тощо. До організаційних заходів відносяться заходи щодо визначення порядку доступу працівників до персональних даних, визначення порядку ведення обліку операцій з персональними даними, укладання договорів NDA та DPA з працівниками та контрагентами тощо³.

¹ Guide for the General Data Protection Regulation (GDPR) / Information Commissioner's Office (ICO). URL: <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf>.

² Про захист персональних даних: Закон України від 1 черв. 2010 р. № 2297-VI. URL: <http://zakon2.rada.gov.ua/laws/show/2297-17>.

³ Дреїс Ю. О. Заходи захисту персональних даних у інформаційних автоматизованих системах. URL: <http://er.nau.edu.ua/bitstream/NAU/32527/1/Заходи%20>

Правила GDPR забезпечують також дотримання конфіденційності даних. Обов'язки із захисту персональних даних, отриманих в ході функціонування соціальної мережі, регулюються кількома статтями Правил GDPR. Для запобігання витоку персональних даних суб'єкта персональних даних контролерам та операторам персональних даних необхідно:

- проводити захист даних користувачів соціальних мереж за замовчуванням;
- укладати договори про нерозголошення конфіденційної інформації (NDA) зі своїми контрагентами та працівниками;
- застосовувати криптографічні алгоритми шифрування персональних даних або їх псевдонімізацію;
- впроваджувати заходи безпеки стосовно оцінки ризиків витоку персональних даних;
- вживати заходів при зберіганні даних для подальшої обробки.

Правила GDPR спеціально вказують на шифрування як на основну вимогу безпеки даних. Крім того, організаціям потрібно провести оцінку ризиків, а потім вжити заходів, що пом'якшують ризики, які вони виявлять. Оскільки жодна організація не може повністю визначити або передбачити всі ризики для своїх даних і жоден підхід до периметра безпеки не є надійним, організації повинні шифрувати свої дані, щоб забезпечити відповідність до Правил GDPR. За допомогою шифрування, неважливо чи є порушення, – дані будуть належно захищені¹.

Крім цього, особливої уваги потребує політика приватності (Privacy Policy), яку повинна надати особа для користувачів соціальної мережі, про яку вже зазначалося вище. У цьому документі має бути визначений перелік персональних даних, які збираються, мета їх обробки, перелік прав користувачів соціальної мережі щодо своїх даних, а також порядок надання відповідей на скарги користувачів щодо порушення умов використання їхніх персональних даних.

До захисту персональних даних законодавець ЄС поставився досить серйозно та відповідально, про це свідчить ст. 83 Правил GDPR, де закріплені дві санкції за порушення положень цього документа:

1. У випадку порушення обов'язків, передбачених Правилами GDPR із захисту персональних даних, застосовується штраф у роз-

захисту%20персональних%20даних%20в%20інформаційних%20%28автоматизованих%29%20системах.pdf.

¹ Нужний В. Нові вимоги ЄС до захисту персональних даних з травня 2018 року // Інтернет ресурс Channel for IT [Електронний ресурс]. URL: <http://channel4it.com/publications/Nov-vimogi-S-do-zahistu-personalnih-danih-z-travnya-2018-roku-30154.html>.

мірі 10 млн євро або до 2 % від загального глобального річного обігу за попередній фінансовий рік, залежно від того, яка сума є вищою.

2. У випадку порушення умов надання згоди, прав суб'єктів даних, правил передавання персональних даних до одержувача в третій країні чи до міжнародної організації застосовується штраф у розмірі 20 млн євро або до 4 % від загального глобального річного обігу за попередній фінансовий рік, залежно від того, яка сума є вищою¹.

Щоб вберегти себе від подібних санкцій особи, що підпадають під поняття контролера чи оператора персональних даних, повинні провести загальний аудит персональних даних. А саме: визначити, як і в якому обсязі збираються персональні дані, до яких саме персональних даних особа має доступ та які з них зберігаються на власних та/або сторонніх носіях чи сховищах інформації, кому персональні дані можуть передаватися (хто з контрагентів особи може мати до них доступ), обсяги, сфери та конкретні цілі використання персональних даних особою.

З вищесказаного можемо зробити висновок, що станом на сьогодні захист персональних даних у соціальній мережі вийшов на новий якісний рівень. Після кількох гучних випадків, пов'язаних з порушенням захисту персональних даних у соціальній мережі, світова спільнота зрозуміла, що дієвий захист персональних даних є нагальною потребою сьогодення. Як наслідок, Європейський Союз у 2016 році прийняв Правила GDPR, які через свою екстериторіальність можуть врегульовувати відносини щодо захисту персональних даних навіть в нашій країні. Відповідно до Угоди про асоціацію від 27 червня 2010 року Україна має впорядковувати внутрішнє законодавство у відповідності до законодавства ЄС, через це зовсім скоро в Україні може з'явитись новий закон у сфері захисту персональних даних, що замінить морально застарілий Закон України «Про захист персональних даних» від 1 червня 2010 року, який є «дзеркалом» скасованої Директиви Європейського парламенту і Ради ЄС N 95/46/ЄС. А тому дослідження Правил GDPR є цілком обґрунтованим та доцільним під час висвітлення особливостей захисту персональних даних у соціальній мережі.

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: <http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf>.

ДЕЯКІ ПРОБЛЕМИ РЕАЛІЗАЦІЇ ПРАВА ДИТИНИ НА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У МЕРЕЖІ ІНТЕРНЕТ ЗГІДНО ІЗ ЗАКОНОДАВСТВОМ ЄС

У травні 2018 року у Європейському Союзі вступив в дію Регламент ЄС 2016/679 Європейського парламенту та Ради ЄС від 27 квітня 2016 року «Про захист фізичних осіб стосовно обробки особистих даних і про вільний рух таких даних, а також про скасування Директиви 95/46 / ЄС (загальне регулювання захисту даних). GDPR містить положення, які адресовані безпосередньо дітям. Зокрема, відповідно до ч. 1 ст. 8 GDPR обробка персональних даних вважається законною у разі наявності згоди дитини, яка досягла 16 років. Щодо осіб, які не досягли 16 років, для законності обробки даних необхідно отримати згоду зі сторони батьків дитини або осіб, що мають батьківську відповідальність. Відступаючи від загального положення в абз. 2 ч. 1 ст. 8, європейський нормотворець надав можливість державам встановлювати менший віковий ценз, але не переступаючи порогу 13 років¹.

Якщо звернутися до національних законодавств держав – членів ЄС, не важко помітити, що в більшості випадків європейські законодавці вважають неповнолітніх у віці від 14 до 16 років здатними усвідомлювати наслідки надання ними згоди на обробку персональних даних. Наприклад, згідно зі ст. 13 Закону «Про захист персональних даних» в Іспанії, «дані, що стосуються суб'єктів даних віком старше 14 років, можуть бути оброблені за їх згодою, крім випадків, коли закон вимагає допомоги батьків або опікунів». Подібним чином вік визначено в Законі «Про захист даних» у Нідерландах: «Якщо суб'єктом даних є неповнолітня особа віком до

¹ Регламент (ЕС) 2016/679 Европейского парламента и совета 27 апреля 2016 «О защите физических лиц в отношении обработки личных данных и о свободном движении таких данных, а также об отмене Директивы 95/46/ЕС (общее регулирование защиты данных)». URL: <https://internetinstitute.ru/wp-content/uploads/2017/07/Telecom-Data-Retention-Leg-appendix2.pdf>.

16 років, згоду на обробку її персональних даних надає її законний представник»¹.

Діти Литви можуть вважатися компетентними у віці від 14 років, оскільки з цього віку вони користуються частковими правами та мають право здійснювати основні правові акти без згоди своїх представників. Внаслідок цього їм також дозволяється надавати згоду на деякі основні операції обробки персональних даних.

У Бельгії вік надання згоди на обробку персональних даних закріплюється консультацією Комісії з питань недоторканності, де зазначено, що хоча, згідно з бельгійським законодавством, вік зрілості становить 18 років, необхідно визнати поступовий розвиток неповнолітніх та потребу в більшій незалежності від батьків, особливо у підлітковому віці, – у віці від 13 до 16 років. Особливий захист встановлений для чутливих даних та у разі обробки даних, що суперечить інтересам дитини. Для дітей, що не досягли 16 років, згода батьків у таких випадках є обов'язковою².

Франція є однією з перших держав, в якій було прийнято правовий акт щодо захисту персональних даних, – Закон про інформатику, файли та свободу 1978 року (останні зміни були внесені у 2004 році). Корируючі принципи правового регулювання, які відповідають сучасним тенденціям розвитку суспільних відносин, вносяться діючою Комісією з інформатики та свобод (далі – Комісія). Французьке законодавство закріплює загальне правило визначення дитини – це особа до 18 років. Комісія неодноразово підкреслювала свою прихильність міжнародним стандартам захисту прав дітей, встановлених в Конвенції ООН з прав дитини. Але в правозастосовній практиці допускає зниження до 15–16-річного порогу у деяких сферах використання персональних даних³.

У Німеччині законодавець передбачив правозастосовчий розсуд у питанні визначення віку дитини для надання самостійної згоди. Якщо лікар, вчитель чи соціальний працівник мають намір збирати, зберігати, оприлюднювати чи іншим чином використовувати ідентифікаційну інформацію про дитину у віці від 12 до 14 років, у них виникає обов'язок збалансувати різні інтереси: дитини, су-

¹ *Macenaite M., Kosta E.* Consent for processing children's personal data in the EU: following in US footsteps? // *Information & Communications Technology Law*. 2017. Vol. 26, Iss. 2. URL: <https://www.tandfonline.com/doi/full/10.1080/13600834.2017.1321096>.

² *Belgian Privacy Commission*, 'Advice No. 38/2002 of 16 September 2002 Concerning the Protection of the Private Life of Minors on the Internet'. 2002. URL: http://www.privacycommission.be/nl/docs/Commission/2002/advies_38_2002.pdf.

³ *Dowty T., Korff D.* 'Protecting the Virtual Child – The Law and Children's Consent to Sharing Personal Data' (Study prepared for arCh – action on rights for Children- and the Nuffield Foundation). 2009. URL: <http://www.nuffieldfoundation.org/sites/default/files/Protecting%20the%20virtual%20child.pdf>.

спільства та батьків. Дитина у віці 13 років може дозволити своєму лікарю надати конфіденційну інформацію стосовно стану свого здоров'я третім особам, але це не означає наявності автоматичного обов'язку виконувати такий запит. Лікар повинен оцінити зрілість дитини, її можливість усвідомлювати наслідки таких дій. Навіть у разі позитивного висновку щодо можливостей 13-річного приймати такі рішення, за наявності обставин, що свідчать про порушення інтересів дитини, лікар може проконсультуватися з батьками. Виходячи з такого підходу, одна й та сама дитина в одних випадках може бути автономною в питанні надання згоди, а в інших – потребувати згоди батьків, що яскраво проілюстровано існуючою німецькою судовою практикою. Вищий адміністративний суд Луненбурга у справі, пов'язаній з відеоспостереженням, зауважив, що згода дитини загалом може бути недійсною, якщо дитина не досягла 14 років. Проте в 2012 році Вищий регіональний суд м. Хамм вирішив, що не можна вважати дітей віком від 15 до 18 років як таких, що мають необхідну здатність передбачати наслідки відповідних операцій обробки даних (випадок стосується обробки особистих даних для проведення розмитнення)¹.

Отже, до моменту вступу у дію GDPR у питанні визначення віку самостійного надання згоди на обробку персональних даних національні законодавства держав – членів ЄС можна поділити на 3 групи: держави, в яких «зрілими» для надання згоди вважаються особи до досягнення повноліття (Литва, Бельгія, Іспанія); держави, що в цілому дотримуються 18-річного порогу із деякими винятками, які чітко передбачені законодавством (Франція); держави, в яких питання самостійності надання згоди на обробку персональних даних залежить від рівня зрілості та інших факторів, що мають значення для забезпечення найкращих інтересів дитини (Німеччина).

GDPR звузив свободу держав – членів ЄС у законодавчому регулюванні даного питання. Національні парламентарі повинні встановити вимогу щодо наявності згоди батьків або піклувальників для законності обробки даних дітей у віці від 13 до 16 років. Таке інноваційне європейське рішення має як позитивні, так і негативні наслідки. З однієї сторони, законодавство держав-членів досягне певної гармонізації у цьому питанні. З іншої сторони, такий варіативний підхід до визначення вікового порогу зумовлює відсутність повної уніфікації та породжує чимало правових колапсів.

На перший погляд, вікові вимоги, встановлені GDPR, не відповідають Основному міжнародному «закону» у сфері захисту прав дитини, – Конвенції про права дитини (далі – Конвенція). Зо-

¹ European data protection law and minors – no legal certainty. URL: <http://germanitlaw.com/european-data-protection-law-and-minors-no-legal-certainty>.

крема, згідно зі ст. 1 Конвенції дитиною є кожна людська істота до досягнення 18-річного віку, якщо за законом, застосовуваним до даної особи, вона не досягає повноліття раніше. Отже, аналіз правових норм Конвенції та GDPR дає можливість науковцям (Хелені Адамович і Дорте Кривокапич) констатувати наступну правову оцінку: 1. Норми права ЄС вступають у протиріччя із нормами міжнародного права; 2. Дане протиріччя породжує два потоки правових вимог щодо обробки персональних даних щодо дітей, – до всіх норм, що містять згадку про дитину, повинен застосовуватись 18-річний віковий ценз. Для ст. 8 встановлений окремий правовий режим: її положення застосовується до дітей, яким не виповнилось 13–16 років. Ця подвійність правил щодо дітей може потенційно викликати деякі непорозуміння та неправильне використання GDPR¹. Видається, що дух норм GDPR не передбачає подвійності правового регулювання обробки персональних даних для дітей і положення щодо надання можливості неповнолітнім надавати самостійно згоду на обробку персональних даних може бути пояснено наступним.

Для того щоб теоретично обґрунтувати віковий ценз, встановлений в GDPR, необхідно встановити, для якого права застосовується даний вік. Вирішення даного питання є своєрідним в праві ЄС, оскільки Хартія основних прав Європейського Союзу (далі – Хартія) передбачає право на захист персональних даних в якості окремого права, – права, що не охоплюється правом на повагу до приватного життя. Так, ст. 7 говорить, що кожна людина має право на повагу до її приватного життя. У ст. 8 закріплюється право на охорону даних особистого характеру. Дещо інший підхід передбачений в Конвенції про права дитини 1989 року (ст. 16) та Конвенції про захист прав людини і основоположних свобод 1950 року (ст. 8): право на захист персональних даних не виділяється в якості окремого права, а розглядається в рамках права на повагу до приватного життя.

В Україні Міністерство юстиції надало роз'яснення «Деякі питання практичного застосування Закону України «Про захист персональних даних», в якому право на захист персональних даних розглядається як право людини на невтручання в її особисте життя². Аналогічним чином вирішено дане питання й у національно-

¹ *Krivokapic D., Adamovic J. Impact of General Data Protection Regulation on Children's Rights in Digital Environment // Annals of the Faculty of Law in Belgrade. 2016. 205 p.*

² *Роз'яснення Міністерства юстиції України «Деякі питання практичного застосування Закону України «Про захист персональних даних». URL: https://mijust.gov.ua/m/str_38266.*

му законодавстві більшості європейських держав (наприклад, Німеччини¹ або Франції²).

Незважаючи на поліінтерпритацію визначення права на захист персональних даних та права на повагу приватного життя, обидва ці права є немайновими правами, що в країнах континентальної правової сім'ї регулюються нормами цивільного права, відповідно питання щодо вікових можливостей реалізовувати дані права повинні вирішуватися за правилами цивільного права.

На думку Є. О. Харитонова, право на повагу до особистого життя є елементом правоздатності³. В теорії цивільного права при визначенні юридичного змісту виокремлюють динамічну та статичну теорії правоздатності. Відповідно до динамічної теорії зміст правоздатності залежить не тільки від її державного визнання, а й від того, якими конкретними правами володіє правоздатна особа, в яких відносинах з іншими суб'єктами вона фактично перебуває. Як стверджує статична теорія, зміст правоздатності повністю залежить від її державного визнання, а зовсім не від відносин її носія з іншими особами. У відносинах з іншими суб'єктами формуються конкретні правомочності й обов'язки, склад яких дійсно не залишається незмінним для кожної окремої правосуб'єктної особи. Але правоздатність – не конкретні права й обов'язки, а абстрактна і загальна передумова володіння ними⁴.

З огляду на той факт, що право на захист персональних даних чітко врегульовано нормативно-правовим актом, більш доцільною видається статична теорія правоздатності. Відповідно право на захист персональних даних як елемент правоздатності абстрактно виникає з моменту народження. Конкретними правомочностями суб'єкта персональних даних до досягнення дитиною відповідного віку (13–16 років) володіють батьки. Після подолання вікового порогу, правомочностями, які пов'язані з реалізацією права на захист персональних даних, наділяється неповнолітній. Аналогічно регулюється, наприклад, право на ім'я, що виникає з моменту народження. Первісно його здійснюють батьки, що реєструють новонародженого. Подальша зміна імені має певні вікові пороги: наприклад, згідно зі ст. 61-2 Цивільного кодексу Франції з 13 років

¹ Nolte N., *Werkmeister Ch.* Privacy in Germany: overview. URL: [https://uk.practicallaw.thomsonreuters.com/4-578-2349?transitionType=Default&contextData=\(sc.Default\)&firstPage=true&comp=pluk&bhcp=1](https://uk.practicallaw.thomsonreuters.com/4-578-2349?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1).

² Saarinen M., Ladousse J. Privacy in France: overview. URL: [https://uk.practicallaw.thomsonreuters.com/7-573-6346?transitionType=Default&contextData=\(sc.Default\)](https://uk.practicallaw.thomsonreuters.com/7-573-6346?transitionType=Default&contextData=(sc.Default)).

³ Харитонов Є. О. Коментар до публікації від 26 червня 2018 р. URL: <https://www.facebook.com/suzan.tsurkanu>.

⁴ Дзера О. В., Кузнецова Н. С., Майданик Р. А. Цивільне право України. Загальна частина. Київ: Юрінком Інтер, 2017. 1176 с.

батьки можуть змінити ім'я дитини лише за її згодою¹. З 16 років неповнолітній може самостійно звертатися із заявою про зміну власного ім'я.

Висвітлення вікового порогу надання згоди на обробку персональних даних через призму визначення правової природи права на захист персональних даних як елемента правоздатності дозволяє констатувати відсутність двох правових потоків, про які зазначають Хелена Коста і Мілда Маценайт. Встановлюючи вік надання згоди, держава тим самим розподіляє правомочності з права на захист персональних даних між батьками та дітьми, які являють собою єдине правове поле (без градації прав залежно від віку, як пропонували зазначені науковці). Отже, до досягнення відповідного віку (13–16 років) правомочностями права на захист персональних даних (право бути забутим, право на доступ до персональних даних, право на виправлення, право на обмеження опрацювання, право на мобільність даних, право на заперечення та ін.) володіють батьки (опікуни чи інші законні представники); з моменту настання віку, встановленого державою на надання згоди, неповнолітній самостійно здійснює передбачені правомочності.

Виходячи із вищезазначеного, можна констатувати, що GDPR не вступає у протиріччя з Конвенцією про права дитини у питанні визначення вікових меж дитинства, оскільки Загальний регламент не говорить про те, хто є дитиною, а лише встановлює особливості реалізації такого немайнового права як право на захист персональних даних. Звісно, під час застосування GDPR мають бути враховані особливості національного законодавства членів ЄС щодо емансипації неповнолітніх. Наприклад, у Литві чи Естонії неповнолітній може бути емансипований у віці 15 років на підставі судового дозволу. Для дівчат вік емансипації може бути меншим ніж 15 років у разі вагітності².

Повертаючись до можливих практичних проблем реалізації норм GDPR, необхідно зазначити, що ст. 8 GDPR вносить неузгодженість між державами-членами у європейському цифровому середовищі³. Зокрема, виникає питання: якщо в одній державі буде встановлена вимога у 13 років, а в іншій у 16 років для надання згоди батьками для обробки персональних даних, чи буде в останній дійсна згода надана особами старше 13 років. Крім того, оскільки від-

¹ Civil code of France. URL: https://www.legifrance.gouv.fr/content/download/1950/13681/version/3/.../Code_22.pdf.

² National report: Lithuania. URL: <http://cefflonline.net/wp-content/uploads/Lithuania-Parental-Responsibilities.pdf>.

³ Kamara I. Dr. Bart Van der Sloot "Children and data protection: awareness and effectiveness in a connected world". URL: <http://arno.uvt.nl/show.cgi?fid=144598>.

повідно до ст. 3 Регламенту його дія поширюється на підприємства, які засновані або мають місце знаходження за рамками території ЄС, але пропонують послуги/товари громадянам ЄС, виникає не-сумісність вимог GDPR з американським COPPA. Так, відповідно до ст. 1 COPPA дитиною вважається особа, яка не досягла 13 років¹. Відповідна позиція США не порушує норм міжнародного права оскільки США є однією з трьох країн, які й досі не підписали Конвенцію про права дитини. Сам факт «непідписання» Конвенції говорить про відкрите ігнорування Сполученими Штатами Америки міжнародних стандартів у сфері захисту прав дитини. Відповідно, американські компанії вимагатимуть згоди лише від батьків, чії діти не досягли 13-річного віку, що обумовить невідповідність їх діяльності вищим віковим вимогам європейських держав.

На сьогоднішній день вже є рішення Верховного суду США, що стосуються виконання приписів GDPR. Справа була порушена за ініціативою Європейської комісії щодо отримання ордеру на вилучення бази даних MICROSOFT CORPORATION, що використовується на території держав – членів Європейського Союзу. В мотивувальній частині Верховний суд зазначив, що згідно із ст. 49 GDPR для виконання даного запиту необхідно чітко визначити суспільний інтерес, який переслідують органи ЄС, надати гарантії захисту персональних даних у разі їх передачі та уточнити запит у частині, які саме дані необхідні заявнику². Правовою підставою для виконання цього запиту стала транскордонна дія GDPR. Факт визнання судовими інстанціями США транскордонної дії GDPR підкреслює можливі протиріччя під час застосування норм щодо віку отримання батьківської згоди.

Таким чином, можливі проблеми взаємного визнання опікунської згоди на обробку персональних даних дітей можуть бути вирішені наступним чином: по-перше, державам – членам Європейського Союзу необхідно визнавати батьківські згоди, надані в рамках вікової варіативності, встановленої в GDPR, незалежно від національного законодавства (тобто процес обробки персональних даних буде вважатися незаконним, якщо він відбувається без наявності батьківської згоди щодо дитини, якій не виповнилось 13 років); по-друге, з метою усунення правових колізій щодо віку на-

¹ Children's online privacy protection of the USA. URL: <http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim> [20.03.2018].

² Decision of Supreme Court of the United States in the matter of a warrant to search a certain e-mail account controlled and maintained by Microsoft Corporation United States of America. URL: https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf.

дання згоди між США та ЄС необхідно у міжнародних договорах про правову допомогу закріпити взаємне визнання законних підстав обробки персональних даних неповнолітніх.

Звісно, запропоновані варіанти вирішення вікових проблем надання згоди можуть призвести до того, що в кінцевому рахунку дана згода буде необхідна лише для обробки персональних даних дітей, які не досягли 13 років, що не зовсім відповідає буквальному тлумаченню ст. 8 GDPR. Але якщо, наприклад, у Німеччині парламент вирішить встановити 16-річний вік для надання згоди на обробку даних, то для всіх німецьких компаній дана вимога буде обов'язковою, в той час як вже американські або литовські компанії будуть діяти незаконно лише у разі відсутності згоди на обробку персональних даних дитини, що не досягла 13 років.

З метою підтвердження зробленого тлумачення GDPR щодо віку зазначимо ще один аргумент.

У процесі прийняття GDPR на етапі розгляду проекту в Європейському парламенті від одного з парламентаріїв надійшла пропозиція підвищити вік надання згоди на обробку персональних даних дітей до 18 років, мотивуючи це тим, що дітям як уразливим суб'єктам права необхідний особливий захист від тих загроз, що існують в мережі Інтернет. Дана пропозиція не знайшла підтримки, оскільки це створювало непомірні обтяження для функціонування компаній та викликало обурення серед молоді у контексті порушення їх права на інформацію та вираження власної думки¹.

Дійсно, питання надання згоди батьками на обробку персональних даних до досягнення певного віку дитиною є кроком встановлення державою потрібного контролю: контролю за дітьми власними батьками і, як наслідок, обмеження їх права на таємницю особистого життя (права на інформацію, власну думку), що було необхідно для захисту прав з урахуванням їх уразливості в мережі; контролю компаній за виконанням батьками свого обов'язку виховувати інет-культуру дітей, адже без згоди батьків, компанії не може надавати послуги, в результаті чого вона щільно слідкує за реакцією батьків щодо поведінки дітей в мережі; нарешті, контроль держави за законністю обробки персональних даних компаніями, що проявляється у накладенні штрафних санкцій у разі порушення норм GDPR. Такий потрібний контроль є свідченням встановлення кордонів публічно-правового регулювання з приватноправовим регулюванням у питанні захисту персональних даних.

Отже, встановлення європейськими законодавцями варіативності віку (13–16 років) у GDPR говорить нам про їх намір надати

¹ Amendments 1014 and 1019 by Axel Voss. URL: <https://www.tandfonline.com/doi/full/10.1080/13600834.2017.1321096>.

дискретні повноваження державам – членам ЄС у вирішенні питання «свободи дій» неповнолітніх з певного віку та полегшення роботи компаній.

Вельми цікавим видається той факт, що розробники передбачили випадки можливого протиріччя інтересів дитини та поведінки батьків. Про це говорить п. 38 GDPR, згідно з яким «згоду особи, що несе батьківську відповідальність, не можна вимагати в контексті надання профілактичних або консультаційних послуг безпосередньо дитині»¹. Дана норма передбачена з метою попередження порушення батьками прав дитини, наприклад, у разі застосування насильства дитина може скористатися консультативними послугами і звернутися за допомогою.

Іншим випадком порушення прав дитини під час надання згоди на опрацювання персональних даних є узурпація влади батьками над своєю дитиною. Інакше кажучи, замість забезпечення захищеного використання персональних даних неповнолітнього опікуни можуть порушувати його право на конфіденційність. Співвідношення права батьків на захист персональних даних дитини з правами дитини на конфіденційність, інформацію, вираження власної думки, правом на доступ до Інтернету складає окрему проблему, що може стати предметом подальших досліджень.

Крім безпосереднього «зіткнення» інтересів дитини та дій батьків, можливі випадки завуальованого порушення права дитини на захист персональних даних, що обумовлюється «людським фактором» поведінки батьків. Як зазначає Хелена Кості та Мілда Маченайт, GDPR вимагає від батьків отримати згоду на всі типи послуг інформаційного суспільства в різних секторах. Перевантаження запитів на згоду може призвести до «втоми через згоду» серед батьків, коли постійний процес погодження стає тривожним роздратуванням, а не серйозним вибором і може зробити ілюзорне надання всієї батьківської згоди². Такий підхід зумовить або повсякчасну відмову у наданні згоди на обробку персональних даних, або згода батьків набере ознак формальності і персональні дані дитини будуть залишатися не захищеними.

¹ Регламент (ЕС) 2016/679 Европейского парламента и совета 27 апреля 2016 «О защите физических лиц в отношении обработки личных данных и о свободном движении таких данных, а также об отмене Директивы 95/46/ЕС (общее регулирование защиты данных)». URL: <https://internetinstitute.ru/wp-content/uploads/2017/07/Telecom-Data-Retention-Leg-appendix2.pdf>.

² *Macenaite M., Kosta E.* Consent for processing children's personal data in the EU: following in US footsteps?// Information & Communications Technology Law. 2017. Vol. 26, Iss. 2. URL: <https://www.tandfonline.com/doi/full/10.1080/13600834.2017.1321096>.

Є два можливі варіанти вирішення цієї проблеми: по-перше, цілком розумною видається думка щодо переміщення «центрів контролю» за використанням персональних даних дітей від батьків до контролерів/операторів, адже набагато легше контролерам/операторам не використовувати заборонені методи збору та обробки даних (наприклад, профілювання, поведінкова реклама, кросплатформенність, націлювання на геолокацію та ін), аніж отримання повсякчасної згоди батьків¹; по-друге, в деяких європейських країнах (наприклад, Франції) передбачається вікова залежність згоди на обробку персональних даних від виду інформаційних послуг, що надаються, та сфери використання отриманої особистої інформації: існуючі веб-сайти та служби зазвичай зазначали мінімальний вік (не менше 16 чи 18 років) в інформаційному полі користування послугами, чим відмічали необхідність отримання згоди.

Отже, розглянемо види інформаційних сервісів, яким для опрацювання персональних даних дітей необхідна згода батьків.

У процесі обговорення GDPR в Європейському парламенті депутати неодноразово домагалися підвищення віку надання самостійної згоди на обробку персональних даних². На їх думку, такий підхід зміг би забезпечити не лише конфіденційність персональних даних дітей, але й допоможе «уберегти» дітей від контенту, що містить насильство³.

До вступу у дію GDPR «дорослі» сайти в графі правила та умови користування сайтом прописували: користувачі мають знати, що у разі використання послуг сайту, для всіх третіх осіб, їм не менше 16 років⁴. Такий підхід, звісно, ставить питання щодо подальшого вдосконалення механізму захисту прав дитини онлайн, у тому числі за допомогою імперативних заходів перевірки особи під час реєстрації.

Буквальне тлумачення ч. 1 ст. 8 GDPR свідчить про те, що згода від батьків необхідна лише у відношенні пропозицій послуг інформаційного суспільства безпосередньо дитині (в подальшому си-

¹ *Montgomery K. C., Chester J.* Data Protection for Youth in the Digital Age: Developing a Rights-Based Global Framework (2015) 1(4) European Data Protection Law Review, 291 p.

² Поправка 1006 від Csaba Sygo (віком від 14 років), поправка 1008 Манфреда Вебера (віком 15 років), поправка 1009 Біргіта Сіпеля, Петри Кампереверт та Йозефа Вайденхольца (16 років), поправка 1012 Жан П'єр Ауді, Сеон Келлі (15 років).

³ *Albrecht J. P.* Draft report. AMENDEMENTS (3) 886–1188. URL: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/am/928/928600/928600en.pdf.

⁴ *Carr J.* 'The point about 16: implication of the GDPR for child grooming laws' (2016), LSE Media and Policy, (London 12 January 2016). URL: <http://blogs.lse.ac.uk/mediapolicyproject/2016/12/01/the-point-about-16-implications-of-the-gdpr-for-child-grooming-laws>.

нонімічно до поняття «послуга інформаційного суспільства» буде використовуватись поняття «онлайн-послуги», «веб-сайти», «контент», онлайн-сервіси»). Відповідно, веб-сайти, що містять інформацію насильницького характеру, не підпадають під дію GDPR.

Разом з тим у всіх європейських державах забороняється порнографія для неповнолітніх, та перевірка віку під час користування такими інформаційними послугами передбачена в деяких країнах, наприклад, у Німеччині з 2007 року¹, Великобританії з 2018 року².

Отже, на сьогоднішній день норми GDPR поширюються на сайти для дорослих лише у разі наявної обов'язкової реєстрації або іншої ідентифікації особи, що дає змогу персоніфікувати її. Відповідно неповнолітні у разі реєстрації не зможуть отримати доступ до контенту, що має насильницький характер, оскільки національні законодавства держав – членів ЄС забороняють надання відповідних послуг дітям. Перед національними парламентами стоїть завдання законодавчо забезпечити обов'язок вікової верифікації при наданні послуг шкідливого змісту.

Більш складною є ситуація, коли засоби вікової перевірки виявляються недієвими і дитина, зазначаючи неправдивий вік, отримує доступ до дорослого контенту. Звісно, основну відповідальність у таких випадках несуть батьки, які виконують свої обов'язки щодо виховання дитини неналежним чином. Але є засоби і технічного характеру (наприклад, файли cookie), які допомагають відстежити вік (як і іншу особисту інформацію) користувача без отримання персональних даних.

Якщо із «забороненими для неповнолітніх сервісами» все зрозуміло у таких випадках, то навколо інших онлайн-послуг виникає чимало питань.

Виходячи із закріплених нормативних положень послуги інформаційного суспільства можуть бути представлені у вигляді: інтерактивної інформації, інтерактивної реклами, інтерактивної покупки, інтерактивного укладання контрактів. Цими послугами можуть користуватись як дорослі, так і діти, тому закономірно виникає питання: чи для всіх послуг, що активно отримують персональні дані, необхідна згода батьків? Інакше кажучи, наприклад, чи необхідно отримувати згоду батьків сайтам продажу продуктів харчування або сайтам, які містять контент, спрямований на бізнес-аудиторію?

Американські правозастосовці при відповіді на це питання користуються критеріями оцінки веб-сайтів: відповідно до п. 312.2

¹ *Carmen Palzer, German. Age Verification System Standards for Youth Protection// IRIS 2003-10:14/30. URL: <http://merlin.obs.coe.int/iris/2003/10/article30.en.html>.*

² *Barr S. Some argue that this tool could be used as a breach of privacy. URL: <https://www.independent.co.uk>.*

Кодексу федеральних постанов при визначенні того, чи веб-сайт або сервісне обслуговування онлайн або його частина спрямовані на дітей, Комісія буде розглядати її предмет, візуальний контент, використання анімованих персонажів або дітей, орієнтованих заходів та стимулів, музики та іншого аудіовмісту, вік моделей, наявність дитячих знаменитостей або знаменитостей, які звертаються до дітей, мову або інші характеристики веб-сайта чи онлайн-служби, а також чи реклама, що відображається на веб-сайті чи онлайн-службі, спрямована на дітей. Комісія також розгляне компетентні та надійні емпіричні докази, що стосуються складу аудиторії, а також свідчення про цільову аудиторію. Веб-сайт або онлайн-служба вважаються спрямованими дітям, коли вони мають фактичні знання про те, що вони збирають особисту інформацію безпосередньо від користувачів іншого веб-сайта чи онлайн-служби, спрямованої на дітей¹.

Практика застосування цієї норми свідчить про те, що, наприклад, сайти продажу продуктів харчування (наприклад, KENTUCKY FRIED CHICKEN (<http://www.kfc.com>), Макдональдс (<http://www.mcdonalds.com>), SNICKERS (<http://www.snickers.com>) повинні отримувати згоду законних представників дитини для опрацювання її персональних даних. Ці сайти включають в себе ігри, головоломки, конкурси, вікторини, загадки, музику, електронні листи, рекламні ролики, тоталізатори, завантажуванні рецепти, шпалери для робочого столу та заставки².

Крім того, інтерес викликає і припис COPPA щодо можливих джерел отримання персональних даних від дітей. Згідно зі ст. 4 інформація про дитину може бути отримана з веб-сайта чи онлайн-служби, призначеної дітям, або через домашню сторінку веб-сайта; пільговий сервіс; електронну пошту; дошку оголошень; чат³.

Отже, аналіз американської правозастосовної практики щодо отримання згоди батьків (опікунів) від інформаційних сервісів дає змогу класифікувати їх на три групи: 1. Веб-сайти, які містять контент, направлений на дорослу аудиторію (згода не потрібна); 2 Веб-сайти, що мають змішану аудиторію (згода необхідна); 3. Веб-сайти, що направлені на дитячу аудиторію (згода необхідна).

¹ Electronic Code of Federal Regulations. URL: https://www.ecfr.gov/cgi-bin/text-idx?SID=ce3a58c7e136396386618bf77568826b&mc=true&node=se16.1.312_15&rgn=div8.

² *Story M., French S.* Food Advertising and Marketing Directed at Children and Adolescents in the US // U.S. National Library of Medicine. Published online 2004 Feb 10. URL: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC416565>.

³ Children's online privacy protection of the USA. URL: <http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim> [20.03.2018].

В цілому такий підхід міг би бути реципований й при тлумаченні ст. 8 GDPR, яка закріплює термін «інформаційні послуги, що пропонуються безпосередньо дітям». Варто звернути увагу лише на тому, що веб-сайти, які мають змішану аудиторію, для законності функціонування повинні отримувати інформацію щодо віку особи.

БЛОКУВАННЯ, ФІЛЬТРАЦІЯ ТА ВИДАЛЕННЯ КОНТЕНТУ В СОЦІАЛЬНИХ МЕРЕЖАХ

Ерік Шмідт¹ і Джерард Коен² з компанії Google прогнозують, що «кожна держава спробує регулювати Інтернет ... всі країни – від найбільш демократичних до авторитарних – намагаються спроектувати закони з реального світу на світ віртуальний»³. Ці тенденції прослідковуються у багатьох сучасних країнах (Великобританія, Ізраїль, Китай, Німеччина, Росія, США, Україна). Уряди цих держав почали збільшувати свій контроль над кіберпростором і демонструють готовність втрутитися в комунікацію між користувачами в Інтернеті.

В останні роки зростає кількість випадків використання програмного забезпечення для управління контентом з метою обмеження або контролю доступу до його вмісту. Це перш за все використовується для фільтрації матеріалів, переданих через Інтернет, електронну пошту, соціальні мережі або інші онлайн-засоби. Чимало установ використовують блокування доступу до інтернет-сайтів, щоб обмежити можливість працівників користуватися соціальними мережами у робочий час, а також спостерігається тенденція до впровадження фільтрації в Інтернеті для захисту дітей від шкідливих матеріалів і зменшення доступу порнографії. Деякі держави блокують доступ до інтернет-контенту з метою «забезпечення прав інтелектуальної власності», «захисту національної безпеки», «збереження культурних норм і релігійних цінностей».

Блокування – це заходи, що використовуються з метою попередження надходження певного контенту до кінцевого користувача. До них належать: закриття для користувачів доступу до конкретних веб-сайтів, адрес інтернет-протоколу і доменних зон, видалення веб-сайтів з веб-сервера, на яких вони розміщені, або ви-

¹ Голова ради директорів компанії Google.

² Засновник і директор наукового центру Google Ideas.

³ Шмідт Е., Коен Дж. Новий цифровий світ / пер. з англ. Г. Ленів. Львів: Літопис, 2015. С. 91.

користання технологій фільтрації, що перешкоджають появі сайтів, які можуть містити матеріали, ключові слова або інший контент. Механізми, які використовують для управління інформацією і цензури в Інтернеті, стають все більш технічно складними із застосуванням багаторівневих систем контролю, часто прихованих від користувачів¹.

Незважаючи на існування технічної можливості блокувати інтернет-контент², у світі сформувалися дві правові моделі регулювання блокування, фільтрації та видалення інтернет-контенту.

Перша модель полягає у відсутності в держав законодавства з питань блокування, фільтрації та видалення інтернет-контенту (Австрія, Великобританія, Ірландія, Нідерланди, Німеччина, Польща, Чехія та Швейцарія). Тобто у наведених країнах не існує законодавчо визначених умов і процедур, яких повинні дотримуватися суб'єкти, що беруть участь у блокуванні, фільтрації та видаленні інтернет-контенту.

Наприклад, у Великобританії відсутні конкретні нормативно-правові норми щодо блокування сайтів. Так, для блокування інформації про жорстоке поводження з дітьми та непристойного контенту для дорослих британські інтернет-провайдери впроваджують технічну систему, розроблену British Telecom під назвою «Система очищення» (список URL-адрес і доменних імен, який підтримується галузевим регуляторним органом «Internet Watch Foundation»). Система передбачає двоетапну переадресацію IP-адрес і систему блокування URL-адрес на основі DPI, здатна блокувати веб-сайти, розміщені на загальних IP-адресах, без блокування інших сайтів, розміщених за тією ж адресою. Такий же метод використовується для блокування матеріалів, які заохочують терористичну діяльність. Для блокування наклепницького контенту та контенту, що порушує авторські права, торгові марки або закони про конфіденційність інтернет-провайдери повинні застосовувати конкретні методи, викладені у відповідному судовому рішенні, прийнятому Високим судом Лондона³. У Нідерландах та Німеччині повноваження щодо

¹ Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. 16 May 2011. URL: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

² Укладачі доповіді «Перспективи блокування інтернет-контенту» (Perspectives on Internet Content Blocking: An Overview) виділяють 5 типів блокування контенту: 1) блокування IP-адрес і протоколів; 2) блокування контенту за допомогою DNS; 3) блокування сайтів за URL-адресою; 4) блокування на інтернет-платформах (пошукові системи, наприклад Google); 5) блокування DPI. Internet Society Perspectives on Internet Content Blocking: An overview. Internet Society, March 2017. URL: <https://www.internetsociety.org/wpcontent/uploads/2017/03/ContentBlockingOverview.pdf>.

³ Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Cont-

блокування інтернет-контенту покладено на муніципальні суди з метою забезпечення балансу між свободою вираження поглядів та захистом інших основних прав людини¹.

Друга модель об'єднує країни, в яких законодавство передбачає юридичні підстави, відповідно до яких може бути застосовано блокування або видалення контенту адміністративними чи судовими органами, які мають компетенцію приймати належні заходи і процедури, яких слід дотримуватися.

Загалом, у даній групі держав блокування доступу до інтернет-ресурсів застосовується відповідно до ч. 2 ст. 10 Конвенції про захист прав людини і основоположних свобод, а саме з метою: захисту національної безпеки, територіальної цілісності або громадської безпеки, для запобігання заворушенням чи злочинам, для охорони здоров'я чи моралі, для захисту репутації чи прав інших осіб, для запобігання розголошенню конфіденційної інформації². Однак деякі держави законодавчо розширили підстави для блокування доступу до інтернет-ресурсів. Для попередження та уникнення жорстокого поводження з дітьми, тероризму, злочинності (зокрема злочинів на ґрунті ненависті) і національної безпеки у деяких державах прийняті норми, що регулюють питання блокування інтернет-контенту та забезпечують термінове блокування таких матеріалів без необхідності прийняття судового рішення. Така практика існує в таких країнах, як Росія, Франція і Туреччина. Адміністративним або правоохоронним органам надано повноваження прийняття рішення про блокування доступу до інтернет-контенту без судового рішення. Зазвичай такі рішення передбачають здійснення блокування провайдерами інтернет-доступу протягом 24 годин і без будь-якого повідомлення постачальника контенту³.

У деяких країнах формується тенденція до тимчасового блокування з метою позбавлення користувачів можливості отримувати та розповсюджувати інформацію в політично значимі періоди, такі як вибори, соціальні протести або святкування річниці важливих істо-

en, prepared by the Swiss Institute of Comparative Law, commissioned by the Council of Europe, 20 December 2015, Lausanne. URL: <https://www.coe.int/en/web/freedom-expression/studyfiltering-blocking-and-take-down-of-illegal-content-on-the-internet>.

¹ Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content, prepared by the Swiss Institute of Comparative Law, commissioned by the Council of Europe, 20 December 2015, Lausanne. URL: <https://www.coe.int/en/web/freedom-expression/studyfiltering-blocking-and-take-down-of-illegal-content-on-the-internet>.

² Конвенція про захист прав і свобод людини і громадянина: від 4 листоп. 1950 р. URL: http://zakon5.rada.gov.ua/laws/show/995_004.

³ Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content, prepared by the Swiss Institute of Comparative Law, commissioned by the Council of Europe, 20 December 2015, Lausanne. URL: <https://www.coe.int/en/web/freedom-expression/studyfiltering-blocking-and-take-down-of-illegal-content-on-the-internet>.

ричних подій. У цей час заблоковано доступ до соціальних мереж, таких як Twitter і Facebook, як це було в період протестів у країнах «Арабської весни» у 2010–2011 роках (Алжир, Бахрейн, Єгипет, Ємен, Йорданія, Ірак, Кувейт, Ліван, Лівія, Мавританія, Марокко, Оман, Саудівська Аравія, Сирія, Судан, Туніс) та під час військового перевороту в Туреччині у липні 2016 року.

Прогнозуючи розвиток блокування доступу до зв'язку та Інтернету, Е. Шмідт і Дж. Коен зазначають, що авторитарні країни недовго думатимуть перед тим, як заборонити одноранговий зв'язок або взяти його під контроль. А от демократичні країни діятимуть помірковано перед застосуванням будь-яких обмежень у цій сфері. Так, під час масових заворушень у Великобританії в серпні 2011 року, протестувальники вимагали відновити справедливість у справі Марка Деггана, якого застрелили працівники поліції в Тоттенгемі. Через декілька днів протести переросли в сутички, внаслідок яких загинуло п'ятеро людей і пошкоджено майна на суму 300 млн фунтів стерлінгів. На думку уряду Великобританії, цьому найбільше посприяли такі засоби комунікації, як Twitter, Facebook і особливо BlackBerry. Коли протести припинилися, британський прем'єр-міністр Девід Кемерон виступив у парламенті та повідомив про можливість блокування цих соціальних сервісів у певних ситуаціях, зокрема тоді, «коли відомо, що люди задумують розбій, безпорядки та злочини»¹.

В авторитарних державах поширена практика довгострокового блокування або обмеження доступу до соціальних мереж: Венесуела (Twitter), Іран (Facebook, Twitter), Китай (Facebook, Twitter, Instagram), Пакистан (Facebook), Російська Федерація (Linkedin, Telegram), Саудівська Аравія (Facebook), Туркменістан (Facebook, Twitter, Instagram). Наприклад, політика уряду Китаю щодо соціальних мереж полягає в блокуванні міжнародних сайтів (Google Plus; Facebook; Twitter; Instagram) і створенні виключно «китайських» цензурованих соціальних мереж. Замість Twitter в Китаї функціонує Weibo (<http://tw.weibo.com>), а замість Facebook є Renren (<http://www.renren.com>).

В Україні сформувалася окрема практика блокування доступу до деяких російських соціальних мереж. Так, з метою «формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни»², 25 лютого 2017 року Президент України Указом № 47/2017 ввів у дію рішення Ради

¹ Шмідт Е., Коен Дж. Новий цифровий світ / пер. з англ. Г. Ленів. Львів: Літопис, 2015. С. 81.

² Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 р.

національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»¹. У цьому документі визначено, що для забезпечення інформаційної безпеки слід законодавчо врегулювати не лише механізм блокування, але й виявлення, фіксації та видалення з українського сегмента мережі Інтернет інформації, яка загрожує життю, здоров'ю громадян України, пропагує війну, національну та релігійну ворожнечу, зміну конституційного ладу насильницьким шляхом або порушення територіальної цілісності України, загрожує державному суверенітету, пропагує комуністичний та/або націонал-соціалістичний (нацистський) тоталітарні режими та їхню символіку².

15 травня 2017 року Президент України підписав Указ щодо застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій), зокрема, до ТОВ «Мэйл.РУ ГРУП», ТОВ «ВКонтакте», ТОВ «ВКонтакте», ТОВ «Мейл.РУ Україна» у формі заборони Інтернет-провайдером надання послуг з доступу користувачам мережі Інтернет до ресурсів сервісів «Mail.ru» та соціальних мереж «ВКонтакте» та «Одноклассники»³. Однак в цьому Указі не зазначено причин та механізму блокування доступу до цих інтернет-сервісів, що зумовило неоднозначні оцінки експертів та широкої громадськості. Проте блокування даних інтернет-сервісів слід розглядати крізь призму «забезпечення національної безпеки»⁴, а не «обмеження свободи слова». Особливої значущості ця

«Про Доктрину інформаційної безпеки України»: указ Президента України від 25 лют. 2017 р. № 47/2017 // Офіційний вісник України. 2017. № 20. Ст. 554.

¹ Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: указ Президента України від 25 лют. 2017 р. № 47/2017 // Офіційний вісник України. 2017. № 20. Ст. 554.

² Там само.

³ Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»: указ Президента України від 15 трав. 2017 р. № 133/2017 // Офіційний вісник України. 2017. № 41. Ст. 1276.

⁴ Крім звернення до суду з метою скасування Указу Президента України «.....» громадянин України А. А. Ткаченко 16 травня 2017 року зареєстрував електронну петицію № 22/036543-еп до Президента України «Отменить блокировку интернет-ресурса ВКонтакте». Президент України відмовив у задоволенні електронної петиції щодо скасування блокування інтернет-ресурсу «ВКонтакте», мотивуючи наступним: соціальні мережі використовуються російськими спецслужбами для просування російської пропаганди і проведення спеціальних інформаційних операцій проти України та її громадян; вказані компанії сприяють спецслужбам Росії у збиранні, зберіганні, використанні та поширенні інформації з обмеженим доступом — персональних даних та особистого листування громадян України; українські користувачі російських мереж потрапляють під контроль спецслужб РФ; контент наповнення цих ресурсів мережі Інтернет спрямований на намагання маніпулювати суспільною свідомістю через поширення недостовірної, неповної та упередженої інформації; російські соціальні мережі

теза набуває в контексті зміни політики соціальної мережі Facebook після виявлення створення Росією фейкових акаунтів для поширення у соціальній мережі політичної реклами під час виборів президента США у 2016 році¹.

На початку червня 2017 року даний Указ Президента України² оскаржено до Вищого адміністративного суду України в частині блокування доступу до інтернет-ресурсів. Позивач вказав, що оскаржуваний Указ у зазначеній частині прийнятий всупереч вимогам Закону України «Про санкції», порушує права на свободу вираження поглядів у відповідності зі ст. 10 Конвенції про захист прав людини та основоположних свобод, а також порушує право позивача на свободу доступу до інформації.

Однак Вищий адміністративний суду України відмовив у задоволенні позовних вимог через відсутність правових підстав, мотивуючи свою позицію тим, що у даному випадку спірним є не користування мережею в цілому, а лише заборона Інтернет-провайдером на певний період здійснювати надання послуг з доступу користувачам мережі Інтернет до ресурсів певних сервісів, яка, у свою чергу, не створює перешкод для користування будь-якими іншими сервісами. Крім цього, на думку суддів Вищого адміністративного суду України, спірним Указом позивача не обмежено у виборі форм і джерел одержання інформації. Окремі перешкоди, які можуть виникнути в процесі використання заблокованих інтернет-ресурсів, не обмежують права громадян на використання цих ресурсів, а спричинені виключно необхідністю створення негативних наслідків для осіб, щодо яких застосовано спеціальні економічні та інші обмежувальні заходи (санкції)³.

стали також розсадником деструктивних груп на кшталт сумнозвісних суїцидних спільнот типу «Синій кит»; соцмережа «ВКонтакте» залишається чи не головним вмістилищем «піратського» контенту у світі; взаємодія російських соціальних мереж з російськими спецслужбами у діяльності, спрямованій на шкоду суверенітету і територіальній цілісності України. Відповідь Президента України на електронну петицію № 22/036543-еп «Отменить блокировку интернет-ресурса ВКонтакте», розміщену на веб-сайті Офіційного інтернет-представництва Президента України 16.05.2017 громадянином А. А. Ткаченком. URL: <https://petition.president.gov.ua/petition/36543>.

¹ Цукербегр: Facebook виявив докази активності РФ в соцмережі і змінить алгоритми. URL: <https://hromadske.ua/posts/tsukerberh-facebook-vyiyavv-dokazy-aktivnosti-rf-v-sotsmerezhi-i-zminyt-alhorytmy>.

² Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»: указ Президента України від 15 трав. 2017 р. № 133/2017 // Офіційний вісник України. 2017. № 41. Ст. 1276.

³ Постанова Вищого адміністративного суду України: від 14 черв. 2017 р. у справі № 800/198/17. URL: <http://reyestr.court.gov.ua/Review/67196698>.

Зважаючи на відсутність правового механізму блокування доступу до інтернет-ресурсів в Україні, слід закріпити процедуру формування списків веб-сайтів з обґрунтуванням необхідності блокування кожного конкретного сайту. Будь-яке рішення про те, який контент необхідно блокувати, повинен приймати судовий орган.

Окрім блокування доступу до соціальних мереж, застосовується фільтрація онлайн-контенту. Найбільш яскравим прикладом фільтрації контенту в Інтернеті та соціальних мережах є «Проект Золотий Щит» (The Golden Shield Project), також відомий як «Великий китайський файрвол» (Great Firewall of China). Проект стартував у 2003 році та є системою серверів на інтернет-каналі між провайдерами і міжнародними мережами передачі інформації, що фільтрує інформацію. Китай реалізував найскладнішу фільтрацію інтернет-контенту, що здатна ефективно фільтрувати контент з використанням безлічі методів регулювання і технічного контролю (блокування IP-адрес і фільтрація контенту; фільтрація DNS і URL; скидання з'єднання тощо).

Фільтрація поширюється на «ключові слова», які внесені до «національного чорного списку» («демократія», «права людини», «диктатура», «пригнічення», «червоний терор», «Далай-лама»), які заблоковані під час запитів місцевих користувачів до іноземних пошукових систем.

Постачальники інтернет-послуг зобов'язані видаляти контент відповідно до вказівок цензорів. Так, у червні 2016 року заборона на незалежний збір або розповсюдження оригінальних новин була поширена на всі додатки для соціальних мереж, в той час як в липні 2016 року пекінський підрозділ адміністрації Китаю прийняв норми, що забороняють китайським інтернет-порталам створювати будь-які оригінальні новини, обмежуючи їх контентом, наданим невеликою кількістю дозволених «офіційних» джерел. Керівництво сайтів новин повинно цілодобово відстежувати зміст заміток і статей, щоб не допустити фактичних, стилістичних та інших помилок.

У серпні 2016 року Кіберпростір адміністрації Китаю (Cyberspace of Administration of China) встановив нові жорсткі вимоги до цензури для інтернет-провайдерів, у тому числі запроваджено постійний моніторинг вмісту новин і персональну відповідальність головних редакторів сайтів за контент.

З метою посилення державного контролю над Інтернетом, у листопаді 2016 року. Всекитайськими зборами народних представників ухвалено новий закон «Про кібербезпеку». Згідно з цим законом, фізичні особи та організації Китаю не мають права «шкодити безпеці, честі та інтересам держави» в Інтернеті. Також за-

коном забороняється діяльність в Інтернеті, спрямована на «повалення соціалістичної системи, розкол нації, підрив національної єдності, захист тероризму та екстремізму»¹.

Механізми, що використовуються для фільтрації інформації та цензури в онлайн-просторі, стають все більш технічно складними із застосуванням багаторівневих систем контролю, часто прихованих від користувачів.

Окрім блокування доступу до соціальних мереж та фільтрації їх контенту, також застосовується видалення вмісту в пошукових сервісах і соціальних мережах, які постійно отримують від різних осіб вимоги щодо видалення певної інформації з їх сервісів.

Основними причинами видалення вмісту в сервісах Google є наступні:

1) видалення вмісту через порушення авторських прав. Згідно з внутрішніми правилами, корпорація Google реагує на чіткі повідомлення про ймовірні порушення авторських прав. Веб-форма сповіщення відповідає зразку в законі США «Про захист авторських прав у цифрову епоху» (DMCA)² і забезпечує простий та ефективний механізм для власників авторських прав у всьому світі. Щоб розпочати процедуру видалення вмісту з результатів пошуку в Google, власник авторських прав, який вважає, що URL-адреса переспрямовує на правопорушний вміст, надсилає запит корпорації Google на видалення такого ймовірно правопорушного матеріалу. Отримавши запит на видалення, представники Google перевіряють його на повноту та наявність інших проблем. Якщо повідомлення повне і не знайдено інших проблем, представники Google видаляють URL-адресу з результатів пошуку Google;

2) запити на видалення вмісту від державних установ. Корпорація Google регулярно отримує від органів державної влади різних країн вимоги видалити з його сервісів такі матеріали, як записи в блогах, відео на YouTube або результати пошуку³.

¹ *Mozur P.* China's Internet Controls Will Get Stricter, to Dismay of Foreign Business. URL: <https://www.nytimes.com/2016/11/08/business/international/china-cyber-security-regulations.html>.

² Digital Millennium Copyright Act. 10,28,1998, Public Law No: 105–304. URL: <https://www.congress.gov/bill/105th-congress/house-bill/2281/text>.

³ У Google щодо причин видалення вмісту того чи іншого сайта зазначають наступне: «Уряди просять нас видалити або перевірити вміст із багатьох причин. Деякі запити містять звинувачення в наклепі, в інших указується, що вміст порушує місцеве законодавство, яке забороняє ворожі висловлювання чи вміст для дорослих. Закони, пов'язані з цими питаннями, відрізняються залежно від країни. Наша команда відносить кожний запит до певної категорії, як-от ворожі висловлювання, непристойний вміст або наклеп. Урядові запити на видалення часто стосуються вмісту політичного характеру та критики уряду. Намагаючись видалити політичний вміст із наших служб, представники урядів по-

Google отримує запити на видалення вмісту різними шляхами та від державних установ усіх рівнів. Це ухвали суду, письмові запити від центральних і місцевих державних установ, правоохоронних органів тощо. Іноді запити на видалення вмісту від державних установ надходять через користувачів (наприклад, скаржник долучає ухвалу суду як доказ того, що певний вміст заборонений). У деяких запитах просять видалити одразу кілька матеріалів або, навпаки, можуть надходити кілька запитів на видалення того самого матеріалу.

Однак не усі запити підлягають задоволенню, оскільки вони мають бути подані у письмовій формі, якомога точніше описувати вміст, який потрібно видалити, і пояснювати, чому цей вміст є незаконним. Не підлягає задоволенню запит, надісланий неналежним чином.

Google може відмовити у видаленні вмісту з різних причин. Деякі запити не містять точної інформації про елементи, які державний орган просить видалити (наприклад, у запиті не вказано URL-адресу). В інших випадках Google отримує скарги на наклеп, оформлені у вигляді офіційних листів від державних установ, а не ухвал суду. Приймаючи рішення про те, чи є повідомлення наклепницьким згідно з місцевим законодавством, Google зазвичай покладається на рішення суду.

Іноді письмових звернень від органів недостатньо й потрібна ухвала суду. Зазвичай Google покладається на рішення суду щодо того, чи повідомлення вважається наклепом згідно зі законодавством держави. Представники Google здійснюють перевірку законності отриманих документів, і якщо виявиться, що ухвала суду є фальшивою, не виконують її¹;

силаються на звинувачення в наклепі, порушення конфіденційності й навіть порушення законів про авторське право. Наша команда оцінює кожний запит і перевіряє вміст у контексті, щоб визначити, чи потрібно видалити вміст через порушення місцевого законодавства або нашої політики щодо вмісту». Запити на видалення вмісту від державних установ. URL: <https://transparencyreport.google.com/government-removals/overview?hl=uk>.

¹ Ось декілька прикладів отриманих корпорацією Google підроблених ухвал суду: ухвала канадського суду з вимогою видалити результати пошуку, які поширюються на три сторінки сайту forums.somethingawful.com. У підробленій ухвалі стверджується, що сайт містить наклепницькі заяви, однак не вказано, який закон порушується (Curt File № K819681. URL: <https://storage.googleapis.com/transparencyreport/faqs/governmentrequests/11639564.pdf>); ухвала окружного суду штату Пенсільванія з вимогою видалити блог, який нібито порушує авторські права особи, використовуючи її ім'я в різних публікаціях блогу (Document 116. Filed. 08/14/12. URL: <https://storage.googleapis.com/transparencyreport/faqs/governmentrequests/97858015.pdf>); ухвала суду Делі в Індії з вимогами видалити блоги й окремі публікації за ймовірний наклеп. Ухвали містили погрози покарати компанію Google за невиконання цих вимог (High Court of Chief Metropolitan Ma-

3) видалення результатів пошуку відповідно до закону про конфіденційність користувачів із ЄС. Згідно з рішенням Суду Європейського Союзу від травня 2014 року¹, користувачі мають право надсилати в пошукові системи, як-от Google, запити на видалення результатів пошукових запитів на основі імені людини. Пошукова система повинна видалити ці посилання, якщо вони «неадекватні, недоречні, неактуальні або надмірні», беручи до уваги чинники суспільного інтересу, зокрема роль людини в житті громадськості. Сторінки видаляються з результатів пошуку лише у відповідь на запити, які стосуються імені особи. Google видаляє URL-адреси з усіх європейських результатів пошуку Google (для користувачів з Іспанії, Німеччини, Франції тощо) і використовує дані геолокації, щоб обмежувати доступ до URL-адреси в країні, звідки надійшов запит на видалення;

4) контроль відповідності правилам спільноти YouTube. Google виявляє на YouTube вміст, що не відповідає його внутрішнім правилам (порнографія, заклики до насильства, переслідування чи ворожжі висловлювання), за допомогою спеціальних алгоритмів, а також завдяки скаргам, які надсилають користувачі. Скарги можуть надходити від систем автоматичного виявлення, учасників програми позначення невідповідних відео (неурядових організацій, державних установ і фізичних осіб) або користувачів спільноти YouTube;

5) видалення відповідно до Закону про регулювання вмісту в соціальних мережах. Так, в Німеччині 1 жовтня 2017 року набрав чинності закон про регулювання вмісту в соціальних мережах (NetzDG)². Відповідно до п. 2. § 1 цього закону, соціальні мережі, у яких зареєстровано понад 2 млн користувачів із Німеччини, мають локально видаляти «очевидно незаконний» вміст (наприклад, публікацію, зображення, відео) упродовж 24 годин після отримання сповіщення. Якщо законність важко визначити одразу, постачальник має розглянути запит упродовж семи днів. Цей процес може тривати довше лише в порядку виключення, наприклад, якщо залучено авторів вмісту або рішення приймає спільний галузевий орган чи установа регульованого саморегулювання. Щоб підлягати

gistrate. Commission of Law India. New Delhi 110001. May 2012. URL: <https://storage.googleapis.com/transparencyreport/faqs/governmentrequests/87941784.pdf>).

¹ Google Spain SL Google Inc. V Agencia Española de Protección de Datos (AEPD) Mario Costeja González Judgment of the Court (Grand Chamber) in Case C-131/12, 13 May 2014. URL: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=794833>.

² Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken. Ausfertigungsdatum: 01.09.2017. URL: <https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html>.

видаленню відповідно NetzDG, вміст має порушувати один із 22 законів Кримінального кодексу Німеччини, на який посилається NetzDG.

24 квітня 2018 року адміністрація Facebook опублікувала внутрішні рекомендації, які використовуються для ухвалення рішень про видалення контенту в цій соціальній мережі¹. Якщо модератори Facebook зафіксують порушення цих правил користувачами соціальної мережі, останнім можуть заборонити публікувати дописи, а згодом – відключать профіль. Facebook використовує комбінацію штучного інтелекту та звіти від осіб для визначення відео, зображень та іншого контенту, який порушує стандарти соціальної мережі².

У Стандартах соціальної мережі Facebook³ визначено перелік умов видалення дописів, якщо вони містять інформацію про:

- насильство (реальне насильство; небезпечних осіб та організації, які здійснюють: терористичну діяльність; організоване насильство; масові чи серійні вбивства; торгівлю людьми; організоване насильство чи злочинну діяльність; пропагування, рекламу злочинності та координування заподіяння шкоди);

- безпеку (пропагування, заохочення, координація чи надання вказівки щодо: самогубства; самоушкодження; харчових порушень; дитяча нагота й сексуальна експлуатація дітей /дорослих/; порушення конфіденційності та прав на конфіденційність зображень);

- вміст, що підлягає запереченню (пропаганда ненависті; насильство та графічний вміст; оголеність і сексуальна активність дорослих; жорстокість і нечуйність);

- цілісність та автентичність (спам; введення в оману; неправдиві новини);

- контент, який порушує авторські права та права на торговельну марку.

¹ Publishing Our Internal Enforcement Guidelines and Expanding Our Appeals Process By Monika Bickert, Vice President of Global Policy Management Facebook. URL: <https://newsroom.fb.com/news/2018/04/comprehensive-community-standards>.

² Віце-президент Facebook з публічної політики у Європі, Близькому Сході та Африці Річард Аллан зазначає, що штучний інтелект стане важливою частиною модерації, але він не зможе фільтрувати все. «Ми експериментуємо зі способами приховувати очевидно токсичну мову, продовжуючи інвестувати в ці перспективні технології. Проте попереду ще довгий шлях, допоки машинне навчання та штучний інтелект зможуть подолати складність, пов'язану з оцінкою ненависті». Richard Allan. Hard Questions: Who Should Decide What Is Hate Speech in an Online Global Community? URL: <https://newsroom.fb.com/news/2017/06/hard-questions-hate-speech>.

³ Стандарти спільноти Facebook. URL: <https://www.facebook.com/communitystandards/introduction>.

Зазвичай дописи видаляють після того, як на них скаржаться інші користувачі. Після отримання скарги, допис відправляється на модерацию.

Наслідки порушення Стандартів спільноти Facebook залежать від тяжкості порушення та історії користувача на платформі. Наприклад, Facebook може попередити користувача про перше порушення. Якщо користувач продовжить порушувати Стандарти соціальної мережі, то модератори можуть скасувати дозвіл на публікацію дописів у Facebook чи заблокувати профіль особи.

Отже, до інформації, що може бути обмежена в соціальних мережах, належить: дитяча порнографія (для захисту прав дітей), підбурювання до ненависті (для захисту прав вразливих категорій осіб), дифамація (для захисту прав і репутації інших осіб від незаконних нападів), пряме і публічне підбурювання до здійснення геноциду (для захисту прав інших осіб), будь-який виступ на користь національної, расової чи релігійної ненависті, що являє собою підбурювання до дискримінації, ворожнечі або насильства (для захисту прав людини)¹. Однак постає питання про межі допустимості держав і корпорацій у сфері блокування, фільтрації та видалення певних видів контенту.

На жаль, часто органи державної влади намагаються законодавчо обмежити, контролювати, обробляти і цензурувати контент, який розповсюджується через інтернет-ресурси, без будь-яких законних підстав або на основі суперечливих законів, що не обґрунтовують такі дії і/або здійснюють це непропорційно до заявленої мети. Такі дії явно не сумісні зі зобов'язаннями держав, передбаченими міжнародними нормами у сфері прав людини, і часто ще більше перешкоджають реалізації права на свободу слова.

Насамкінець необхідно зазначити, що використання державами і корпораціями технологій блокування, фільтрації та видалення онлайн-контенту часто є порушенням їхніх зобов'язань щодо гарантування права на свободу слова, адже:

1) конкретні підстави для блокування, фільтрації та видалення інтернет-контенту не закріплені в законодавстві або вони вкрай широко і нечітко прописані в законах, що створює небезпеку довільного і надмірного їх застосування;

2) блокування, фільтрація та видалення інтернет-контенту не завжди спрямоване на виконання цілей, передбачених в ч. 2 ст. 10 Конвенції про захист прав людини і основоположних свобод, та ч. 3 ст. 19 Міжнародного пакту про громадянські і політичні пра-

¹ Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. 16 May 2011. URL: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

ва, а списки сайтів, які підлягають блокуванню, зазвичай не розголошуються, що ускладнює оцінку того, чи є обмеження доступу до контенту законним;

3) навіть у випадку обґрунтування заходів блокування, фільтрації та видалення інтернет-контенту вони є зайвими і непропорційними досягненню поставленої мети, оскільки часто є неналежно обґрунтованими і зумовлюють закриття доступу до більшого обсягу контенту, ніж той, який вважається незаконним;

4) контент часто блокують без участі судового або незалежного органу або без можливості перегляду відповідного рішення цими органами.

ПОНЯТТЯ ТА ВИДИ ІНФОРМАЦІЙНИХ ПРАВОПОРУШЕНЬ У СОЦІАЛЬНИХ МЕРЕЖАХ

Інтенсивність розвитку та впровадження інформаційних технологій та засобів зв'язку в життєдіяльність суспільства активізувало увагу науковців до різних інформаційних проблем. Особливо актуальним напрямом наукових розвідок є розкриття окремих аспектів інформаційних правопорушень, зокрема в соціальних мережах.

Водночас нині на науковому та законодавчому рівні відсутнє уніфіковане бачення понятійно-термінологічного апарату у цій сфері, зокрема поряд з поняттям «інформаційні правопорушення» як синонімічні поняття застосовуються і інші: «комп'ютерні правопорушення», «ІТ-правопорушення», «інформаційні делікти», «інформаційні злочини», «комп'ютерні злочини», «правопорушення у сфері інформації» тощо. Не менш однозначно дослідниками визначаються й поняття, сутність, зміст, характерні риси інформаційних правопорушень. Відсутня також у наукових колах і єдність щодо визначення видів інформаційних правопорушень, підходів до віднесення тих чи інших правопорушень до інформаційних.

Нині серйозне занепокоєння викликає поширення фактів протизаконного збору і використання інформації, несанкціонованого доступу до інформаційних ресурсів та соціальних мереж, незаконного копіювання інформації в електронних системах, викрадення інформації з бібліотек, архівів, банків та баз даних, порушення технологій оброблення інформації, запуску програм-вірусів, троянів, фішингових програм, знищення та модифікація даних у інформаційних системах, перехоплення інформації в технічних каналах її витоку, маніпулювання суспільною та індивідуальною свідомістю тощо.

Особливо деструктивними є порушення права людини та громадянина на інформацію, а саме ненадання інформації органами державної влади, несвоєчасне чи неповне надання інформації, надання інформації, що не відповідає дійсності, тощо.

Тривалий час інформаційні правопорушення розглядалися крізь призму загроз інформаційній безпеці України, що закріплювалися у Законі України «Про основи національної безпеки України»¹.

Окремі питання юридичної відповідальності за інформаційні правопорушення досліджувалися крізь призму адміністративного та кримінального права. Зокрема такий підхід подано в роботах І. Арістової, О. Логінова, Г. Линника, П. Матвієнко, І. Сопілко, О. Стоєцького, О. Полушкіна, А. Туніка та ін.

У більшості наукових досліджень розглядаються окремі види правопорушень: кримінально-правові, цивільно-правові, адміністративно-правові тощо.

Для інформаційних правопорушень, зокрема в соціальних мережах, характерні всі ознаки, які властиві іншим видам правопорушень: суспільна небезпечність (шкідливість), протиправність, винність та караність.

Окрім загальних ознак інформаційні правопорушення в соціальних мережах мають і низку специфічних, тобто таких, які характерні винятково їм.

Інформаційні суспільні відносини неодмінно супроводжуються деліктними правовідносинами, що виникають з приводу вчинення правопорушення в інформаційній сфері. Підставою виникнення деліктних інформаційних правовідносин є факт вчинення правопорушення в інформаційній сфері. Виходячи із загальноправового поняття правопорушення, інформаційне правопорушення визначається як винне, суспільно небезпечне, протиправне діяння деліктоздатної особи, яка посягає на інформаційні інтереси власника або розпорядника інформації чи іншого учасника інформаційних відносин, за вчинення яких настає юридична відповідальність.

Ступінь суспільної небезпечності інформаційних правопорушень визначається соціальними цінностями, на які вони посягають. Беручи до уваги цей критерій, слід класифікувати інформаційні правопорушення на інформаційні делікти та інформаційні злочини.

Інформаційне правопорушення має загальні та спеціальні ознаки, що дозволяє виділяти їх в окрему групу.

Загальними ознаками інформаційного правопорушення є суспільна небезпека, протиправність, вина та деліктоздатність особи, яка його здійснила. Особливість та ступінь суспільної небезпеки інформаційного делікту визначаються соціальними цінностями, на які посягає правопорушник. До таких цінностей відноситься низка інформаційних прав, закріплених в Конституції України та інших нормативно-правових актах. Це може бути право на вільний

¹ Про основи національної безпеки України: Закон України // Офіційний вісник України. 2003. № 29. Ст. 1433.

доступ до інформації та свободу її поширення будь-якими способами, не забороненими законом, обмеження в доступі до окремих видів інформації, охорона та захист об'єктів інтелектуальної власності, втручання в особисте життя та збирання, зберігання, використання й поширення конфіденційної інформації про особу без її згоди тощо.

Спеціальними ознаками інформаційного правопорушення, що виділяє його серед інших, є вчинення деліктів в інформаційній сфері суспільних відносин, використання інформаційних технологій та засобів вчинення правопорушень. Інформаційні правопорушення мають складну структурну природу, що пояснюється єдністю соціально-конфліктного, інформаційного та юридичного елементів. Такі правопорушення вчиняються у сфері інформаційної діяльності людини, суспільства та держави зі створення, збирання, одержання, використання, поширення, охорони та захисту інформації тощо. Особливою ознакою правопорушень в інформаційній сфері є і той факт, що при їх вчиненні можуть використовуватися різні техніко-технологічні системи, прийоми та способи впливу на інформаційне середовище у вигляді комп'ютерної техніки та Інтернет-мережі, електронних засобів зв'язку тощо. Ця особливість вказує на широкий зміст інформаційного правопорушення, яким охоплюються такі поняття, як комп'ютерні правопорушення, кіберзлочинність та інші, пов'язані з нанесенням шкоди інформаційним технологіям.

Сутність інформаційного правопорушення проявляється у тісному поєднанні системи дозволів, заборон, обмежень та стимулів, що формують правовий режим в інформаційній сфері, з нормами, що встановлюють юридичну відповідальність за їх вчинення. Такий взаємозв'язок відіграє значну роль у формуванні складів інформаційних правопорушень та вирішенні питань протидії таким порушенням.

Складність природи інформаційних правопорушень визначає різноманітність методів та засобів попередження та припинення інформаційних деліктів, заснованих на нормах цивільного, адміністративного та кримінального права. Протиправність делікту в інформаційній сфері виражається в порушенні правових норм, що регулюють інформаційні відносини. Юридичні склади інформаційних деліктів закріплюються законами України та нормативно-правовими актами різних органів державної влади та органів місцевого самоврядування та їх посадових осіб. Необхідною ознакою інформаційних деліктів є вина у формі умислу або необережності, а ознакою караності за їх вчинення є застосування до правопорушників специфічних правових санкцій, передбачених нормами адміністративного, кримінального та цивільного права.

За сутністю інформаційний делікт є суспільно небезпечним посяганням на цінності, що охороняються інформаційним правом, шляхом спричинення або загрози спричинення їм шкоди. За змістом він є винним діянням суб'єкта правопорушення, що посягає на інформаційні відносини. За формою делікт є протиправною дією або бездіяльністю, за вчинення якої передбачена правова відповідальність. Тобто інформаційний делікт є юридичним фактом, що породжує право уповноваженої державою особи притягнути винну особу до юридичної відповідальності.

Між уповноваженим органом чи його посадовою особою та правопорушником виникають владні правовідносини юридичної відповідальності, засновані на механізмі державно-правового примусу до винної особи. Віднесення складу правопорушення до того чи іншого виду залежить від ступеня суспільної небезпеки, розміру заподіяної шкоди, особи правопорушника, інших кваліфікуючих ознак, що впливають на рівень відповідальності.

Таким чином, інформаційним правопорушенням визнається протиправне, суспільно небезпечне, винне посягання деліктоздатного суб'єкта на інформаційні інтереси людини, суспільства і держави, що охороняються законом, за яке встановлена юридична відповідальність.

За останні роки величезної популярності набули сайти соціальних мереж. Це сайти, що дозволяють користувачам завантажувати інформацію на загальнодоступний профайл, створювати он-лайн список друзів і переглядати профайли інших користувачів.

Соціальна мережа – соціальна структура, утворена індивідами або організаціями. Вона відображає зв'язки між ними через різноманітні соціальні взаємовідносини, починаючи з випадкових знайомств і закінчуючи тісними родинними зв'язками.

Зазначимо, що Інтернет швидко став основним інструментом для здійснення права на вираження думок, ідей, поглядів, реалізації права на свободу слова. Утім через різноманітність змісту і простоту використання Інтернет-інформація стала спірною і суперечливою та може використовуватися в різних цілях. З одного боку, наприклад, це дозволяє отримати відомості про поточні події в країнах, де інші засоби масової інформації піддаються жорсткій цензурі; з іншого – Інтернет може бути використаний з метою сприяння вчиненню правопорушення і навіть злочину.

Насамперед слід зазначити, що першочергово Інтернет¹ створювався як мережа для вільного поширення та одержання корисних для суспільства даних з урахуванням норм права та морально-етич-

¹ Турута О. Інтернет і право на свободу слова (порівняльно-правовий аспект) // Публічне право. 2012. № 4 (8). С. 31–32.

них принципів, що забезпечують соціальну справедливість і рух у напрямі до свободи. Проте, на жаль, на сьогоднішній день Інтернет перетворився на повсякденний засіб висилання будь-якої інформації, не завжди достовірної, що досить часто призводить до порушення прав людини.

Широке використання Інтернету породжує значні правові проблеми, що стосуються, зокрема, таких важливих питань, як: інформаційна безпека, права та свободи в галузі інформації, доступ до інформації, інформаційних ресурсів, інформаційних продуктів та отримання інформаційних послуг, ведення електронної комерції (торгівлі), оподаткування комерційної діяльності в Інтернеті, укладання договорів електронним способом, використання комп'ютерного програмного забезпечення, використання доменних імен, неправомірна поведінка користувачів у мережі (кіберсквотинг, тайпсквотинг, хакінг), охорона та захист прав інтелектуальної власності (авторських та суміжних прав, патентних прав, прав на засоби індивідуалізації та ін.).

Слід проаналізувати випадки порушення прав людини в соціальних мережах. З однієї сторони, можливість вільного висловлювання в мережі Інтернет користувачам гарантована Конституцією України¹, а саме, ст. 34 гарантовано право на свободу думки і слова, вільне вираження своїх поглядів і переконань. Виникає запитання, як захистити свою честь, гідність та ділову репутацію у разі їх порушення у всесвітній мережі Інтернет та хто буде нести відповідальність за таке порушення.

Інформаційні делікти в залежності від ступеня суспільної небезпеки поділяються на дисциплінарні, адміністративні, цивільні правопорушення та злочини. Критеріями такої класифікації інформаційних правопорушень є рівень суспільної небезпеки протиправних діянь в інформаційній сфері, нормативно закріплений вид та міра юридичної відповідальності суб'єкта інформаційного правопорушення тощо. Для правильної кваліфікації будь-якого правопорушення, у тому числі інформаційного правопорушення в соціальних мережах, важливо встановити його склад, елементами якого завжди виступають об'єкт та об'єктивна сторона, суб'єкт та суб'єктивна сторона.

Об'єктом інформаційного правопорушення в соціальній мережі є урегульовані нормами права суспільні відносини, що складаються в соціальних Інтернет-мережах. В якості об'єктів можуть виступати відносини у сферах забезпечення інформаційної безпеки, діяльності засобів масової інформації, охорони авторського права, бібліо-

¹ Конституція України: Закон України від 28 черв. 1996 р. № 254к/96-ВР // Відомості Верховної Ради України. 1996. № 30. Ст. 141.

течної та архівної справи, відносини у сфері правового режиму розповсюдження інформації з обмеженим доступом, таємницю особистого життя тощо. Їх предметом є матеріальні, духовні та інші соціальні блага, а також явища та процеси, дії та поступки суб'єктів по створенню таких благ. Об'єкт інформаційного правопорушення та його предмет виступають головним елементом, за яким проводиться його відмежування від інших складів правопорушень.

Об'єктивна сторона інформаційного правопорушення в соціальних мережах полягає в діях або бездіяльності суб'єкта правопорушення. Дії можуть бути у вигляді порушення встановлених правил чи порядку збору або розповсюдження інформації, надання неправдивої інформації, негласні способи отримання інформації тощо. Бездіяльність проявляється, зокрема, у відмові відповіді на інформаційний запит, приховуванні інформації. Факультативними ознаками об'єктивної сторони є час, місце, спосіб, характер скоєння інформаційного правопорушення, його шкідливі наслідки. В цілому об'єктивна сторона інформаційного правопорушення з формальним складом характеризується порушенням норми права, що регулює інформаційні відносини, а з матеріальним – нанесенням майнової шкоди інформаційним інтересам особи, суспільства чи держави та наявністю причинного зв'язку між діями та нанесеною шкодою.

Суб'єктами інформаційних правопорушень у соціальних мережах можуть бути фізичні та юридичні особи в залежності від виду правопорушення та міри юридичної відповідальності. Юридичні особи можуть бути тільки суб'єктом адміністративної чи цивільно-правової відповідальності. Загальним суб'єктом інформаційних правопорушень є осудні фізичні особи віком від 16 років. Спеціальним суб'єктом можуть бути посадові особи, уповноважені на здійснення організаційно-розпорядчих та адміністративно-господарчих функцій в органах державної влади та органах місцевого самоврядування в інформаційній сфері. Особливим спеціальним суб'єктом можуть бути військовослужбовці та інші особи, на яких поширюється дія дисциплінарних статутів або спеціальних положень про службу, у випадках вчинення правопорушення, пов'язаного з дотриманням та збереженням державної таємниці.

Суб'єктивна сторона інформаційного правопорушення в соціальній мережі відображає психічне відношення особи до свого діяння та являє собою вину у формі умислу або необережності. Форма вини впливає на кваліфікацію діяння та індивідуалізацію покарання. Особливість вини юридичної особи полягає у встановленні можливості дотримання норм та правил, за порушення яких передбачена юридична відповідальність. При цьому притягнення до

відповідальності юридичної особи не звільняє від відповідальності і винну фізичну особу.

Адміністративний інформаційний делікт – це суспільно небезпечне, винне, протиправне діяння, що посягає на встановлений порядок державного управління в інформаційній сфері та порушення інформаційних прав особи, що тягне за собою адміністративну відповідальність. Об'єктивна сторона інформаційного адміністративного правопорушення проявляється у діях чи бездіяльності, що заборонені інформаційним правом і шкідливими наслідками цього діяння. Суспільна шкідливість інформаційного адміністративного правопорушення означає, що ним заподіюється шкода інформаційним відносинам, які охороняються інформаційними правовими нормами, зокрема правам і свободам людини та громадянина, а також встановленому порядку управління інформаційною сферою. Суб'єктами адміністративних правопорушень виступають громадяни чи посадові особи. Посадові особи підлягають адміністративній відповідальності за правопорушення, пов'язані з недотриманням установлених правил у сфері порядку управління інформаційною сферою, та порушення інших правил інформаційної діяльності, виконання яких входить до їхніх службових обов'язків. Це означає, що посадові особи несуть відповідальність не тільки за порушення певних правил своїми діями, а й за неналежне забезпечення виконання їх іншими особами, насамперед підлеглими. На них накладається дисциплінарне стягнення, якщо правопорушення було здійснене під час виконання ними службових обов'язків. Суб'єктивна сторона інформаційного адміністративного правопорушення охоплює вину, мотив і мету поведінки правопорушника і може бути вчинене як умисно, так і з необережності.

Дисциплінарне інформаційне правопорушення являє собою суспільно небезпечне, винне, протиправне діяння, що виражається у невиконанні або неналежному виконанні працівником покладених на нього інформаційним законодавством обов'язків у межах займаної посади щодо створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації і тягне за собою дисциплінарну відповідальність. З цього випливає, що дисциплінарні проступки проявляються в порушенні трудової, службової чи військової дисципліни у сфері інформаційних відносин. Суб'єктом дисциплінарного проступку завжди є особа, яка перебуває у трудових правовідносинах з власником або уповноваженим ним органом і яка наділена відповідними повноваженнями в інформаційній сфері. Суб'єктивну сторону дисциплінарного інформаційного проступку характеризує вина у формі умислу або необережності. Об'єктивну сторону дисциплінарного проступку відображає проти-

правна поведінка суб'єкта, яка полягає в порушенні трудових обов'язків, закріплених за конкретним працівником. Об'єктом дисциплінарного правопорушення є трудові обов'язки в інформаційній сфері, які не виконані або виконані неналежним чином.

Цивільні інформаційні делікти – це суспільно небезпечне, винне, протиправне діяння, що посягає на майнові та особисті немайнові блага в інформаційній сфері, за що передбачена цивільно-правова відповідальність. Цивільно-правові проступки в інформаційній сфері передбачені нормами цивільного права і тягнуть за собою правовідновлюючі заходи (невиконання обов'язків за цивільно-правовим договором). Особливістю складу цивільного правопорушення є причинний зв'язок між протиправною поведінкою суб'єкта і заподіяними реальними збитками потерпілої сторони.

Інформаційний злочин – це суспільно небезпечне, винне, протиправне діяння осудної особи, здійснене в інформаційній сфері, за що передбачена кримінальна відповідальність, навмисні дії, спрямовані на розкрадання або руйнування інформації в інформаційних системах і мережах, які виходять з корисливих або хуліганських спонукань. Особливість складу інформаційних злочинів проявляється в особливому предметі, якими є державна таємниця та інша таємна чи конфіденційна інформація, комп'ютерна інформація тощо.

Державно-правовий механізм попередження інформаційних правопорушень

Інформаційні правовідносини є частиною суспільних відносин і перебувають під охороною та захистом держави. Одним з правоохоронних заходів в інформаційній сфері є попередження правопорушень з використанням спеціального державного механізму правового регулювання. Основою такого механізму є, насамперед, сукупність державних органів та недержавних організацій, уповноважених на виконання функцій держави в правоохоронній та правозастосовній діяльності.

Уповноважені державні та інші органи для охорони та захисту інформації, інформаційних систем та мереж від протиправного посягання, забезпечення інформаційної безпеки розробляють та використовують спеціальні елементи механізму правового регулювання. Складовими цього механізму є юридичні засоби та способи впливу на учасників інформаційних відносин та інших осіб, що мають сприяти виробленню у них правомірної поведінки, відповідного рівня правової свідомості та правової інформаційної культури. Засобами такого впливу є інформаційно-правові норми, які не тільки встановлюють правила обігу інформації, але й порядок поведінки учасників інформаційних відносин та інших осіб. Такі

норми містяться в Конституції України, Законі України «Про інформацію», інших нормативних актах, що регулюють інформаційні правовідносини і мають правоохоронний зміст.

У той же час норми Кодексу України про адміністративні правопорушення, Кримінального, Цивільного кодексів України, інші нормативні акти не тільки встановлюють міру відповідальності за інформаційні правопорушення, але й виконують попереджувальну та відновлювальну функції.

Роль державних органів у механізмі правового регулювання залежить від статусу органу та його повноважень. Верховна Рада України приймає закони, спрямовані на урегулювання інформаційних правовідносин, визначає напрями державної інформаційної політики та інформаційної безпеки тощо. Президент України, Кабінет Міністрів України, центральні органи виконавчої влади на виконання законів України видають необхідні підзаконні нормативно-правові акти для конкретизації певної сфери інформаційних відносин, тобто організовують реалізацію законодавчих положень, спрямованих, зокрема, на охорону об'єктів інформаційних відносин від протиправних посягань.

В механізмі правової охорони об'єктів інформаційних відносин задіяні практично всі органи державної влади на центральному та місцевому рівнях. Особливе місце в цьому механізмі посідають правоохоронні органи, серед яких органи прокуратури, служби безпеки, органи внутрішніх справ, які наділені спеціальними повноваженнями щодо попередження, розкриття та розслідування злочинів та інших правопорушень. Суди України виконують правозахисну функцію в процесі розгляду конкретних цивільних, адміністративних чи кримінальних справ, а їх діяльність спрямована на встановлення істини по справі і при необхідності відновлення порушених прав потерпілим учасником інформаційних відносин.

Названі та й інші органи, залучені до охорони та захисту об'єктів інформаційних відносин, з допомогою правових норм та юридичних способів впливають на суспільні інформаційні відносини та поведінку суб'єктів цих відносин, що в цілому є методом правового регулювання. Методологічне забезпечення правового регулювання інформаційних відносин ґрунтується на системному комплексному застосуванні методів конституційного, цивільного, адміністративного, трудового та кримінального права, тобто поєднання імперативного та диспозитивного методів з використанням загальноправових та спеціальних способів. Елементами загальноправових способів впливу є дозволи, зобов'язання та заборони, використання яких супроводжується дотриманням принципів законності, демократизму, гуманізму, гарантованості судового захисту. Викори-

стання спеціальних галузевих способів правового регулювання інформаційної сфери залежить від об'єкта правової охорони, якими можуть бути доступ до інформації, недоторканність особистого життя, інформація з обмеженим доступом, об'єкти інтелектуальної власності тощо.

Для попередження та усунення загрози таким специфічним об'єктам використовуються спеціальні норми інформаційного законодавства, інформатизація правової сфери, використання організаційно-технічних засобів, громадський контроль за діяльністю органів публічної влади. В цілому правовими методами попередження інформаційних правопорушень є наповнення інформаційного законодавства нормами, спрямованими на підвищення інформаційної безпеки людини, суспільства, держави, узгодження вітчизняного законодавства з відповідними нормами міжнародного права тощо. Організаційно-технічні способи попередження правопорушень передбачають удосконалення технічних засобів захисту інформації та розвиток системи протидії несанкціонованому проникненню в інформаційне середовище. Організуюча складова механізму попередження інформаційних правопорушень включає визначення компетенції органів публічної влади, недержавних організацій у сфері інформаційної безпеки, напрямів їх діяльності та завдань, збалансованості інтересів особи, суспільства та держави в інформаційній сфері.

Держава в рамках попереджувальних заходів формує державну інформаційну політику, організовує роботу відповідних органів, підтримує діяльність громадських організацій, контролює розробку та виробництво засобів захисту інформації, проводить практичну діяльність по захисту внутрішнього ринку від проникнення до нього неякісних інформаційних продуктів. Діяльність держави щодо попередження правопорушень в інформаційній сфері охоплює основні напрями та способи реалізації державної інформаційної політики, в основі якої є забезпечення інформаційної безпеки людини, суспільства, держави.

Слід зауважити, що законодавство України виділяє два способи захисту: загальні та спеціальні, які застосовуються в судовому та позасудовому порядку.

Отже у випадку розміщення в мережі Інтернет інформації, що порушує честь, гідність та ділову репутацію, особа, права якої порушено, може або ж безпосередньо звернутися до особи, яка здійснила дане порушення, з вимогою про спростування такої інформації або до суду.

Питання про захист авторського права в мережі Інтернет гостро підіймається у більшості країн світу, на жаль, в Україні йому приді-

ляється мало уваги, тому необхідно знайти оптимальні способи вирішення даної проблеми, спираючись на міжнародний досвід. Крім того, можна помітити певні прорахунки в реалізації національної програми захисту авторських прав у мережі Інтернет внаслідок відсутності нормативно-правових актів, які б стосувалися виключно даного питання. Навпаки, у пострадянській державознавчій літературі, присвяченій різним аспектам теорії й практики захисту права на недоторканність приватного життя (зокрема у працях Н. Г. Беляєвої, Г. О. Мітцукової, І. Л. Петрухіна, В. С. Сивухіна, Е. О. Цадикової та ін.), проблема соціальних мереж досі перебуває поза межами уваги, хоча кількість користувачів Інтернету з колишніх радянських республік зростає з геометричною прогресією.

Серед багатьох ризиків для привнесі у соціальних мережах варто виокремити принаймні три:

- 1) повна поінформованість про особу;
- 2) повідомлення інформації злочинцям;
- 3) відсутність у особи реального контролю за домірністю інформації про себе.

Наприкінці слід зазначити, що Інтернет не повинен бути самоціллю для суспільства, а лише засобом для розвитку людської особистості. Право людини на розвиток має бути базовим критерієм для оцінки міри реалізації всіх її інших прав і свобод, зокрема свободи слова та доступу до інформації. Адже те, що руйнує людину, не може вважатися свободою, заради якої відстоюється право на вільний Інтернет. Загалом мережа Інтернет виступає як галузь масової комунікації, яка стрімко розвивається і змінюється, а правове регулювання таких галузей завжди розвивається з запізненням.

Таким чином, інформаційні правопорушення в соціальних мережах є новітнім самостійним видом правопорушень, що обумовлює необхідність становлення та розвитку інформаційної деліктології¹, метою якої є вивчення змісту, природи, сутності, специфіки та різноманіття інформаційних правопорушень, а також розроблення та впровадження конкретних шляхів, напрямів, способів їх профілактики.

¹ Максименко Ю. Є., Ліпкан В. А. Засади розвитку інформаційної деліктології // Право України. 2013. № 10. С. 249–256.

ЦИВІЛЬНА ТА КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ ПРИ КОРИСТУВАННІ СОЦІАЛЬНИМИ МЕРЕЖАМИ

Соціальні медіа в даний час є однією з найбільш часто використовуваних форм вираження та спілкування. Користувачі публікують і коментують думки та висловлювання з поза екрана комп'ютера, і це часто створює відчуття того, що вони дистанціюються від своїх дій.

Наразі існує дві форми суспільної поведінки, які можуть призвести до відповідальності користувача соціальної мережі. Дані дії називаються «тролінг» і «наклеп».

Тролінг – це акт образи або залякування інших користувачів у соціальних мережах, а наклеп – це несправедливе та образливе твердження людини, яке шкодить репутації іншої особи.

Соціальні медіа створюють проблему того, що користувачі часто відчують себе дистанційованими від своїх дій, розміщуючи контент в Інтернеті. Контент, хоч і в основному нешкідливий, може мати і часто має досить серйозні наслідки для користувачів, які поділилися контентом в Інтернеті.

Деякі користувачі можуть відчувати себе віддаленими від людей, на яких вони націлюються в соціальних медіа завдяки тролінгу, тому вони, навіть знаючи, що їх твердження є хибними, висловлюють їх, сподіваючись на дистанцію та межу відстані, яку створює Інтернет. У випадку з наклепом очевидним фактом є те, що користувачі часто не розуміють, що те, про що вони говорять, може трактуватися як наклепницькі твердження, чи що вони не думають про наслідки, поки не буде занадто пізно¹.

А таких випадків, коли особа вчинила самогубство через тролінг в Інтернеті накопичилось вже чимало.

Наприклад, в Італії 14-річна дівчина стрибнула з даху будинку одного з покинутих готелів у місті Чіттаделла (регіон Венето, про-

¹ Waterson J. P. Social Media Responsibility and Liability – a UK Perspective. 2016. URL: <http://arno.uvt.nl/show.cgi?fid=142039>.

вінція Падуа). Прокуратура Італії відразу почала розслідування обставин загибелі школярки, в рамках якого і стало відомо про те, що над дівчинкою щосили знущалися на сайті Ask.fm. З'ясувалося, що якийсь користувач відправив дівчині рекламний кліп фільму *Suicide Room*, а анонімний коментатор заявив: «Я сподіваюся, що одного разу ти проріжеш на руці вени і помреш!». У своєму останньому повідомленні зневірена школярка написала: «Досить, дурний світ!»¹ Як зазначає газета *Mattino Podova*, аноніми також писали їй: «Ти дивна і заслуговуєш самотності».

Ще один яскравий приклад мав місце у Шотландії нещодавно, у 2017 році. Мешканка шотландського міста Камбусбаррон Лієнн Моррісон наклала на себе руки в день свого 23-річчя. Невідомі створили від її імені підроблену сторінку в додатку для знайомств *Tinder* і почали над нею знущатися. Не витримавши тролінгу, дівчина скоїла суїцид, залишивши чотирирічного сина Мейсона².

В цьому ж 2017 році ще одна 27-річна жінка-мисливець Меланія Кептан (*Melania Capitan*) покінчила життя самогубством після років тролінгу з боку обурених її діяльністю активістів. Часом в соціальних мережах вони бажали їй бути побитою.

Президент Іспанської федерації полювання подав скаргу державному прокурору країни, звинувативши авторів жорстких коментарів у смерті дівчини. У скарзі йдеться про те, що полювання є законним в Іспанії, а тролі порушували права загиблої.

Смерть Меланії стала причиною закликів до зміни закону, щоб розглядати інтернет-знущання також як злочин³.

Отже, як можна бачити з наведених прикладів, тролінг в Інтернеті вже став доволі масштабною проблемою для суспільства в цілому, оскільки користувачі соціальних мереж вже почали порушувати закон та створювати для себе підстави для правової відповідальності. Питома вага сучасних користувачів соціальних мереж не розуміє, що те, що вони роблять, є наразі протиправними діями, призводить до жаклих наслідків та карається законом.

Користувачі також часто піддаються враженню, що з якоїсь причини відповідальність за їх проступки не настане, оскільки вони апіорі не можуть нести відповідальність за те, що написано в Інтернеті. Хоча дані судів та статистика розгляду судових

¹ Самоубийство из-за троллинга // Вести сегодня. 2014. URL: <http://vesti.vesti.lv/crime/theme/criminal/81934-samoubijstvo-izza-trollinga.html>.

² Молодая мать покончила с собой из-за издевательств на *Tinder* // Ридус. 2017. URL: <https://www.ridus.ru/news/260445>.

³ В Испании ярая охотница совершила самоубийство после годов троллинга защитников животных // ТСН. 2017. URL: <https://ru.tsn.ua/svit/v-ispanii-ya-ya-ya-ohotnica-sovershila-samoubiystvo-posle-godov-trollinga-zaschitnikov-zhivotnyh-901667.html>.

справ вказує на те, що користувачі потенційно можуть бути притягнуті до відповідальності за контент, який вони розміщують в Інтернеті.

Говорячи про юридичну відповідальність при користуванні соціальними мережами, варто вказати на розробленість даного питання у такій відомій соціальній мережі, як Facebook. Слід зауважити, що в приписах «Умов надання послуг» Facebook стосовно призупинення або припинення дії акаунту (при виявленні Facebook порушення з боку користувача) Facebook має право призупинити доступ до акаунту або заблокувати доступ до нього (за власною ініціативою або на вимогу законодавства).

При цьому досить цікавим є застереження в «Умовах надання послуг» Facebook стосовно того, що Facebook не контролює та не керує діями та висловлюваннями користувачів Facebook, не несе відповідальності за дії та поведінку користувачів онлайн чи оффлайн, за будь-який контент, який вони поширюють (образливий, неналежний, нецензурний, незаконний та інший неприйнятний контент).

Що ж стосується кримінальної відповідальності, то перш за все варто вказати, що в деяких «Умовах надання послуг» соціальних мереж вже при реєстрації вказується, що не можуть створювати в соціальних мережах акаунти особи, яких було засуджено за вчинення протиправних дії сексуального характеру¹.

Також у «Політиці використання персональних даних» міститься розділ стосовно взаємодії Facebook з владними структурами, реагування на запити та запобігання завданню шкоди.

Так, Facebook, маючи доступ до персональної інформації користувача, його повідомлень, контенту, активності в соціальній мережі, має можливість зберігати таку інформацію, відкрито співпрацює з контрольно-наглядовими, правоохоронними та іншими органами (владними структурами) та може надавати їм наявну в Facebook інформацію стосовно конкретного користувача.

Facebook надає доступ до персональної інформації користувача при наявності офіційного запиту (наприклад, ордер на обшук, судові розпорядження чи повістка), якщо Facebook буде переконаний, що органи діють на законних підставах. Така співпраця може включати відповіді на офіційні запити від органів державної влади інших країн, а не тільки Сполучених Штатів Америки, при умові, що особа стосовно якої направлено офіційний запит, підпадає під юрисдикцію такої країни та такий запит відповідає міжнародно визнаним стандартам.

¹ Terms of Service. 2018. URL: <https://en-gb.facebook.com/legal/terms>.

Інший випадок, при наявності якого Facebook може надавати доступ до персональної інформації користувача, – це коли вказано необхідність:

- виявлення, запобігання та усунення шахрайства, несанкціонованого використання продуктів Facebook, порушення положень та правил використання Facebook чи іншої шкідливої або незаконної діяльності;

- для захисту прав Facebook, майна та продуктів Facebook, користувачів, в тому числі в рамках розслідування або запитів правоохоронних органів. Даний пункт включає можливість ділитись персональними даними користувачів із третіми особами або отримувати відповідну інформацію від третіх осіб стосовно надійності акаунту з метою запобігання шахрайству, зловживання та іншим шкідливим діям продуктам компанії Facebook.

Персональна інформація про користувача може зберігатись упродовж довгих строків за умови, що вона є предметом офіційного запиту, така інформація необхідна в рамках розслідування державним органам, а також в інших випадках з метою запобігання шкоді.

Facebook протягом одного року зберігає інформацію стосовно акаунту, який було відключено через порушення Умов використання Facebook з метою запобігання зловживанню або вчиненню інших протиправних дій¹.

В багатьох країнах світу особа може нести відповідальність за пост на своїй сторінці в соціальних мережах. Україна також не стала виключенням. За даними статистики з 2014 по 2017 рік українські суди винесли більше 30 вироків за пости в соціальних мережах, в яких містились заклики до насильницького повалення конституційного ладу в Україні або захоплення державної влади в країні.

Так, наприклад, у 2016 році суд міста Суми своїм рішенням від 2 лютого 2016 року по справі № 591/442/16 визнав власника сторінки (22-річний громадянин України) «ВКонтакте» винним по ч. 3 ст. 109 Кримінального кодексу України за публічні заклик до насильного повалення конституційного строю та до захоплення державної влади через ЗМІ. За результатами розгляду справи суд прийняв рішення призначити покарання у вигляді штрафу в розмірі 8500 грн. Дана особа через свою сторінку у соціальній мережі розповсюджувала інформацію антиукраїнського змісту з метою початку боротьби проти чинної української влади та зміни існуючого режиму².

¹ Data Policy. 2018. URL: <https://en-gb.facebook.com/about/privacy/update>.

² Кримінальна відповідальність за пост у соціальній мережі // УКРПРАСТ. 2016. URL: <http://ukrtrust.net/uk/news/55>.

У даному випадку важливо зауважити, що і пост і репост є розповсюдженням матеріалу, тому навіть якщо особа не створювала тексту з закликами до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади, репост такої інформації також підпадає під ст. 109 Кримінального кодексу України.

У Сполучених Штатах Америки та деяких країнах Європейського Союзу (таких як Франція, Німеччина, Великобританія) лайки, пости та репости вже досить тривалий час використовуються як джерело доказів розслідування злочинів та правопорушень.

Якщо з постом і репостом все більш-менш зрозуміло, то з лайками виникає низка питань. Яку саме дію вчиняє особа, ставлячи лайк? Це підтримка особи, посту, мовчазна згода чи просто жест ввічливості в бік знайомої користувачеві особи? Більш того, часто трапляються випадки, коли лайк ставиться помилково, в процесі перегляду нових публікацій в стрічці, наприклад такої соціальної мережі, як Instagram. Тобто якщо пост та репост можливо кваліфікувати в рамках існуючого законодавства як поширення інформації, то як кваліфікувати лайк?

Американська спілка захисту громадянських свобод зазначає, що процес «лайкання» чого-небудь виражає чітке повідомлення – визнане мільйонами користувачів Facebook і не користувачів також – і є одночасно прямим висловлюванням і вираженням думки за допомогою символу.

Говорячи про лайки, слід згадати справу, яка мала місце в США, *Bland v. Roberts*, де поліцейських було звільнено з посади за те, що вони лайкнули сторінку у Facebook опонента діючого шерифа на виборах. Стосовно лайків апеляційний суд зробив наступне зауваження: «На найпростішому рівні сприйняття клікання кнопки like означає опубліковане ствердження таким, яке відверто подобається користувачу, і саме по собі є доволі сильною стверджувальною заявою з його боку»¹.

Але, між тим, на жаль, на даний момент в Україні на законодавчому рівні немає чіткого визначення Інтернет-простору, регулювання діяльності в Інтернет-просторі та відсутнє нормативне закріплення того, яка інформація заборонена до публікації у соціальних мережах.

Цікавим є те, що коли справа доходить до миттєвого розповсюдження інформації, соціальні мережі – перші серед усіх інших шляхів розповсюдження інформації. Так, у січні 2016 року було виявлено, що існує близько 2,3 млрд користувачів соціальної мережі.

¹ За лайк за грати: чи можна в Україні отримати юридичні проблеми в соц-мережах // PLATFORMA. 2017. URL: <https://opinion.platforma.ua/za-laik-za-grati>.

Глобальне населення становить близько 7,4 млрд, тому очевидним є те, що чимала сила в цифрах за соціальними медіа.

Із цієї цифри на Facebook припадає понад 1,7 млрд користувачів. Користувачі соціальних мереж також не обмежуються однією мережею. Twitter, Instagram, Tumblr, Reddit та інші – у всіх є свої величезні успіхи. Крім того, додатки для обміну повідомленнями, такі як WhatsApp, Kik, Viber та Telegram, заохотили мільйони користувачів уникати традиційних комунікацій мобільних пристроїв на користь їх інтегрованих платформ.

Результатом став зв'язок груп окремих користувачів, здатних безперешкодно спілкуватися по всьому світу. Проте соціальні медіа – це не просто кумедні картинки та галасливі відеоролики. Користувачі соціальних медіа XXI століття можуть так само легко потрапити під вплив набагато більш «темного» та жахливого контенту, який, наприклад, поширюється технологічно-кваліфікованими терористичними групами та їх технічними фахівцями.

Терористи ІДІЛ продовжують робити заголовки по всьому світу. На щастя, це пов'язано з тим, що повстанська терористична група втрачає простір території. Проте, ІДІЛ використовувала соціальні мережі під час їх швидкого розширення на Близькому Сході, транслюючи абсолютно варварські звірства безпосередньо в соціальні медіа-потоки.

Інші терористичні організації використовують глобальні мережі для розповсюдження новин, щоб поширювати страх. ІДІЛ зробила це особистим, підступним та неминучим.

ІДІЛ є крайнім прикладом. Але вони дають яскравий приклад, як соціальні засоби масової інформації можуть бути легко схильні до волі автора.

Зважаючи на вищенаведене, можна стверджувати, що соціальні медіа часто і все більше використовуються у різних злочинах. Мета правоохоронних органів полягає в класифікації масового розмаїття таких злочинів, які безпосередньо пов'язані з соціальними медіа, та в притягненні безпосередньо самих злочинців до відповідальності. Деякі «лише» використовують соціальні медіа як інструмент планування, а інші – як повноцінний плацдарм та мережу для поширення злочинної інформації.

Судити про тяжкість злочину, вчиненого у соціальних медіа, також є складним завданням. Злочини можуть включати расистське зловживання, випадки гомофобії, випадки догляду та переслідування.

У 2014 році центр злочинності в Інтернеті ФБР повідомив, що 12 % усіх виявлених скарг стосуються соціальних мереж. Ці 12 % становлять 32 330 скарг, отриманих протягом 12 місяців. На жаль,

у доповіді IC3 2015 року не враховано точну цифру. Проте, оскільки загальна кількість скарг у 2015 році зросла з 269 422 до 288 012, поряд із посиленою перевіркою соціальних мереж, можна передбачити їх зростання¹.

Слід зазначити, що мільйони громадян США та інших країн стають жертвами кіберзлочинів щороку. Незалежно від соціальних мереж, за оцінками IC3 (Internet Crime Complaint Center²), лише 15 % жертв шахрайства в країні повідомляє про свої злочини правоохоронним органам. Мільйони злочинів у соціальних мережах залишаються без уваги правоохоронних органів, а отже, злочинці залишаються без притягнення до відповідальності.

Соціальні медіа не завжди є місцем злочину. Сучасні грабіжники легко використовують нашу очевидну відданість трансляції кожної деталі про наше повсякденне життя.

Опитування 2011 року, проведене фірмою Friedland, повідомляє:

- 78 % опитаних колишніх грабіжників заявили, що вони твердо вважають, що соціальні медіа-платформи, такі як Facebook, Twitter і Four Square, використовуються нинішніми злодіями при націлюванні на власність, яку вони прагнуть пограбувати;

- три чверті (74 %) стверджують, що, за їхньою оцінкою, «Google перегляд вулиці» відіграє значну роль у сьогоdnішніх крадіжках у домах;

- 54 % опитаних визначили статуси в соціальних мережах та оновлення власного місцезнаходження як одну з найбільш поширених помилок, які може зробити домовласник.

Слід також звернути увагу на цікавий випадок, за яким наступила кримінальна відповідальність і який стався у штаті Делавер США за участі YouTube та відеоблогера. Вісімнадцятирічний Сем Моеллер із Нью Джерсі був арештований після того, як він незаконно потрапив на Делаверський музичний фестиваль феєрверків без квитка і запостив «як-потрапити-до» відео на YouTube.

Моеллер навіть не намагався приховати свою протиправну поведінку – він дав відеозаголовок «Камери дозволені: Як таємно потрапити на музичний фестиваль». Після того як офіцери поліції побачили відео, вони отримали дозвіл на його арешт. Моеллер самостійно з'явився до поліцейської дільниці. Хлопець був звинувачений у проході без пропуску та в крадіжці на суму близько

¹ Philips G. Crime, Terrorism and Security: The Dark Side of Social Media. 2016. URL: <https://www.makeuseof.com/tag/crime-terrorism-security-dark-side-social-media>.

² IC3 // Википедія. 2018. URL: <https://ru.wikipedia.org/wiki/IC3>.

1,500 \$ – і все це тому, що він не заплатив 199 \$ за квиток та виклав відео на YouTube¹.

Отже, як вже відзначалось, наразі в Україні ситуація із відповідальністю за злочини, вчинені у процесі користування соціальними медіа, також супроводжується певними складностями – зокрема відсутністю комплексної нормативно-правової бази, яка конкретно та збалансовано врегульовувала би ті відносини, що складаються у процесі користування громадянами соціальними мережами.

Так, у парламенті не відмовились від ідеї прийняття законопроекту щодо протидії загрозам національній безпеці в інформаційній сфері. В разі його прийняття влада отримає можливість запросто блокувати сайти.

У Комітеті Верховної Ради України з питань національної безпеки та оборони надали позитивний висновок і рекомендували Раді підтримати законопроект.

Проте низка громадських та правозахисних організацій виступають проти даного законопроекту, посиляючись на його непередуманість та цензуру, що може бути запроваджена завдяки його прийняттю.

Оператори телекомунікацій та інші суб'єкти надання телекомунікаційних послуг отримають значне посилення відповідальності за невиконання будь-яких вимог щодо надання телекомунікаційних послуг чи блокування ресурсів, незалежно від серйозності порушень. Також вони отримають значні фінансові зобов'язання – за власні кошти закуповувати та встановлювати визначені державою технічні засоби, необхідні для блокування доступу до інформаційних ресурсів.

Оскільки влада і СБУ отримають можливість на власний розсуд вирішувати, чи може той чи інший сайт нести кіберзагрози та «інформаційний тероризм», то і блокувати за це зможуть практично будь-який ресурс. Від інтернет-ЗМІ до сайтів компаній².

Варто зазначити, що зміст даного законопроекту носить еkleктичний характер та містить зміни, що стосуються багатьох нормативно-правових актів, у тому числі Кримінального кодексу України та Кодексу України про адміністративні правопорушення.

З аналізу даного законопроекту випливає наступне:

- створюються умови для необмеженої дискреції органів державної влади та їх представників у прийнятті рішень щодо блокування інформаційних ресурсів;

¹ Social media related crimes. URL: <https://www.cbsnews.com/pictures/social-media-related-crimes>.

² Ткачук Я. Блокувати інтернет: кому і як загрожує новий законопроект № 6688 щодо інформбезпеки. 2018. URL: https://24tv.ua/zakon_pro_blokuvannya_saytiv_ukrayina_komu_zagrozhuje_zakon_blokuvannya_saytiv_n994475.

– спостерігається відсутність належних механізмів контролю за діями уповноважених органів та їх представників, гарантій захисту прав людини, граничних термінів тимчасового блокування веб-сайтів тощо;

– суттєво посилюється відповідальність операторів телекомунікацій та інших суб'єктів надання телекомунікаційних послуг за невиконання будь-яких вимог щодо надання телекомунікаційних послуг чи блокування ресурсів, незалежно від серйозності порушень;

– на операторів покладаються надмірні фінансові зобов'язання за власні кошти закуповувати та встановлювати визначені державою технічні засоби, необхідні для блокування доступу до інформаційних ресурсів (веб-сайтів).

СБУ наділяється повноваженнями у сфері нагляду за виконанням вимог щодо блокування веб-сайтів¹.

Таким чином, можна сказати, що хоча проект Закону № 6688 і не є ідеальним та повинен бути доопрацьований, законодавець робить перші кроки, направлені на посилення відповідальності у сфері використання медіа-простору та направляє свої зусилля на зміцнення державної кібербезпеки.

Окрім того, слід зазначити, що саме держава формує культуру відносин у сфері інтернет-відносин шляхом правового регулювання. Проте без участі громадянського суспільства в обговоренні змін до законодавства, що стосується медіа-простору не повинен обходитись жодний нормативно-правовий акт, оскільки такі сфери суспільного життя є доволі важливими та кореспондують до принципів гуманізму, рівності та свободи слова, що за своєю суттю є основою громадянського суспільства.

¹ Юридичний аналіз законопроекту № 6688 щодо досудового блокування сайтів. URL: <https://detector.media/withoutsection/article/138996/2018-07-02-yuridichnii-analiz-zakonoproektu-6688-shchodo-dosudovogo-blokuvannya-saitiv>.

1. Актуальні проблеми цивілістики у цифрову добу: монографія / за ред. Є. О. Харитонова, О. І. Харитонової; НУ ОЮА. — Одеса: Юрид. літ., 2018. — 248 с. — (Серія: Цивілістика та «ІТ-право»).
2. Грігор'янц Г. І. Піратство як порушення авторських і суміжних прав в мережі Інтернет: дис. ... канд. юрид. наук: 12.00.03 / Г. І. Грігор'янц. — Одеса, 2016. — 195 с.
3. ІТ-право та інформаційна безпека: монографія / за ред. О. І. Харитонової, Є. О. Харитонова. — Одеса: Фенікс, 2017. — 176 с.
4. ІТ-право: сутність та поняття: монографія / за ред. О. І. Харитонової, Є. О. Харитонова. — Одеса: Фенікс, 2017. — 316 с.
5. ІТ-право: теорія та практика: навч. посіб. / за ред. О. І. Харитонової, Є. О. Харитонова. — Одеса: Фенікс, 2017. — 472 с.
6. Кормич Б. А. Інформаційне право: підручник / Б. А. Кормич. — Харків: БУРУН і К., 2011. — 334 с.
7. ІТ-право — це просто: посібник / за ред. Є. О. Харитонова. — Одеса: Фенікс, 2017. — 106 с.
8. Кормич Б. А. Правові важелі протидії інформаційним загрозам: міжнародний і вітчизняний досвід // Актуальні проблеми політики: зб. наук. пр. / редкол.: С. В. Ківалов (голов. ред.), Л. І. Кормич (заст. голов. ред.), Ю. П. Аленін [та ін.]; МОНмолодьспорт України, НУ ОЮА. — Одеса: Фенікс, 2011. — Вип. 42. — С. 80–89.
9. Некіт К. Г. Доменне ім'я як об'єкт цивільних прав // Часопис цивілістики. — 2017. — № 23. — С. 40–45.
10. Право інтелектуальної власності: підручник / О. І. Харитонова, Є. О. Харитонов, Т. С. Ківалова, В. С. Дмитришин, О. О. Кулініч, Л. Д. Романадзе [та ін.]; за заг. ред. О. І. Харитонової. — Київ: Юрінком Інтер, 2016. — 540 с.
11. Правове регулювання використання зображень у електронних бібліотеках за законодавством України: монографія / О. І. Харитонова, О. О. Кулініч, С. В. Мазуренко, І. В. Менсо; НУ ОЮА. — Одеса: Юрид. літ., 2017. — 72 с.
12. Фасій Б. В. Субсидіарне застосування норм цивільного законодавства до ІТ-відносин // ІТ-право: проблеми та перспективи розвитку в Україні: зб. матеріалів наук.-практ. конф. — Львів: НУ «Львів. політехніка», 2016. — С. 264–273.

13. Фасій Б. В. Agile, waterfall та out staff договір або договори на розробку програмного забезпечення // Часопис цивілістики. – 2017. – Вип. 26. – С. 98–102.
14. Фасій Б. В. Правове регулювання комп'ютерних ігор у сфері ІТ // Часопис цивілістики. – 2017. – Вип. 27. – С. 121–124.
15. Фасій Б. В. Субсидіарне застосування положень цивільного законодавства про договори до ІТ-відносин // Правова адаптації законодавства України до умов внутрішнього ринку ЄС: матеріали Міжнар. інтернет-конф., присвяч. пам'яті І. В. Шерешевського (Одеса, 2 груд. 2016 р.). – Одеса: Фенікс, 2016. – С. 28–30.
16. Харитонов Є. О. Інформаційна безпека з погляду цивілістики // Збірник матеріалів Міжнародного конгресу «Правові проблеми державно-правового партнерства в умовах євроінтеграції», присвяченого 20-річчю Національного університету «Одеська юридична академія», Одеса, 2–4 черв. 2017 р. / відп. ред.: Є. О. Харитонов, О. І. Харитонova, Т. Є. Харитонova; Нац. ун-т «Одес. юрид. акад.». – Одеса: Юрид. літ., 2017. – С. 64–68.
17. Харитонов Є. О. ІТ-право з погляду цивілізаційного та концептного підходів // Часопис цивілістики. – 2016. – Вип. 22. – С. 122–127.
18. Харитонов Є. О. Спроба класифікації порушення авторських прав у мережі Інтернет // Захист права інтелектуальної власності у мережі Інтернет: теоретичні та практичні аспекти: матеріали Інтернет-конф. (Одеса, 22 трав. 2015 р.) / за заг. ред. О. І. Харитонovої; упоряд.: А. В. Кирилюк, Н. П. Бааджи. – Одеса: Юрид. літ., 2015. – С. 75–78.
19. Харитонов Є. О. Сутність ІТ-права (ІТ-право як концепт) // ІТ-право: проблеми та перспективи розвитку в Україні: зб. матеріалів наук.-практ. конф. – Львів: НУ «Львів. політехніка», 2016. – С. 274–280.
20. Харитонов Є. О. Інформаційні технології та авторське право / Є. О. Харитонов, О. І. Харитонova // Вісник Південного регіонального центру Національної академії правових наук України. – 2017. – № 10. – С. 119–127.
21. Харитонов Є. О. Проблема ІТ-права / / Є. О. Харитонов, О. І. Харитонova // Матеріали Всеукр. наук.-практ. конф., яка проводиться в рамках тижня цивільного процесу (Одеса, 18 квіт. 2017 р.) / за заг. ред. Н. Ю. Голубової. – Одеса: Фенікс, 2017. – С. 112–115.
22. Харитонов Є. О. Проблеми правового регулювання в ІТ-сфері в умовах гібридної, інформаційної війни / Є. О. Харитонов, О. І. Харитонova // Проблеми відновлення конституційного ладу в Україні: матеріали міжнар. наук.-практ. конф. (Київ, 19–20 трав. 2017 р.) / Таврійс. нац. ун-т ім. В. І. Вернадського. – Київ, 2017. – С. 159–163.
23. Харитонов Є. О. «ІТ-право» як феномен правового регулювання / Є. О. Харитонов, О. І. Харитонova // Право як регулятор суспільних

- відносин: історія, теорія, практика : зб. матеріалів 3-ї міжнар. наук.-практ. конф. (Київ, 20–21 квіт. 2017 р.) / відп. ред.: С. Г. Стеценко, Л. О. Васечко. — Київ, 2017. — С. 91–94.
24. Харитонов Є. О. Інтернет-право, інформаційне право та ІТ-право: проблема співвідношення / Є. О. Харитонов, О. І. Харитонova // *Правова адаптація законодавства України до умов внутрішнього ринку ЄС: матеріали Міжнар. інтернет-конф., присвяч. пам'яті І. В. Шерешевського* (Одеса, 2 груд. 2016 р.). — Одеса : Фенікс, 2016. — С. 3–7.
25. Харитонов Є. О. Інтерпретація пропріетарної концепції права інтелектуальної власності у контексті DCFR / Є. О. Харитонов, О. І. Харитонova // *Актуальні проблеми юридичної науки : зб. Міжнар. наук. конф. «П'ятнадцять осінніх юридичних читань» (Хмельницький, 21–22 жовт. 2016 р.) : у 2 ч. / Хмельн. ун-т упр. та права.* — Хмельницький, 2016. — Ч. 1. — С. 159–161.
26. Харитонов Є. О. Цивільні правовідносини : монографія / Є. О. Харитонов, О. І. Харитонova. — 2-ге вид., перероб. і допов. — Одеса : Фенікс, 2011. — 456 с.
27. Харитонova О. І. Відносини, що виникають у мережі інтернет: специфіка і проблеми визначення правової природи // *Вісник Південного регіонального центру Національної академії правових наук України.* — 2016. — № 6. — С. 63–68.
28. Харитонova О. І. До проблеми визначення правової природи мережі Інтернет / О. І. Харитонova, Д. Позова // *Вісник Південного регіонального центру Національної академії правових наук України.* — 2015. — № 4. — С. 79–88.
29. Харитонova О. І. Адміністративно-правові відносини (проблеми теорії) : монографія / О. І. Харитонova. — Одеса : Юрид. літ., 2004. — 328 с.
30. Харитонova О. І. До питання про коректність вживання термінопоняття «Інтернет-відносини» // *«Римське право і сучасність» (Шерешевські читання) : матеріали Міжнар. наук. конф. (Одеса, 11 трав. 2012 р.).* — Одеса, 2012. — Ч. 1. — С. 111–112.
31. Харитонova О. І. До проблеми визначення суб'єктного складу відносин у мережі Інтернет // *Проблеми вдосконалення цивільного законодавства України : матеріали круглого столу (Одеса, 12 трав. 2012 р.) / за ред. Є. О. Харитонova.* — Одеса : Фенікс, 2012. — С. 143–145.
32. Харитонova О. І. Електронні твори як об'єкти авторського права в епоху комп'ютерних технологій // *Правові та інституційні механізми забезпечення розвитку держави та права в умовах євроінтеграції : матеріали Міжнар. наук.-практ. конф. (Одеса, 20 трав. 2016 р.) : у 2 т. / відп. ред. М. В. Афанасьєва.* — Одеса : Юрид. літ., 2016. — Т. 2. — С. 535–537.

33. Харитонова О. І. Інтерактивне громадянське суспільство: до проблеми формування // Римське право як підґрунтя сучасного права Європи : матеріали міжнар. наук.-практ. конф. (Одеса, 27 трав. 2016 р.) / за заг. ред. Є. О. Харитонова. — Одеса : Фенікс, 2016. — С. 103–105.
34. Харитонова О. І. Інтернет і поява нових категорій цивільного права: до постановки проблеми // Правові та інституційні механізми забезпечення розвитку держави та права в умовах євроінтеграції : матеріали Міжнар. наук.-практ. конф. (Одеса, 20 трав. 2016 р.) : у 2 т. / відп. ред. М. В. Афанасьєва. — Одеса : Юрид. літ., 2016. — Т. 2. — С. 556–559.
35. Харитонова О. І. Об'єкти авторського права і електронні бібліотеки // Роль принципів DCFR в імплементації угод про асоціацію ЄС-Україна : матеріали круглого столу (Одеса, 12 груд. 2015 р.) — Одеса : Фенікс, 2015. — С. 41–44.
36. Харитонова О. І. Перший посібник з ІТ-права // Право України. — 2016. — № 11. — С. 274–275.
37. Харитонова О. І. Питання боротьби з порушенням авторських прав у Всесвітній мережі Інтернет // Досвід правових реформ України та Республіки Молдова на шляху до євроінтеграції : матеріали інтернет-конф. (Одеса, 29 берез. 2016 р.) / за заг. ред. Є. О. Харитонова. — Одеса : Фенікс, 2016. — С. 58–61.
38. Харитонова О. І. Піратство у всесвітній мережі Інтернет // Правові та інституційні механізми забезпечення сталого розвитку України : матеріали Міжнар. наук.-практ. конф. (Одеса, 15–16 трав. 2015 р.) : у 2 т. / відп. ред. М. В. Афанасьєва. — Одеса : Юрид. літ., 2015. — Т. 2. — С. 507–509.
39. Харитонова О. І. Поняття піратства у сфері інтелектуальної власності // Актуальні проблеми держави і права : зб. наук. пр. / редкол.: С. В. Ківалов (голов. ред.), В. М. Дрьомін (заст. голов. ред.), Ю. П. Аленін [та ін.] ; МОН України, НУ ОЮА. — Одеса : Юрид. літ., 2012. — Вип. 66. — С. 231–238.
40. Харитонова О. І. Порушення прав інтелектуальної власності за законодавством України та Польщі в умовах інформаційного суспільства // Розвиток системи приватного права України та Польщі : матеріали круглого столу (Одеса, 15 жовт. 2016 р.) : у 2 ч. / за заг. ред. Є. О. Харитонова. — Одеса, 2016. — Ч. 1. — С. 8–12.
41. Харитонова О. І. Проблеми створення єдиного цифрового ринку й авторські права // Наукові праці Національного університету «Одеська юридична академія». — 2015. — Т. 16. — С. 44–50.
42. Харитонова О. І. Проблемні питання визначення системи (структури) ІТ-права // ІТ-право: проблеми та перспективи розвитку в Україні : зб. матеріалів наук.-практ. конф. — Львів: НУ «Львів. політехніка», 2016. — С. 280–285.

43. Харитонова О. І. Проблемні питання порушення авторських прав у Всесвітній мережі Інтернет // Правове життя сучасної України : матеріали Міжнар. наук.-практ. конф. (Одеса, 16– 17 трав. 2013 р.) / відп. за вип. В. М. Дрьомін ; Нац. ун-т «Одес. юрид. акад.». — Одеса : Фенікс, 2013. — Т. 2. — С. 652–654.
44. Харитонова О. І. Рецензія на посібник Т. В. Бачинського як привід для роздумів про систему ІТ-права // Часопис цивілістики. — 2016. — Вип. 22. — С. 145–148.
45. Харитонова О. І. Розвиток законодавства щодо регулювання відносин у мережі Інтернет: досвід ЄС // Цивілістичні читання, присвячені пам'яті І. В. Шерешевського «Проблеми адаптації законодавства України до законодавства ЄС: матеріали інтернет-конф. (Одеса, 11 груд. 2015 р.). — Одеса : Фенікс, 2015. — С. 9–14.
46. Харитонова О. І. Специфіка регулювання відносин у всесвітній мережі Інтернет: проблемні питання // Римське право і сучасність : матеріали Міжнар. наук. конф. (Одеса, 29 трав. 2015 р.) / за заг. ред. Є. О. Харитонова. — Одеса : Фенікс, 2015. — С. 90–91.
47. Харитонова О. І. Проблемні питання визначення правової природи і структури правовідносин інтелектуальної власності, що виникають у мережі Інтернет / О. І. Харитонова, Г. О. Ульянова [та ін.] // Наукові праці Національного університету «Одеська юридична академія» : зб. наук. пр. — Одеса, 2015. — Т. 17. — С. 159–200.
48. Харитонова О. І. «Інтернет-відносини» — віртуальна нереальність / О. І. Харитонова, Є. О. Харитонов // Захист права інтелектуальної власності у мережі Інтернет: теоретичні та практичні аспекти : матеріали Інтернет-конф. (Одеса, 22 трав. 2015 р. / за заг. ред. О. І. Харитонової ; упоряд.: А. В. Кирилюк, Н. П. Бааджи. — Одеса : Юрид. літ., 2015. — С. 72–75.
49. Харитонова О. І. Деякі проблеми захисту прав користувачів у мережі Інтернет / О. І. Харитонова, Є. О. Харитонов // Актуальні проблеми приватного права : матеріали наук.-практ. конф., присвяч. 94-й річниці з дня народж. д-ра юрид. наук, проф., чл.-кор. АН УРСР В. П. Маслова (Харків, 19 лют. 2016 р.). — Харків: Право, 2016. — С. 51–54.
50. Цехан Д. М. Правове регулювання мережі Інтернет як передумова її декриміналізації // Актуальні проблеми держави і права : зб. наук. пр. — 2012. — Вип. 65. — С. 668–676.
51. Kharitonova O. I. Some aspects of the legal nature of the internet network / O. I. Kharitonova, D. D. Pozova // Часопис цивілістики. — 2016. — Вип. 20. — С. 188–192.

Харитонов Євген Олегович, доктор юридичних наук, професор, член-кореспондент Національної академії правових наук України, заслужений діяч науки та техніки України, завідувач кафедри цивільного права Національного університету «Одеська юридична академія»

Харитонova Олена Іванівна, доктор юридичних наук, професор, член-кореспондент Національної академії правових наук України, заслужений діяч науки та техніки України, завідувач кафедри права інтелектуальної власності та корпоративного права Національного університету «Одеська юридична академія»

Куліч Ольга Олексіївна, доктор юридичних наук, в.о. завідувача кафедри інтелектуальної власності та цивільно-правових дисциплін Київського інституту інтелектуальної власності та права Національного університету «Одеська юридична академія»

Берназ-Лукавецька Олена Михайлівна, кандидат юридичних наук, доцент, доцент кафедри цивільного права Національного університету «Одеська юридична академія»

Давидова Ірина Віталіївна, кандидат юридичних наук, доцент, доцент кафедри цивільного права Національного університету «Одеська юридична академія»

Колодін Денис Олексійович, кандидат юридичних наук, доцент, доцент кафедри кримінального права Національного університету «Одеська юридична академія»

Некіт Катерина Георгіївна, кандидат юридичних наук, доцент, доцент кафедри цивільного права Національного університету «Одеська юридична академія»

Радейко Роман Ігорович, кандидат юридичних наук, асистент кафедри адміністративного та інформаційного права Національного університету «Львівська політехніка»

Сафончик Оксана Іванівна, кандидат юридичних наук, доцент, доцент кафедри цивільного права Національного університету «Одеська юридична академія»

Пасій Богдан Володимирович, кандидат юридичних наук, доцент кафедри цивільного права Національного університету «Одеська юридична академія»

Цуркану Сюзанна Іванівна, кандидат юридичних наук, доцент кафедри міжнародного права та порівняльного правознавства Міжнародного гуманітарного університету

Толмачевська Юлія Олегівна, магістрантка факультету цивільної та господарської юстиції Національного університету «Одеська юридична академія»

ЗМІСТ

Харитонов Є. О., Некіт К. Г.

Соціальні мережі у системі правових зв'язків	3
Розділ 1. Концептуальні питання правового регулювання відносин у онлайн-соціальних мережах (<i>Харитонов Є. О.</i>)	9
Розділ 2. Соціальні мережі і права інтелектуальної власності: проблеми і перспективи (<i>Харитонova О. І.</i>)	22
Розділ 3. Інтерактивні соціальні мережі – парадигма громадянського суспільства цифрової доби? (<i>Харитонов Є. О., Харитонova О. І.</i>)	41
Розділ 4. Правове регулювання відносин користування соціальними мережами (<i>Толмачевська Ю. О.</i>)	56
Розділ 5. Правочини в соціальній мережі (<i>Давидова І. В.</i>)	65
Розділ 6. Акаунт у соціальній мережі як об'єкт цивільних правовідносин (<i>Некіт К. Г.</i>)	77
Розділ 7. Правовий статус реклами в соціальних мережах (<i>Фасій Б. В.</i>)	93
Розділ 8. Проблеми забезпечення правової охорони зображення людини у соціальних мережах (<i>Кулініч О. О.</i>)	102
Розділ 9. Захист персональних даних у соціальній мережі (<i>Берназ-Лукавецька О. М.</i>)	113
Розділ 10. Деякі проблеми реалізації права дитини на захист персональних даних у мережі Інтернет згідно із законодавством ЄС (<i>Цуркану С. І.</i>)	122
Розділ 11. Блокування, фільтрація та видалення контенту в соціальних мережах (<i>Радейко Р. І.</i>)	135
Розділ 12. Поняття та види інформаційних правопорушень у соціальних мережах (<i>Сафончик О. І.</i>)	148
Розділ 13. Цивільна та кримінальна відповідальність при користуванні соціальними мережами (<i>Фасій Б. В., Колодін Д. О.</i>)	159
Вибрані праці одеської школи ІТ-права	168
Авторський колектив	173

- Актуальні проблеми цивілістики у цифрову добу :**
А437 онлайніві соціальні мережі : монографія / за ред. Є. О. Харитонова, О. І. Харитонової ; уклад. Б. В. Фасій ; НУ ОЮА. — Одеса : Юридична література, 2018. — 176 с. — (Серія : Цивілістика та «ІТ-право»).
- ISBN 978–966–419–355–6.
ISBN 978–966–419–340–2 (серія).

У монографії досліджуються актуальні проблеми, що виникають у зв'язку з інтенсивним розвитком інформаційних технологій, ІТ-права, призначеного забезпечити регулювання відносин в ІТ-сфері, та соціальних мереж. Аналізуються особливості правового регулювання соціальних мереж, зокрема концептуальні питання правового регулювання відносин у онлайн-ових соціальних мережах, правочинів, акаунтів, реклами, захисту персональних даних, блокування, фільтрації та видалення контенту в соціальних мережах, цивільної та кримінальної відповідальності при користуванні соціальними мережами.

Монографія розрахована на наукових та науково-педагогічних працівників вищих навчальних закладів і наукових установ, студентів юридичного напрямку, практичних працівників судових, правоохоронних, правозастосовних органів, а також усіх, хто цікавиться проблемами ІТ-права та соціальними мережами.

Наукове видання

Серія
ЦИВІЛІСТИКА ТА «ІТ-ПРАВО»

*Євген Олегович ХАРИТОНОВ
Олена Іванівна ХАРИТОНОВА
Ольга Олексіївна КУЛІНІЧ та ін.*

АКТУАЛЬНІ ПРОБЛЕМИ ЦИВІЛІСТИКИ У ЦИФРОВУ ДОБУ: Онлайнві соціальні мережі

Монографія

За редакцією
Є. О. Харитонова, О. І. Харитонової

Редактор-коректор *Н. І. Крилова*
Технічний редактор *Т. В. Іванова*

Формат 60×84/16. Ум. друк. арк. 10,23.
Тираж 300 прим. Зам. № 174 (25).

Видавництво і друкарня «Юридична література»
65009, м. Одеса, вул. Піонерська, 7. Тел./факс: 777-48-79
Свідцтво суб'єкта видавничої справи
ДК № 4284 від 23.03.2012 р.