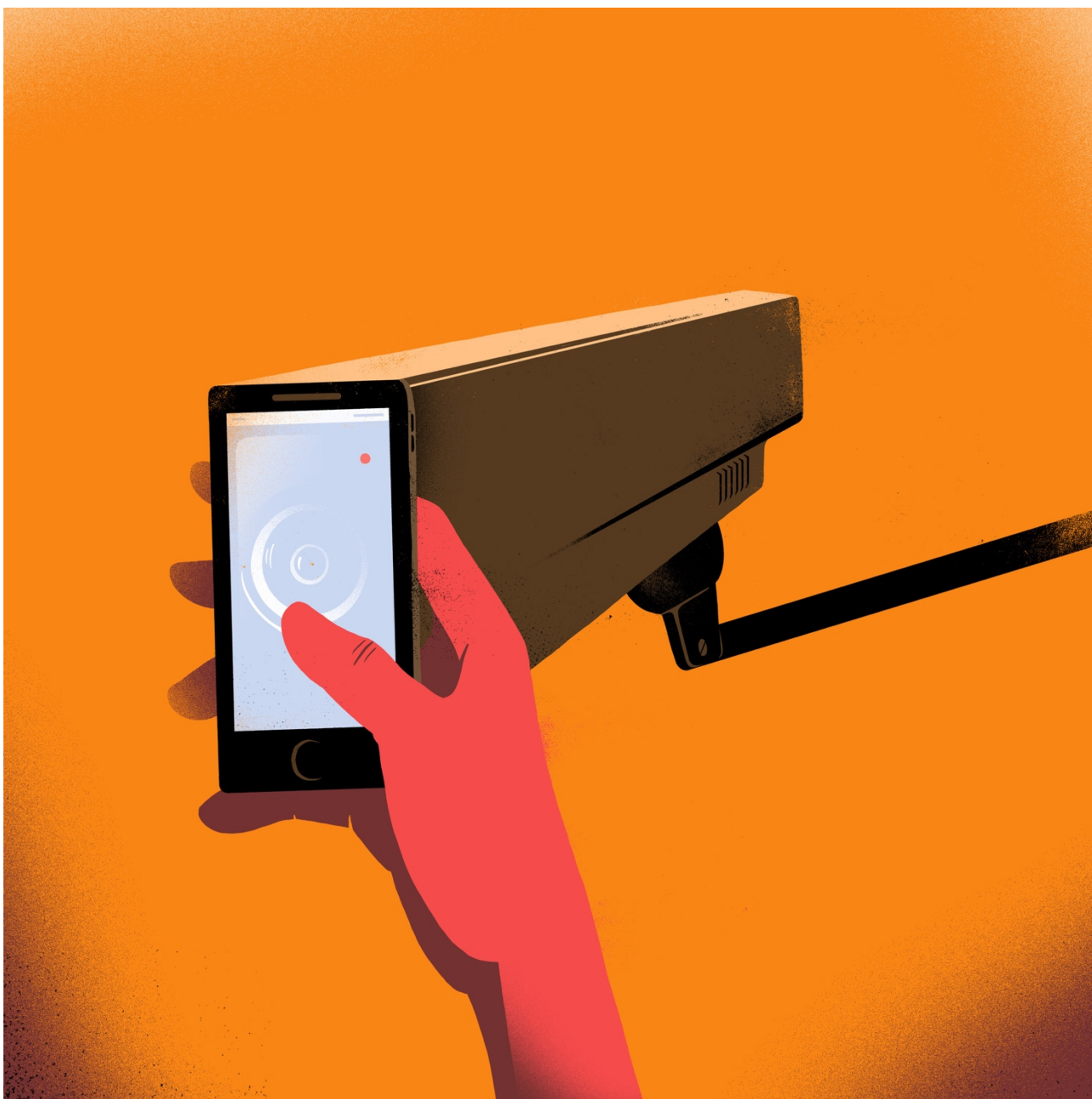




Гіганти стеження

Як бізнес-модель Google та Facebook несе загрозу правам людини

Amnesty International – це глобальний рух, що складається з понад 7 мільйонів людей, які борються за світ, де нічийі права людини не порушують.

Наше бачення – щоб всі люди мали змогу користуватися всіма правами, що вказані в Загальній декларації прав людини та інших міжнародних правозахисних стандартах.

Ми не залежимо від жодного уряду, жодної політичної ідеології, економічних інтересів чи релігії та переважно отримуємо фінансування від учасників руху та через публічні пожертви.

© Amnesty International 2019

Де не зазначено інше, до змісту цього документу застосовується ліцензія Creative Commons (вказання авторства, некомерційне використання, недопущення зміни вмісту, міжнародна версія 4.0).

<https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>

Щоб отримати більше інформації, будь ласка, відвідайте сторінку Permissions («Дозволи») на сайті www.amnesty.org

До тих частин матеріалу, інтелектуальне право на які не належить Amnesty International, не застосовується ліцензія Creative Commons.

Вперше опубліковано у 2019 році Amnesty International Ltd.

Пітер Бененсон Хаус, Істон-Стріт 1, Лондон, Велика Британія, WC1X 0DW

Код: POL 30/1404/2019

Мова оригіналу: англійська

Amnesty.org

← Всі зображення © Себастьян Тібо/agoodson.com

Гіганти стеження:

Як бізнес-модель Google та Facebook несе загрозу правам людини

Зміст

Аналітичне резюме.....	5
1. Бізнес на основі стеження	9
Бізнес-модель Google і Facebook.....	10
Домінування Google і Facebook	11
Добування та накопичення даних.....	13
Збір даних на Глобальному Півдні	15
Повсюдне стеження.....	17
Бізнес і права людини	19
2. Напад на приватність.....	21
Бізнес-модель на основі стеження та право на приватність	21
Захист даних.....	23
Обіцянки дотримуватися приватності та нездатність це робити: історія.....	25
Доступ держав до сховищ даних Google і Facebook.....	27
Права людини в Google і Facebook.....	28
3. Масштабна аналітика даних: додаткові ризики для прав людини.....	31
Зростання персоналізації, профайлінгу та мікротаргетингу.....	32
Вплив на думки та переконання	33
Масштабна прихована маніпуляція.....	35
Скандал із Cambridge Analytica	36
Максимальне збільшення взаємодії	38
Практичний приклад: екосистема радикалізації на YouTube	40
Дискримінація	42
4. Концентрація влади — перешкода для підзвітності	45
Стеження як плата за доступ до інтернету	45
Зосередження влади погіршує наслідки.....	47
Порушення прав людини сприяють концентрації влади	48
Влада перешкоджає корпоративній підзвітності.....	49
Корпоративне лобіювання	52
Перешкоди для поновлення в порушених правах.....	54
Висновки та рекомендації.....	56
Рекомендації для держав	57
Рекомендації для компаній	58

Аналітичне резюме

Інтернет різко змінив наш світ — змін такого масштабу не відбувалося з часів винайдення електрики. Понад половина населення світу користується інтернетом, щоб читати новини, спілкуватися з рідними, шукати роботу чи відповіді на термінові запитання. Він створив соціальні й економічні можливості такого масштабу і з такою швидкістю, які більшість людей п'ятдесят років тому не могли й уявити собі.

Враховуючи цю зміну, доступ до інтернету зараз вже вважається необхідним для забезпечення прав людини. Для понад 4 мільярдів людей інтернет став ключовим елементом спілкування, навчання, участі в економічній діяльності та соціальної й політичної самоорганізації.

Разом з цим, онлайн-життя цих мільярдів людей переважно залежить від сервісів, якими володіють лише дві корпорації. Дві компанії контролюють основні канали, якими послуговуються люди при користуванні інтернетом. Саме вони є власницями настільки важливих сервісів, що без них годі й уявити собі інтернет.

Facebook – найбільший оператор соцмереж у світі. Якщо поррахувати загальну кількість користувачів і користувачок його соціальної платформи, сервісів для обміну повідомленнями WhatsApp і Messenger, а також таких додатків, як Instagram, виявиться, що третина людей на планеті щодня користуються якимсь сервісом, що належить Facebook. Саме ця компанія визначає умови значної частини спілкування між людьми в цифрову епоху.

Інша компанія, Google, — власниця ще більшої частки онлайн-світу. Пошукові служби — критично важливе джерело інформації, і саме через Google відбувається близько 90% всього пошуку в інтернеті. Веб-переглядач Google Chrome — найбільш популярний серед аналогів у світі. Відеоплатформа YouTube, що належить цій компанії, — друга за розміром пошукова служба у світі та найбільша платформа відеоконтенту. На мобільній операційній системі Android, що належить Google, працює абсолютна більшість смартфонів світу.

Домінування Android особливо критичне, оскільки смартфони вже замінили комп'ютери як основний засіб доступу до інтернету та його використання. Смартфони знають про нас далеко не лише ту інформацію, що ми переглядаємо онлайн — вони також знають, куди ми їздимо і де перебуваємо. Вони часто містять тисячі приватних мейлів та повідомлень, фотографії, контакти та записи в календарі.

Google і Facebook допомогли нам встановити зв'язок зі світом і дали можливість мільярдам людей використовувати свої сервіси. Щоб бути залученими в сучасну економіку та суспільне життя, а також щоб користуватися правами людини, люди використовують доступ до інтернету — й інструменти, які пропонують Google і Facebook.

Однак попри те, що їхні сервіси дійсно важливі, люди систематично платять чималу ціну за використання платформ Google і Facebook. Бізнес-модель цих компаній, що ґрунтується на стеженні за людьми, змушує користувачів і користувачок іти на фаустівську угоду, в якій вони мусять коритися системі, що працює завдяки порушенням прав людини, щоб користуватися своїми правами людини онлайн. Починається все з порушення права на приватність у досі небачених масштабах, а далі спрацьовує ефект доміно, бо наслідки цього порушення серйозно загрожують деяким іншим правам, від свободи висловлювань та переконань до свободи думки та права не бути дискримінованими.

Це не той інтернет, на який колись погодилися люди. Коли Google і Facebook були започатковані зо двадцять років тому, в обох компаній були кардинально інакші бізнес-моделі, які не залежали від повсякчасного стеження. Те, що Google і Facebook поступово руйнували приватність — безпосередній наслідок того, як ці компанії займали лідерську позицію на ринку та починали контролювати глобальний онлайн-простір.

У розділі 1, «Бізнес на основі стеження», у звіті пояснюється, як працює бізнес-модель, що ґрунтується на стеженні: Google і Facebook пропонують безкоштовні послуги мільярдам людей — натомість громадяни платять за ці послуги своєю особистою інформацією. Зібравши ці дані, Google і Facebook використовують їх, щоб аналізувати людей, ділити їх на групи та передбачати їхні інтереси, характеристики і, зрештою, поведінку — насамперед для того, щоб використовувати цю інформацію для збільшення доходів від реклами.

Ця система стеження простягається далеко за межі пошукового рядка Google чи самої соцмережі Facebook. За людьми стежать по всьому інтернету, через додатки на телефонах, а також у реальному світі, поки вони займаються повсякденними справами.

Ці дві компанії збирають детальну інформацію про те, що ми шукаємо, куди ходимо, з ким розмовляємо, що кажемо, що читаємо, а за допомогою аналізу, що став можливим завдяки технологічному прогресу, можуть вгадувати наш можливий настрій, етнічне походження, сексуальну орієнтацію, політичні погляди та вразливі місця. Деякі з цих категорій інформації — включаючи характеристики, що захищаються відповідно до законів про права людини — вони надають третім сторонам, щоб вони могли обирати цільову аудиторію для реклами чи іншої інформації.

У розділі 2, «Напад на приватність», ми пояснюємо, як це повсякчасне стеження зруйнувало саму сутність нашого права на приватність. Йдеться не лише про втручання в особисте життя мільярдів людей, яке зовсім не можна вважати необхідним чи бодай пропорційним, а й про те, що як умову використання своїх сервісів ці компанії поставили «згоду» на обробку та поширення особистої інформації для маркетингу та реклами, що прямо суперечить праву вирішувати, коли і як наші особисті дані можна поширювати третім особам. Нарешті, використання алгоритмів, щоб створювати і вгадувати детальні характеристики людей, позбавляє нас можливості формувати власну ідентичність приватно.

Спершу цією інформацією користувалися рекламодавці, але як тільки ці банки даних було створено, вони стали ласим шматочком для урядових структур. Все просто: збір даних мільярдів користувачів і користувачок, який проводили Google і Facebook, сягнув такого

рівня, що якби уряди намагалися збирати їх безпосередньо, з цим би ніхто не мирився. Обидві компанії відмовлялися надавати інформацію про своїх користувачів і користувачок урядовим структурам, однак можливість доступу до таких даних значно знизила мотивацію урядів регулювати те, як корпорації збирають дані про користувачів і користувачок.

Порушення приватності — наріжний елемент бізнес-моделі Google і Facebook, що ґрунтується на стеженні — яскраво проявляється у численних скандалах на цю тему в обох компаній. Попри запевнення цих компаній, що вони дотримуються політики приватності, такі порушення вбачаються швидше як елемент нормального функціонування їхнього бізнесу, а не як виняткові випадки.

У розділі 3 «Масштабна аналітика даних: додаткові ризики для прав людини» ми розглядаємо, як платформи Google і Facebook залежать не лише від збору величезної кількості даних користувачів і користувачок, а й від отримання додаткових висновків й інформації на основі цих даних за допомогою складних алгоритмічних систем. Ці системи створено для того, щоб знайти якнайкращий спосіб досягти тих результатів, які потрібні компанії, включно з якнайточнішою демонстрацією реклами та «гачками», які змушують людей повертатися на платформу. В результаті, коли дані користувачів і користувачок вже було зібрано, ця інформація повертається до них самих.

Вже виявлено, що такі системи алгоритмів мають ефект доміно, що серйозно загрожує правам людини, включно зі свободою висловлювань та переконань, свободою думки та правом на рівність і недискримінацію. Ці ризики тільки підсилює те, наскільки великі та потужні платформи Google і Facebook, оскільки їхній масштаб уможливлює загрозу для прав людини на рівні цілого народу. До того ж, системи, що займаються аналізом складних даних, не завжди зрозумілі навіть для спеціалістів із комп'ютерних наук, не кажучи вже про мільярди людей, дані яких при цьому обробляються.

Скандал із Cambridge Analytica, у якому було зібрано дані з профілів 87 мільйонів користувачів і користувачок Facebook з метою мікротаргетингу та маніпуляції в рамках передвиборчих політичних кампаній показав усьому світові, наскільки велика здатність цих платформ маніпулювати людьми у великих масштабах — і наскільки велика загроза того, що цими даними недоброчесно скористається хтось інший. Однак яким би шокуючим не був цей випадок, це була лише верхівка того айсберга стеження, без якого неможлива бізнес-модель Google і Facebook.

Нарешті, у розділі 4 «Концентрація влади — перешкода для підзвітності» ми показуємо, як завдяки величезним обсягам накопичених даних та обчислювальним потужностям Google і Facebook стали одними з найдорожчих і найсильніших компаній у наш час. Ринкова вартість Google майже вдвічі перевищує ВВП Ірландії (де розташовані центральні європейські офіси обох компаній), а вартість Facebook на третину вища. Бізнес-модель обох компаній допомогла їм фактично монополізувати владу, включно з фінансовим потенціалом, політичним впливом та здатністю творити онлайн-досвід мільярдів людей. Наслідком цього стала безпрецедентна асиметрія знання між компанією та інтернет-користувачами та користувачками — як зазначає науковиця Шошана Зубофф: «Вони знають про нас все, ми про них — майже нічого».

Ця влада, сконцентрована у двох компаній, тісно пов'язана з наслідками такої бізнес-моделі для прав людини і створила прогалину в підзвітності, за якої державній владі складно притягнути ці компанії до відповідальності, а окремим користувачам і користувачкам — домогтися справедливості.

Держави зобов'язані захищати людей від порушень прав людини з боку корпорацій. Але протягом останніх двох десятиліть ІТ-компанії переважно мали можливість самостійно регулювати свою діяльність — у 2013 році колишній генеральний директор Google Ерік Шмідт описав онлайн-світ як «найбільший некерований простір у світі». Разом з тим, регуляторні установи та державні органи влади у різних юрисдикціях почали більше схилитися до того, що треба боротися з владою, зосередженою в руках Google і Facebook. Вони розслідують діяльність цих компаній у зв'язку з антимонопольними порушеннями, штрафують їх за порушення європейського Регламенту захисту персональних даних або встановлюють окремі правила оподаткування для великих ІТ-компаній.

Компанії відповідальні за дотримання прав людини в контексті своєї діяльності, що зобов'язує їх проводити так звану «правозахисну перевірку», щоб визначити можливі наслідки їхньої роботи для прав людини та вжити заходів для недопущення порушень. Google і Facebook прийняли політики та процедури, щоб забезпечити дотримання приватності та свободи висловлювання, — однак, враховуючи, що їхня бізнес-модель на основі стеження підриває саму сутність права на приватність та серйозно загрожує деяким іншим правам, вони не переймаються ані комплексним підходом до цих політик, ані тим, чи їхня нинішня бізнес-модель узагалі поєднується з відповідальністю за дотримання прав людини.

Amnesty International дала і Google, і Facebook можливість відреагувати на результати цього звіту до його публікації. Лист Facebook, надісланий у відповідь, подано в додатку до звіту. Amnesty International також поспілкувалась із менеджерами Google високого рівня, які надали інформацію про відповідні політики та практики. Зміст обох відповідей використовується у тексті звіту.

Зрештою, вже очевидно, що доба саморегулювання у сфері технологій добігає кінця: потрібне буде потужніше державне регулювання, але критично важливо, щоб підхід до цього регулювання, в якій би формі воно не здійснювалось, ґрунтувався на дотриманні прав людини. Урядам слід вжити заходів для зменшення шкоди від бізнес-моделей на основі стеження — запровадити політику цифрового регулювання, що мала б на меті забезпечити універсальний доступ до прав людини та їх дотримання, зменшити чи ліквідувати нав'язливе стеження та втілити реформи, зокрема структурні, які б відновили довіру до інтернету.

1. Бізнес на основі стеження

«Ми не заробляємо на тому, що ми створюємо... ми заробляємо на користувачах».

Енді Рубін, співзасновник Android, 2013¹

Щоразу, коли ми взаємодіємо з онлайн-платформами, ми залишаємо по собі слід даних, цифровий запис про наші дії. Коли ми відправляємо мейл, зміст повідомлення, час відправки, адресат, адресант та інша інформація записуються і зберігаються на серверах і в центрах зберігання й обробки даних. Подібним чином зберігаються відомості про нас, коли ми щось переглядаємо в інтернеті, використовуємо додаток на телефоні чи купуємо щось карткою онлайн. Наше життя все більше проходить саме в інтернеті, і до нього під'єднано все більше пристроїв і послуг, від машин і тостерів до цілих фабрик — і разом з цим все більше зростає обсяг збережених даних про нас.

Цифрові «сліди», які ми залишаємо, в якійсь мірі — лише побічний продукт роботи комп'ютерних технологій, які обробляють цифрову інформацію. Але ІТ-компанії вже давно зрозуміли, наскільки важливі дані, і виявили, що цей «вихлоп» насправді є дуже цінним джерелом інформації. Дані часто називають «ною нафтою», і хоч ця аналогія недосконала², великі ІТ-компанії дійсно вже замінили нафтових гігантів на позиції найдорожчих компаній світу³. Через масовий збір та монетизацію даних — насамперед для реклами — стеження стало «бізнес-моделлю інтернету»⁴.

«Дані» можуть здаватися абстрактною концепцією. Але вони включають факти про наше життя і поведінку, а коли ці факти обробляють і організують, вони розкривають чимало інформації про наші переконання, поведінку та ідентичність. Захист персональних даних вже давно вважається критично важливим для забезпечення права на приватність⁵, права, яке в свою чергу захищає простір, де ми можемо вільно виражати свою ідентичність⁶. Невиправдане та надмірне втручання в персональні дані — це втручання в наше особисте життя. Це також ставить під загрозу нашу здатність вільно і незалежно розвиватися та

¹ Стівен Леві, Wired, «Історія Moto X зсередини: чому Google купив компанію Motorola», 8 січня 2013 року (Steven Levy, Wired, The Inside Story of the Moto X: The Reason Google Bought Motorola, 8 January 2013)

² Наприклад, див. Бернард Мapp, «Ось чому дані — не нова нафта», Forbes, 5 березня 2018; Жослін Голдфайн, Айві Нгуєн, «Дані — не нова нафта», Tech Crunch, 27 березня 2018

³ Statista, «Сто найбільших компаній у світі за ринковою вартістю у 2019 році», серпень 2019
<https://www.statista.com/statistics/263264/topcompanies-in-the-world-by-market-value/>

⁴ Брюс Шнаєр, «Стеження — бізнес-модель інтернету», квітень 2014,
https://www.schneier.com/news/archives/2014/04/surveillance_is_the.html

⁵ «С і Марпер проти Великої Британії», Заяви № 30562/04 і 30566/04, ЄСПЛ, 4 грудня 2008; а в 1988 у Загальному коментарі 16 про право на приватність (HRI/GEN/1/Rev.9 (Vol. I), Комітет ООН з прав людини зазначає, що «збір та зберігання персональної інформації на комп'ютерах, у банках даних та на інших пристроях, з боку державної влади чи приватних осіб чи установ, повинні регулюватися законом. Держави повинні вжити ефективних заходів для недопущення передачі інформації про приватне життя особи тим, хто за законом не уповноважений отримувати, обробляти і використовувати таку інформацію, а також щоб така інформація не використовувалась із метою, що несумісна з цим Пактом». (пункт 10)

⁶ Комітет ООН з прав людини, Куріель і Аурік проти Нідерландів (1994), Комунікація №453/1991, пункт. 10.2

виражати думки і переконання, що робить нас вразливими до зовнішнього впливу і контролю.

У цьому звіті викладено наслідки бізнес-моделі на основі стеження, за якою працює інтернет, для прав людини, з особливою увагою до двох компаній — Google і Facebook. Спершу в цьому розділі пояснюється, як ці дві компанії започаткували бізнес-модель, що ґрунтується на зборі, аналізі й отриманні вигоди від даних людей, що часто описується як «капіталізм стеження»⁷. Таким чином вони встановили майже повну монополію над основними каналами, через які люди спілкуються та взаємодіють із інтернетом, знаходять інформацію та діляться нею онлайн, що перетворює ці компанії на таких собі посередників між більшістю людства й інтернетом. Це наділяє їх безпрецедентною корпоративною владою впливати на те, як люди використовують свої права.

Бізнес-модель Google і Facebook

Послуги, що надають Google і Facebook, генерують дохід завдяки накопиченню й аналізу даних про людей⁸. Замість того, щоб отримувати оплату за продукти чи послуги, ці компанії натомість вимагають від користувачів і користувачок, щоб вони ділилися своїми персональними даними.

Facebook і Google (дочірня компанія холдингу Alphabet Inc.) — багатонаціональні конгломерати, діяльність яких значно різниться залежно від того, про яку структурну частину, продукт чи послугу йдеться. Однак діяльність обох компаній ґрунтується на тій самій ключовій бізнес-моделі, а саме:

- а) розвитку цифрових продуктів та послуг, які корисні людям, та зборі детальних даних про людей, які використовують ці платформи чи взаємодіють із ними. Однак, як роз'яснюється в Розділі 2, йдеться не лише про людей, зареєстрованих на цих платформах, а й про всіх, хто стикається з повсюдним стеженням від цих компаній, встановленим на різних інтернет-сторінках;
- б) використанні алгоритмів для аналізу цього великого об'єму зведених даних, створенні детальних профілів окремих осіб та груп людей та передбаченні поведінки й інтересів людей;
- в) продажі доступу до цієї інформації будь-кому, хто хоче донести інформацію до конкретної групи людей. Головна мета цих компаній — продавати розміщення реклами, що дає змогу маркетологам і рекламодавцям знаходити конкретну цільову аудиторію онлайн⁹. Важливо зауважити, що ці компанії не продають персональні дані самі по собі.

⁷ . Шошана Зубофф, «Доба капіталізму стеження: боротьба за людське майбутнє на новому фронті влади», 2018 (Зубофф, 2018)

⁸ Facebook заявляє, що його бізнес не побудовано на зборі даних про людей, і що збір даних не є кінцевою метою компанії — натомість Facebook фінансується за рахунок продажу реклами. Див. Додаток.

⁹ Alphabet, Щорічний звіт за формою 10-K, 2018, частина 1, пункт 1, доступ за адресою <https://www.sec.gov/Archives/edgar/data/1652044/000165204419000004/goog10-kq42018.htm> ; Facebook, щорічний звіт за формою 10-K, 2018, частина 1, пункт 1 доступ за адресою <https://www.sec.gov/Archives/edgar/data/1326801/000132680119000009/fb-12312018x10k.htm>

Дохід Google і Facebook майже цілком складається з доходу від реклами — на 84% і 98% відповідно¹⁰. Інформація, якою вони володіють, настільки приваблива для рекламодавців, що про ці компанії часто кажуть, що вони мають «дуополію» на ринку онлайн-реклами¹¹. Однак йдеться не лише про рекламу: інформація в їхніх сховищах даних — а також інформація, яку Google і Facebook отримують із цих даних за допомогою комп'ютерного аналізу, — приваблює чимало зацікавлених сторін, від компаній, які встановлюють вартість страховок, до правоохоронних органів.

Розвиток «великих даних» і постійне відстежування життя людей онлайн породили те, що називають «золотою добою стеження» для урядів: влада отримала доступ до детальної інформації про те, що робить населення, який до цифрової доби годі було й уявити¹². Разом з тим, бізнес-модель Google і Facebook відчутно виграла від підходу «невтручання» в регулювання ІТ-індустрії в таких країнах, як Сполучені Штати Америки — рідній країні обох компаній (див. розділ 4 нижче)¹³. Публічне і приватне стеження паралельно стрімко розвиваються принаймні з 2001 року¹⁴.

Домінування Google і Facebook

Екосистема даних — масштабна і складна, і складається вона з мережі пов'язаних між собою гравців у різних секторах. Серед «великої п'ятірки» ІТ-компаній — до якої зазвичай включають Facebook, Amazon, Apple, Microsoft і Google — Amazon і Microsoft теж частково запровадили викладену вище бізнес-модель¹⁵. Amazon є лідером на ринку інтернет-торгівлі, а ще Amazon і Microsoft — лідери на ринку хмарної інфраструктури, і саме на їхніх серверах зберігається значна частина даних у світі¹⁶. Окрім відомих брендів, є чимала мережа компаній, які заробляють на використанні даних, включно з «брокерами даних», які збирають та торгують даними з різних джерел, та індустрією «реklamних технологій», яка забезпечує аналітику й інструменти для цифрової реклами¹⁷. Компанії-постачальники телекомунікаційних послуг також перейшли до впровадження технологій таргетованої реклами. Все більше компаній у різних галузях переходять до бізнес-моделей, що ґрунтуються на використанні даних.

¹⁰ Reuters, «Доходи компанії-власниці Google, Alphabet, не відповідають оцінкам, зростають найповільніше за останні три роки», 29 квітня 2019; Facebook, Результати за другий квартал 2019, 24 липня 2019

¹¹ Шошана Водінські, «Цифрова дуополія все ще керує світом реклами», 22 березня 2019

¹² Обидві компанії вказали на свої політики та звіти про прозорість, що стосується реакції на запити урядів на дані, яка відповідає нормам у сфері прав людини. Google, «Легальний процес запиту даних користувачі та користувачки», поширені запитання»: <https://support.google.com/transparencyreport/answer/7381738>; Facebook, «Урядові запити про дані користувачі та користувачки», <https://transparency.facebook.com/government-data-requests>

¹³ Експерт з кібербезпеки Брюс Шнаєр стверджує, що «уряди насправді не хочуть обмежувати власний доступ до даних, руйнуючи свою корпоративну «годівничку». Брюс Шнаєр, «Дані та Голіаф», 2015 (Шнаєр 2015)

¹⁴ Зубофф, 2018, с. 115

¹⁵ Дохід Apple переважно надходить від продажу технологічних пристроїв та послуг для споживачів.

¹⁶ ZDNet, «Найбільші хмарні сервіси 2019 року», серпень 2019, <https://www.zdnet.com/article/top-cloud-providers-2019-aws-microsoft-azure-googlecloud-ibm-makes-hybrid-move-salesforce-dominates-saas/>

¹⁷ Privacy International, «Як компанії, що працюють з даними, отримують наші дані?» 25 травня 2018 <https://privacyinternational.org/feature/2048/how-do-datacompanies-get-our-data>

Однак у Google і Facebook є безпрецедентний контроль над тим, що люди роблять онлайн, оскільки вони встановили контроль над основними каналами взаємодії з інтернетом, якими користується більшість людей. Google і Facebook, а також компанії, що їм належать, такі як YouTube і WhatsApp, виступають посередниками, коли люди шукають інформацію та діляться нею, дискутують та беруть участь у суспільному житті. Платформи цих компаній стали невід'ємною частиною сучасного світу та спілкування людей у ньому.

Звісно, в різних країнах є винятки, насамперед у Китаї. Китайський уряд встановив «фаєрвол», технічний набір заходів, що контролюють, якими додатками та сайтами можуть користуватися китайські користувачі та користувачки, що виділяє Китай серед глобальної інтернет-економіки і дає змогу уряду підтримувати репресивну інтернет-цензуру і режим онлайн-стеження¹⁸. Це означає, що в Китаю переважно окрема екосистема китайських інтернет-послуг, у якій WeChat і Weibo виконують більшість функцій Facebook, а Baidu — найпопулярніша пошукова система, що замінює Google.

За межами ж Китаю домінування Google і Facebook різке очевидне у наступних сферах:

- Соцмережі: Facebook домінує серед соціальних мереж, маючи 2,45 мільярдів активних користувачів і користувачок основної платформи на місяць, що становить близько 70% користувачів і користувачок соцмереж і значно переважає над найближчими конкурентами¹⁹.
- Обмін повідомленнями: WhatsApp, месенджер, що належить Facebook, разом із Facebook Messenger, займають близько 75% ринку обміну повідомленнями за межами Китаю²⁰.
- Пошук: Google з величезним відривом лідирує як пошуковий сервіс, оскільки 90% пошукових запитів в інтернеті проводяться саме через платформи Google²¹. Корпоративна назва Google стала синонімом пошуку в інтернеті.
- Відео: YouTube, що належить Google, є другою найбільшою пошуковою системою у світі, а також найбільшою відео-платформою²².
- Веб-перегляд: Google Chrome — найбільший веб-переглядач у світі, що означає, що саме Google забезпечує доступ до всього інтернету²³.

¹⁸ Див. наприклад щорічний звіт Amnesty International, профіль Китаю, 2017/2018
<https://www.amnesty.org/en/countries/asia-and-the-pacific/china/report-china/>

¹⁹ Facebook, Інформація про компанію, де згадується статистика за користувачами та користувачками станом на 30 вересня 2019 р.; StatCounter, «Статистика за соцмережами в усьому світі», жовтень 2018 — жовтень 2019
<https://gs.statcounter.com/social-media-stats>

²⁰ Statista, «Найпопулярніші месенджери у світі у 2019 році», станом на липень 2019
<https://www.statista.com/statistics/258749/most-popularglobal-mobile-messenger-apps/>.

²¹ Visual Capitalist, «Ця діаграма показує, наскільки Google дійсно панує в цифровому просторі», квітень 2018 р.
<https://www.visualcapitalist.com/this-chartreveals-googles-true-dominance-over-the-web/>

²² Mushroom Networks, «YouTube: другий найбільший пошуковий сервіс», 2018
<https://www.mushroomnetworks.com/infographics/youtube---the-2nd-largest-search-engine-infographic/>.

²³ Statista, «Частка глобального ринку, яку займають інтернет-переглядачі, 2012-2019», станом на вересень 2019,
<https://www.statista.com/statistics/268254/market-share-of-internet-browsers-worldwide-since-2009/>.

- Мобільні платформи: Android, що належить Google, — найбільша мобільна операційна система у світі²⁴. Щомісяця нараховується понад 2,5 мільярди активних користувачів і користувачок Android-пристроїв²⁵. Це означає, що Google постійно присутній на пристрої, який розкриває найбільше інформації про життя людини в сучасному світі, — на смартфоні.

- Реклама: Google і Facebook разом отримують понад 60% доходу від онлайн-реклами у світі²⁶, а також саме на них припадає 90% зростання ринку цифрової реклами²⁷.

Влада, якою наділені Google і Facebook в інтернеті, становить унікальну загрозу для прав людини, як пояснюється в подальших розділах. Як зображено у статистиці вище, для більшості людей було б просто неможливо використовувати інтернет, уникаючи послуг Google і Facebook²⁸. Ці платформи-лідери в багатьох випадках перетворилися на неодмінну умову участі в сучасному суспільному житті.

Добування та накопичення даних

Як ми вже побачили, бізнес-модель Google і Facebook заснована насамперед на добуванні та накопиченні величезного об'єму даних про людей. Ці компанії не лише збирають наші дані, а й використовують їх для того, щоб визначити нову інформацію про нас. Їхні платформи працюють на передових розробках штучного інтелекту та машинного навчання, які можуть визначити надзвичайно детальні характеристики людей та зібрати їх у дуже конкретні групи.

Щоб збільшити дохід від реклами, Google і Facebook конкурують, щоб запропонувати якнайкращі передбачення про користувачів і користувачок. Щоб цього досягти, вони мають розширювати сховища даних та збільшувати точність алгоритмів передбачення. Це мотивує компанії збирати все більше даних про людей, щоб збільшити свій вплив на інтернет, на фізичний світ та, зрештою, на весь світ в цілому.

Цей «експансіоністський» підхід до добування даних відбувається в кількох формах. По-перше, компанії збирають та зберігають значні об'єми даних про людей²⁹. Наприклад, Google за замовчуванням зберігає історію пошуку на всіх пристроях особи, інформацію про

²⁴ StatCounter, «Ринкова частка мобільних операційних систем у світі», жовтень 2018 — жовтень 2019 <https://gs.statcounter.com/os-marketshare/mobile/worldwide>

²⁵ VentureBeat, «Android долає позначку 2.5 мільярди активних пристроїв щомісяця», травень 2019 р. <https://venturebeat.com/2019/05/07/android-passes-2-5-billion-monthly-active-devices/>

²⁶ eMarketer, «Витрати на цифрову рекламу в 2019 році», березень 2019 р. <https://www.emarketer.com/content/global-digital-ad-spending-2019>

²⁷ AdExchanger, «Ринок цифрової реклами злітає до рівня у 88 мільярдів доларів США, Facebook і Google займають 90% зростання», травень 2018 р. <https://adexchanger.com/online-advertising/digital-ad-market-soars-to-88-billion-facebook-and-google-contribute-90-of-growth/>

²⁸ Кашмір Гілл, «Прощавайте, Велика п'ятірка», Gizmodo, січень 2019 р., <https://gizmodo.com/c/goodbye-big-five>

²⁹ У своїй відповіді (див. Додаток) Facebook стверджує, що єдина особиста інформація, яку він вимагає від людей при реєстрації — «ім'я, вік, гендер та контактна інформація». Однак Facebook також збирає чималий обсяг даних про користувачів та користувачки після того, як вони реєструються, зокрема зміст інформації, якою вони діляться на Facebook, інформацію про те, з ким люди зв'язуються чи взаємодіють на платформі, та що вони там роблять. Див. Політику даних Facebook, <https://www.facebook.com/policy.php>

всі додатки та розширення, якими ця особа користується, та всю історію переглядів на YouTube³⁰, в той час як Facebook збирає інформацію навіть про тих людей, у яких немає облікового запису на Facebook³¹.

Колись дані збиралися як побічний продукт надання інтернет-послуги і розглядалися як «сміття» чи «вихлоп», але відкриття, що ці дані розкривають важливу інформацію про поведінку людей — а отже, їх можна монетизувати — стало ключовим кроком у розвитку бізнес-моделі Google і Facebook³². Це відкриття поєднувалося зі швидким зниженням витрат на збереження даних, що означало, що в ІТ-компаній з'явилася можливість розширювати свої сховища даних в рамках стандартної роботи³³.

Бізнес-модель Google і Facebook також мотивує так звану «датафікацію» — перетворення на дані такої кількості аспектів життя у сучасному світі, які раніше ніколи не обчислювалися³⁴. Саме стеження перетнуло межу до фізичного світу, оскільки поширення «Інтернету речей»³⁵ створює світ, повний сенсорів, що аналізують середовище. Вони проникли в будинки людей завдяки використанню Домашніх асистентів, таких як Assistant від Google та Portal від Facebook, а також систем смарт-будинків, що поєднують численні пристрої, такі як телефони, телевізори та системи опалення³⁶. Добування даних також все більше проникає у міський простір завдяки інфраструктурі «смарт-міст», що створена для збору даних на міських територіях³⁷. Facebook навіть розробляє технологію, яка могла б відстежувати роботу людського мозку³⁸.

Ці компанії також постійно шукають можливості вийти на нові міжнародні ринки (див. рамку нижче). Найяскравіший приклад — «безкоштовний» інтернет-доступ від Facebook під назвою Free Basics, в рамках якого Facebook уклав угоду з мобільними операторами в 65 країнах, щоб надати людям доступ до інтернету. У кількох країнах Глобального Півдня Free

³⁰ Ділан Курран, Guardian, «Ви готові? Ось всі дані про вас, які мають Google і Facebook», березень 2018 р.

³¹ Facebook, Складні запитання: «Які дані Facebook збирає, коли я ним не користуюся, і навіщо?» Квітень 2018 р., <https://newsroom.fb.com/news/2018/04/data-off-facebook>. Facebook заявляє, що не створює профілі людей, які не є користувачами та користувачками платформи — див. Додаток

³² Zuboff наводить патент, поданий Google у 2003 році, щоб продемонструвати перехід компанії до моделі поведінкового таргетування. У патенті написано «даний винахід може включати новітні методи, способи, формати повідомлень і/або структури даних, щоб визначити інформацію про користувачі та користувачки та використовувати таку інформацію для показу реклами». Шошана Зубофф, «Як Google відкрив цінність стеження», 2019 <https://longreads.com/2019/09/05/how-google-discovered-the-value-of-surveillance/>

³³ Шнаєр 2015, с. 27

³⁴ Кеннет Ніл Цукер і Віктор Маєр-Шунбергер, «Поширення великих даних: як вони змінюють наш погляд на світ», Foreign Affairs, травень/червень 2013, <https://www.foreignaffairs.com/articles/2013-04-03/rise-big-data>

³⁵ Інтернет речей можна описати як все більшу мережу пристроїв, що під'єднані до інтернету, від смарт-холодильників до розумних систем обігріву, що дозволяє їм спілкуватися з користувачами та користувачками і розробниками, додатками і одне з одним завдяки збору та обміну даними про середовище, яке вони моніторять.

³⁶ CNet, Google називає прихований у Nest мікрофон «помилкою», лютий 2019 р.

³⁷ Стеження за людьми у фізичному світі — мета іншої дочірньої компанії Alphabet, Sidewalk Labs, яка розробляє технології «розумного міста» та забезпечує ними муніципалітети. Див. Еллет П. Гудман, Джулія Паулз, «Урбаністика в часи Google: уроки з тротуару Торонто», Fordham Law Review, травень 2019 р. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3390610

³⁸ TechCrunch, «Facebook досліджує контроль над мозком для пристроїв доповненої реальності», липень 2019 р. <https://techcrunch.com/2019/07/30/facebook-is-exploring-brain-control-for-ar-wearables/>

Basics — це і є інтернет³⁹. Приклад такого розширення Google — проект Dragonfly, спроба компанії наново вийти на ринок пошукових систем у Китаї — й отримати доступ до даних про понад 800 мільйонів інтернет-користувачів і користувачок⁴⁰. Це тривало, поки протести власних працівників Google та правозахисних груп не змусили компанію закрити програму⁴¹.

Збір даних на Глобальному Півдні

І Facebook, і Google роблять спроби розширити свій вплив у країнах, що розвиваються, на Глобальному Півдні⁴². Ці нові ринки надали б Google і Facebook вигідні можливості розвитку, насамперед завдяки потенційному збільшенню обсягу даних, до яких компанії мають доступ.

Сервіс Free Basics — ще один спосіб, що дозволяє Facebook збирати масиви даних про людей у країнах, що розвиваються. Згідно з нещодавнім світом ООН, «Для рекламних платформ, таких як Google і Facebook, більше (місцевих) даних означало б можливість надавати кращу, точніше адресовану рекламу... Завдяки Free Basics від Facebook інтернет-трафік фактично проходить через портал, що відповідає бізнес-моделі, яку Facebook використовує на більш закритій платформі»⁴³. У відповідь на цей звіт (див. Додаток) Facebook стверджує, що «Free Basics не зберігає інформації про те, що люди роблять чи переглядають у будь-якому сторонньому додатку».

Разом з тим, відповідно до політики приватності Free Basics, вони таки збирають дані про використання сторонніх сервісів, щоб пропонувати більш персоналізовані послуги, та зберігають інформацію про сервіси, якими користувалися люди — разом з їхніми номерами телефонів — на 90 днів⁴⁴. Facebook позиціонує Free Basics як благодійну ініціативу, яка

³⁹ Люди у країнах, що розвиваються, які можуть собі дозволити платити за інтернет, найчастіше використовують телефони на ОС Android, що означає, що Google може стежити і за ними.

⁴⁰ China Internet Watch, «Статистика китайських інтернет-користувачів та користувачкив станом на 2019 рік», квітень 2019 р., де йдеться про кількість інтернет-користувачів та користувачкив Китаю станом на грудень 2018 року. З коментарів голови пошукової системи Google Бена Гомеса, які випадково потрапили в пресу, стало відомо, що проект Dragonfly був частиною ініціативи компанії «Наступний мільярд користувачів та користувачкив», що мала на меті розширити базу користувачів та користувачкив по всьому світу. Див. Раян Галлагер, «Розшифровка приватної зустрічі в Google суперечить офіційним заявам Google про Китай», The Intercept, 9 жовтня 2018 р.

⁴¹ Amnesty International, «Google повинен взяти на себе зобов'язання ніколи не впроваджувати цензуру пошуку в Китаї», липень 2019 р.

⁴² Wired, «Перегони Facebook and Google, щоб зробити світ ближчим, стають все більш запеклими», 26 липня 2018 р., <https://www.wired.co.uk/article/google-projectlooon-balloon-facebook-aquila-internet-africa>

⁴³ Конференція ООН про торгівлю та розвиток, Звіт з цифрової економіки за 2019 р., вересень 2019 р., доступ за посиланням: https://unctad.org/en/PublicationsLibrary/der2019_en.pdf

⁴⁴ Facebook, про приватність у Free Basics, тут: https://www.facebook.com/legal/internet.org_fbsterms. Згідно з політикою: «Щоб це все працювало, ми отримуємо та зберігаємо обмежений обсяг інформації — доменне ім'я або назву стороннього сервісу, доступ через які було отримано через Free Basics, та який обсяг даних (в мегабайтах) було використано при доступі до такого сервісу. Ця інформація також допомагає нам покращувати та персоналізувати ваше користування Free Basics, бо з її допомогою ми можемо надавати прискорений доступ до сервісів, якими ви найчастіше користуєтесь. Ми зберігаємо цю інформацію разом з вашим номером телефону лише протягом 90 днів, після чого вона зводиться або іншим чином позбавляється ідентифікаторів».

забезпечує «вхід до ширшого інтернету» для людей на Глобальному Півдні, які без цієї послуги не мали б доступу до інтернету — але натомість, схоже, ця ініціатива радше забезпечує доступ до все більшого збору даних про користувачів і користувачок у цьому регіоні⁴⁵.

Дослідження Privacy International виявило, що недорогий мобільний телефон на системі Android від Google, розроблений для ринку Філіппін, недостатньо захищений, особливо через попередньо встановлені виробником додатки, що можуть дати доступ до даних користувачів і користувачок шахрям, політичним партіям й урядовим установам⁴⁶.

Користувачі та користувачки на Глобальному Півдні, для яких такі дешевші пристрої можуть бути єдиним способом доступу до інтернету, таким чином стають ще більш вразливими до масового стеження та практики експлуатації їхніх даних.

Google і Facebook також знаходять нові сегменти ринку, завдяки яким вони можуть збирати ще більше даних. Facebook займається впровадженням нової глобальної криптовалюти, Libra — через таке рішення компанії спільноти захисту даних з усього світу висловили побоювання щодо наслідків поєднання великих обсягів персональних даних з фінансовою інформацією⁴⁷. Доступ Google до даних пацієнтів Національної служби здоров'я Великобританії, спершу через дочірню компанію DeepMind, а тепер прямо через підрозділ Health, від самого початку вважався і донині вважається неоднозначним явищем через ризик, що ці дані можна поєднати з даними зі сховищ Google⁴⁸. Google також нещодавно придбав компанію фітнес-трекінгу Fitbit, що дало Google доступ до найбільшої бази даних у світі про рівень активності людей, фізичні вправи та сон⁴⁹.

Прагнення розширити обсяги наявних даних також мотивує технічних гігантів поєднувати та зводити дані з різних платформ, що в свою чергу збільшує владу та домінування цих компаній. У 2012 році Google провів масштабне оновлення політики приватності, запроваджуючи дозвіл на поєднання даних різних сервісів, на що негативно відреагували захисники приватності та регуляторні органи⁵⁰. Подібним чином, коли Facebook придбав WhatsApp у 2014 році, компанія публічно заявляла про те, що ці сервіси залишаться приватними, однак у 2016 році компанія запровадила неоднозначне оновлення політики

⁴⁵ Facebook Free Basics <https://connectivity.fb.com/free-basics/>

⁴⁶ Privacy International, «Купуєте дешевий смартфон? Приватність може бути додатковою ціною, яку ви заплатите», 20 вересня 2019 р., <https://privacyinternational.org/long-read/3226/buying-smart-phone-cheap-privacy-might-be-price-you-have-pay>

⁴⁷ Спільна заява про глобальні очікування від приватності мережі Libra, 5 серпня 2019 р. <https://ico.org.uk/media/about-the-ico/documents/2615521/libra-network-joint-statement-20190802.pdf>

⁴⁸ Наташа Ломас, «Те, як Google зжер додаток про здоров'я від DeepMind, може бути тим шоком, який нам всім потрібен», TechCrunch, листопад 2018 р., <https://techcrunch.com/2018/11/14/google-gobbling-deepminds-health-app-might-be-the-trust-shock-we-need/>. Google стверджує, що підрозділи Національної служби здоров'я «повністю контролюють усі дані пацієнтів, а ми лише використовуємо ці дані, щоб допомогти покращити піклування про пацієнтів, під контролем та за інструкціями НСЗ», <https://www.blog.google/technology/health/deepmind-health-joins-google-health/>

⁴⁹ Fitbit, «Google купує Fitbit», 1 листопада 2019 р., <https://investor.fitbit.com/press/press-releases/press-release-details/2019/Fitbit-to-Be-Acquired-by-Google/default.aspx>

⁵⁰ The Verge, «Зміни в політиці приватності Google у 2012 році: реакції», лютий 2012 р., <https://www.theverge.com/2012/2/1/2763898/google-privacy-policy-changes-terms-of-service-2012>

приватності, що дозволило обмін даних між цими сервісами, зокрема з рекламною метою⁵¹. Через розслідування цієї справи європейськими регуляторними органами компанії довелося відмовитися від цього оновлення в межах ЄС⁵². За наявною інформацією, Facebook планує в майбутньому ще більш тісно інтегрувати Facebook, Messenger, Instagram і WhatsApp, але компанія заявляє, що це не дозволить їй збирати більше даних про користувачів і користувачок⁵³.

Повсюдне стеження

Експерт з кібербезпеки Брюс Шнаєр описує оптову природу даних в інтернеті як «повсюдне стеження»⁵⁴. На практиці це означає, що за людьми постійно стежать, коли вони займаються повсякденними справами онлайн, і все більше це стеження переходить і до фізичного світу.

Стеження сягає далеко за межі інформації, яку користувачі та користувачки надають, використовуючи самі Google і Facebook, такої як електронна адреса, дата народження та номер телефону — сюди належать також місце перебування, історія пошуку та використання додатків.

Google і Facebook — основні суб'єкти стеження за онлайн-активністю, включно з пошуковими запитами, сайтами, які відвідують користувачі та користувачки, та локацією, з якої вони це роблять. Наприклад, Google збирає дані за допомогою механізму стеження, вбудованого в переглядач Chrome та операційну систему Android, через будь-які сайти, що використовують Google-аналітику, та за допомогою AdSense, рекламної програми від компанії. Facebook відстежує дані, коли користувач чи користувачка відвідує сайт із плагіном Facebook, таким як кнопки «Подобається» чи «Поділитися», або прихованим кодом під назвою Facebook Pixel. У 2018 році Facebook заявив, що «Кнопка «Подобається» встановлена на 8,4 млн сайтів, кнопка «Поділитися» — на 931 тисячі сайтів, а Facebook Pixel працює на 2,2 млн сайтів» — і Facebook отримує інформацію, коли будь-який користувач чи користувачка заходить на один з цих сайтів⁵⁵.

У відповіді Facebook на цей звіт (див. Додаток), компанія пояснює, що «Facebook вже не зберігає даних із соціальних плагінів (таких як кнопка «Подобається»), з яких можна ідентифікувати користувача або пристрій, окрім як із метою безпеки та запобігання

⁵¹ Наташа Ломас, «WhatsApp буде ділитися з даними користувачі та користувачки з Facebook для таргетування реклами — ось як від цього відмовитися», TechCrunch, серпень 2016 р. <https://techcrunch.com/2016/08/25/whatsapp-to-share-user-data-with-facebook-for-ad-targeting-heres-how-to-opt-out/>

⁵² Управління комісара Великої Британії з інформації «Перемога для захисту даних британських споживачів», березень 2018 р., <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/03/blog-a-win-for-the-data-protection-of-uk-consumers/>

⁵³ Майк Айзек, «Цукерберг планує об'єднати WhatsApp, Instagram і Facebook Messenger», New York Times, 25 січня 2019 р., <https://www.nytimes.com/2019/01/25/technology/facebook-instagram-whatsapp-messenger.html>; Див. відповідь Facebook на резюме звіту Amnesty International в додатку.

⁵⁴ Шнаєр 2015, с. 38

⁵⁵ Ребекка Стімсон, голова публічної політики, Facebook Велика Британія, Лист голові Комітету з цифрової політики, культури, медіа та спорту Палати громад Великої Британії, 14 травня 2018 р., с. 2 <https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/180514-RebeccaStimson-Facebook-to-Ctte-Chair-re-oral-ev-follow-up.pdf>

шахрайству». При цьому з політики даних Facebook очевидно, що компанія як мінімум отримує такі дані: «Рекламодавці, розробники та веб-майстри можуть надсилати нам інформацію через Бізнес-інструменти Facebook, які вони використовують, включно з соціальними плагінами... Ці партнери надають нам інформацію про ваші дії за межами Facebook... незалежно від того, чи є у вас обліковий запис Facebook і чи ви залогінені»⁵⁶.

Смартфони дедалі частіше використовують як основний засіб доступу до інтернету — а ще вони збирають чималий набір даних, від даних про локацію до інформації з усіх додатків і сервісів на телефоні⁵⁷.

Абсолютна більшість смартфонів використовують Android, операційну систему від Google — одне дослідження виявило, що телефон на Android, яким власник навіть не користується, надсилає в Google 900 одиниць даних за 24 години, включно з даними про географічні координати⁵⁸. Sensorvault, база даних Google про локацію з телефонів на Android, включає «детальні записи про місце перебування з принаймні сотень мільйонів пристроїв по всьому світу за майже десять років»⁵⁹. Facebook також відстежує користувачів і користувачок Android за допомогою своїх додатків, включно з інформацією про історію дзвінків і повідомлень — хоча компанія стверджує, що робить це лише зі згоди користувачів і користувачок⁶⁰. Крім того, інші додатки Android також можуть ділитися даними з Facebook⁶¹.

Що важливо, інформація, яку збирають Google і Facebook, це не просто самі по собі дані, а метадані, або «дані про дані». Сюди належать, зокрема, адресати мейлів, записи про місце перебування та час, коли було відправлено мейл або зроблено фото. Все більш поширене використання наскрізного шифрування повідомлень, наприклад, у WhatsApp, означає, що

⁵⁶ Політика даних Facebook, <https://www.facebook.com/policy.php>. В політиці cookie-файлів Facebook також йдеться про те, що «ми можемо розміщувати реп'яшки на вашому комп'ютері або пристрої й отримувати інформацію, що зберігається в реп'яшках, коли ви використовуєте чи відвідуєте... сайти та додатки інших компаній, що використовують продукти Facebook... Facebook використовує реп'яшки та отримує інформацію, коли ви відвідуєте такі сайти та додатки, зокрема інформацію про пристрій і про ваші дії, без будь-яких додаткових дій з вашого боку. Це відбувається незалежно від того, чи ви маєте обліковий запис у Facebook та чи ви залогінені». <https://www.facebook.com/policies/cookies>

⁵⁷ Світовий центр дослідження реклами (WARC), «Майже три чверті інтернет-користувачі та користувачки будуть користуватися лише мобільними пристроями до 2025 року», січень 2019 р.; «Дослідження New York Times про відстеження координат у смартфонах показало, що продаються великі обсяги особистих даних про координати. Див. «Ваші додатки знають, де ви були минулого вечора, і вони не тримають це в секреті», 10 грудня 2018 р., <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html>

⁵⁸ Професор Дуглас С. Шмідт, Університет Вандербільта, «Збір даних Google — наступним буде цифровий контент», серпень 2018 р., пункт 24, <https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf>

⁵⁹ За словами працівників Google, коментарі яких включено в матеріал The New York Times, «Відстежуючи телефони, Google — бажана система для поліції», квітень 2019 р. <https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.htm>

⁶⁰ Комітет з цифрової політики, культури, медіа та спорту Палати громад Великої Британії, Кінцевий звіт про дезінформацію і «фейкові новини», лютий 2019 р., с. 35; Facebook, «Перевірка фактів: ваша історія дзвінків і повідомлень», 25 березня 2018 р., <https://newsroom.fb.com/news/2018/03/fact-check-your-call-and-sms-history/>

⁶¹ Privacy International, «Як додатки на Android діляться інформацією з Facebook», грудень 2018 р. Дослідження виявило, що 61% додатків, що було автоматично перевірено, передають дані в Facebook, щойно користувач чи користувачка відкриє додаток; після цього частина цих додатків припинили таку практику. <https://privacyinternational.org/appdata>

зараз навіть самі компанії часто не можуть отримувати доступ до змісту спілкування. Разом з тим, добре відомо, що метадані «становлять інформацію, яка настільки ж приватна і стосується права на приватність, як і сам зміст листування»⁶². Управління Верховного комісара ООН з прав людини (УВКПЛ) визнає, що при аналізі та зведенні метадані «можуть надати навіть більше інформації про поведінку користувача, соціальні взаємини, особисті вподобання та ідентичність, ніж сам зміст комунікації»⁶³.

Крім того, хоча зміст даних вже розкриває чимало інформації про окрему особу чи невелику групу людей, коли дані збираються в таких масштабах, як це роблять Google і Facebook, метадані стають більш цінними, уможливлючи складну аналітику, яка передбачає сценарії поведінки в масштабах населення⁶⁴ і яка потенційно може використовуватися, щоб розкрити особисту інформацію про людину, таку як сексуальна ідентичність, політичні погляди, риси характеру чи сексуальна орієнтація, за допомогою складних алгоритмів⁶⁵. Ці припущення можна робити незважаючи на те, якими даними поділився сам користувач, і часто саме вони впливають на сприйняття користувачів і користувачок третіми сторонами: наприклад, такі дані вже використовувалися, щоб визначити, кому показувати рекламу оренди⁶⁶ і хто відповідає критеріям для надання кредиту⁶⁷.

Бізнес і права людини

Відповідно до міжнародних норм у сфері прав людини, відповідальність за дотримання прав людини покладається саме на держави, і вони зобов'язані захищати людей від порушення їхніх прав третіми сторонами, такими як корпорації. Рада ООН з прав людини підтвердила, що онлайн мають захищатися ті самі права людей, що й офлайн, і що держави зобов'язані створити та підтримувати «сприятливе онлайн-середовище», в якому буде забезпечено дотримання прав людини⁶⁸.

⁶² Tele2 Sverige AB і C-698/15 Ватсон та інші (ECLI:EU:C:2016:970) («Ватсон»), Суд Європейського Союзу, об'єднані справи C-203/15, пункт 99, <http://curia.europa.eu/juris/liste.jsf?num=C-203/15>

⁶³ Звіт УВКПЛ про право на приватність у цифрову добу, 30 червня 2014 р., A/HRC/27/37, пункт 19

⁶⁴ Саме з цієї причини WhatsApp настільки цінний. На відміну від інших платформ Facebook, у WhatsApp немає реклами, а завдяки наскрізному шифруванню, Facebook не може отримати зміст повідомлень, однак цей додаток передає Facebook величезний обсяг даних, зокрема інформацію про координати користувачів та користувачки, список контактів та метадані про понад 65 мільярдів повідомлень на день.

⁶⁵ Privacy International, «Приклади одиниць даних, що використовуються для профайлінгу», квітень 2018 р., https://privacyinternational.org/sites/default/files/2018-04/data%20points%20used%20in%20tracking_0.pdf; заявляє, що не робить висновків про сексуальну ідентичність, риси характеру чи сексуальну орієнтацію людей — див. Додаток

⁶⁶ Джулія Ан'він, Аріана Тобіт і Маделін Варнер, «Facebook (все ще) дозволяє тим, хто рекламує житло, виключати користувачів та користувачки за расою», ProPublica, листопад 2017 р. У березні 2019 р., Facebook оголосив про обмеження опцій таргетування рекламних оголошень на тему забезпечення житлом, вакансій чи надання кредитів у США в рамках угоди з організаціями захисту громадянських прав.

⁶⁷ Астра Тейлор і Ятан Садовські, «Як компанії перетворюють ваші дії у Facebook на кредитний рейтинг, The Nation, травень 2015 р., <https://www.thenation.com/article/how-companies-turn-your-facebook-activity-credit-score/>

⁶⁸ Рада ООН з прав людини, «Просування, захист і використання прав людини в інтернеті», липень 2018 р., Документ ООН: A/HRC/38/L.10/Rev.1

Компанії зобов'язані поважати права людини, які існують незалежно від здатності чи бажання держави виконувати свої зобов'язання з захисту прав, а також стоять вище за державні закони та регулювання⁶⁹. Стандарти взаємодії бізнесу і прав людини, такі як Керівні принципи ООН щодо бізнесу і прав людини, встановлюють «глобальний(-і) стандарт(и) очікуваної поведінки», які застосовуються до всієї діяльності компанії⁷⁰.

В рамках виконання цього зобов'язання компанії мають заявляти про підтримку прав людини на рівні власних політик, а також вжити тривалих, проактивних і реактивних заходів, щоб не допустити порушень прав людини в результаті їхньої діяльності — це процес, який називається «правозахисною перевіркою». В рамках правозахисної перевірки компанії мають визначити наслідки для прав людини, пов'язані з їхньою діяльністю (як реальні, так і потенційні), вжити заходів для їх запобігання та зменшення, а також прозоро звітувати про свої зусилля в цій сфері. До таких зусиль належать заходи для зниження серйозних ризиків для прав людини, що наявні у певній сфері через характеристики цієї сфери⁷¹.

⁶⁹ Керівні принципи ООН щодо бізнесу і прав людини: впровадження рамкової стратегії ООН «Захищати, поважати і поновлювати», 2011 р., Документ ООН HR/PUB/11/04, (Керівні принципи) www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

⁷⁰ Керівні принципи, принцип 11

⁷¹ Інструкція ОЕСР з належної перевірки для відповідального ведення бізнесу, розділ II, 2.1, Додаток, питання 22

2. Напад на приватність

«Ми знаємо, де ви. Знаємо, де ви були. Ми можемо в більшій чи меншій мірі дізнатися, про що ви думаєте».

Ерік Шмідт, колишній генеральний директор Google, 2010⁷²

Захисники приватності вже не перший рік критикують Google і Facebook. За останні два десятиріччя ці компанії зіткнулися з численними скандалами через те, як вони використовують персональні дані. Попри це, з кожним роком вони збирали й обробляли все більше даних, що й утворило нинішню архітектуру стеження, описану вище.

У 2010 році генеральний директор Facebook Марк Цукерберг зробив відому заяву про те, що соцмережі змінили приватність «як суспільну норму»⁷³. Насправді ж поширення цифрових технологій зробило приватність ще більш важливим правом у сучасному світі — однак бізнес-модель Google і Facebook підриває саму сутність права на приватність.

Facebook чітко заявив, що «зовсім не погоджується» з характеристикою своєї бізнес-моделі як такої, що «ґрунтується на стеженні», стверджуючи, що використання його продуктів цілком добровільне, а отже, відрізняється від урядового стеження, про яке йдеться у праві на приватність⁷⁴. Однак відповідно до міжнародних норм у сфері прав людини, право на приватність має бути захищене від свавільного втручання «від державної влади або від фізичних чи юридичних осіб [таких як корпорації]»⁷⁵. У цій секції пояснюється, як нинішні бізнес-практики Google і Facebook за своєю суттю несумісні з цим правом.

Бізнес-модель на основі стеження та право на приватність

Згідно з правом на приватність, ніхто не може зазнавати «безпідставного чи незаконного втручання» в особисте чи сімейне життя, недоторканність житла і таємницю кореспонденції, і це має захищатися законом⁷⁶. Комітет ООН з прав людини визнає, що такий захист включає регуляцію «збору та зберігання особистої інформації на комп'ютерах, у банках даних та інших пристроях, як з боку державної влади, так і з боку приватних осіб чи установ»⁷⁷.

Масштаб приватності розвивався паралельно зі змінами в суспільстві, особливо в контексті розвитку технологій. УВКПЛ заявило, що «приватність можна вважати презумпцією того, що

⁷² The Atlantic, Генеральний директор Google: «Закони пишуть лобісти», жовтень 2010 р., <https://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/>

⁷³ Енн Кавукян, (тодішня) Комісарка з інформації та приватності Онтаріо, «Приватність залишається соціальною нормою», The Globe та Mail, березень 2010 р., <https://www.theglobeandmail.com/opinion/privacy-is-still-a-social-norm/article1209523/>

⁷⁴ Лист Facebook до Amnesty International, листопад 2019 — див. Додаток

⁷⁵ Комітет ООН з прав людини, Коментар загального порядку №16 про право на приватність, HRI/GEN/1/Rev.9 (Vol. I), 1988, пункт 1. Керівні принципи ООН щодо бізнесу і прав людини також роз'яснюють, що компанії зобов'язані поважати «весь спектр міжнародно визнаних прав людини» (Принцип 12).

⁷⁶ Загальна декларація прав людини, стаття 12; Міжнародний пакт про громадянські та політичні права, стаття 17

⁷⁷ Комітет ООН з прав людини, Міжнародний пакт про громадянські та політичні права, коментар №16: стаття 17 (право на приватність), право на дотримання приватності особистого чи сімейного життя, недоторканності житла і таємниці кореспонденції, а також захист честі та репутації, 8 квітня 1988 р., <https://www.refworld.org/docid/453883f922.html>

особи повинні мати зону автономного розвитку, взаємодії та свободи, «приватну сферу», що включає чи не включає взаємодію з іншими, позбавлену втручання держави та надмірного безпідставного втручання з боку інших осіб»⁷⁸. Це включає в себе три взаємопов'язані концепції: свободу від втручання в приватне життя, право контролювати інформацію про нас та право на простір, у якому ми можемо вільно виражати свою ідентичність. Бізнес-модель Google і Facebook, що ґрунтується на стеженні, підриває всі три ці аспекти настільки, що вона зашкодила самій сутності приватності.

Верховний комісар ООН з прав людини визнає, що «сам по собі збір даних, що стосуються ідентичності людини, її родини чи життя, вже впливає на право на приватність, оскільки таким чином особа частково втрачає контроль над інформацією, яка ставить під загрозу її приватність»⁷⁹. Обсяги даних, які збирають Google і Facebook, означають, що ці компанії збирають більше інформації про людей та їхні дії, ніж колись було взагалі можливо. Зведення такого обсягу даних у поєднанні зі складними аналітичними інструментами може розкрити дуже особисту, детальну інформацію. Фактично, ці компанії знають майже все про окрему особу⁸⁰.

Втручання в право особи на приватність дозволяється за міжнародними стандартами прав людини лише в тому випадку, якщо це обґрунтовано і законно. Правозахисні механізми раз за разом тлумачать, що ці слова вказують на загальні принципи законності, необхідності та пропорційності⁸¹. Невибіркове корпоративне стеження у таких масштабах саме по собі не є необхідним та пропорційним і не може вважатися допустимим втручанням у право на приватність. Для порівняння, коли органи державної влади заявляли про те, що масове стеження за населенням необхідне в інтересах національної безпеки, правозахисні механізми відповідали, що така практика «недопустима відповідно до міжнародних стандартів у сфері прав людини, оскільки в контексті таких заходів неможливо провести індивідуалізований аналіз необхідності та пропорційності втручання»⁸².

Другий компонент приватності надає людям право на контроль над своєю особистою інформацією, або право на «самостійне розпорядження інформацією»⁸³, тобто здатність визначати, коли і як нашою особистою інформацією можна ділитися з іншими⁸⁴. На основі

⁷⁸ Верховний комісар ООН з прав людини, «Право на приватність у цифрову добу», 3 серпня 2018 р., A/HRC/39/29, para.5.

⁷⁹ A/HRC/39/29, пункт 7; див. також A/HRC/27/37, пункт 20; та ЄСПЛ, Вебер і Саравія проти Німеччини, пункт 78, Малоун проти Великої Британії, пункт 64

⁸⁰ Privacy International, «Картина корпоративного профайлінгу», квітень 2018 р., <https://privacyinternational.org/long-read/1721/snapshotcorporate-profiling>

⁸¹ A/HRC/27/37, пункти 21-27.

⁸² Звіт УВКПЛ про найкращі практики та отримані знання про те, як захист і просування прав людини допомагає запобігати жорстокому екстремізму та боротися з ним, 21 липня 2016 р., A/HRC/33/29, пункт 58; див. також Звіт Спеціального доповідача ООН про просування і захист прав людини та фундаментальних свобод при протидії тероризму, 23 вересня 2014 р., A/69/397, пункт 47; і A/HRC/27/37, пункт 25

⁸³ Термін «самостійне розпорядження інформацією» вперше використали в контексті німецького рішення щодо особистої інформації, яка збиралась протягом перепису населення 1983 року: Bundesverfassungsgericht [BVerfG], 15 грудня 1983 р., 65 Entscheidungen des Bundesverfassungsgerichts [BVerfGE] 1. Суд тлумачив це як здатність особи вирішувати, коли і в яких межах ділитися інформацією про своє особисте життя з іншими.

⁸⁴ Алан Вестін, «Приватність і свобода», 1967

цього формується захист даних, важливість якого особливо зросла після появи великих баз даних та на фоні технологічного прогресу. Європейський суд з прав людини визнає, що захист особистих даних критично важливий для того, щоб особа мала можливість користуватися своїм правом на приватність⁸⁵, і що приватність забезпечує право на самостійне розпорядження інформацією⁸⁶. Бізнес-модель на основі стеження прямо суперечить фундаментальним принципам, на яких ґрунтується цей другий компонент, а отже, шкодить здатності людей приймати рішення про власну особисту інформацію, включно з вільним вибором способів і причин використання їхніх даних (див. рамку нижче).

Захист даних

Загальний регламент про захист даних ЄС (ЗРЗД), який вступив у дію в травні 2018 року, став глобальним стандартом захисту даних та регулювання приватності. Google і Facebook зобов'язані дотримуватися ЗРЗД, що стосується всіх організацій, розміщених в ЄС, а також організацій за межами ЄС, якщо вони пропонують послуги чи відстежують поведінку осіб, що перебувають в ЄС.

Що важливо, цей регламент визначає персональні дані в широкому сенсі — це «будь-яка інформація, що стосується визначеної фізичної особи, або такої, яку можна визначити»⁸⁷. Визначення включає в себе дані, що пов'язані з особою, яку можна прямо чи непрямо ідентифікувати за допомогою таких даних⁸⁸. ЗРЗД роз'яснює, що персональні дані, переведені в анонімну форму, які при цьому можна віднести до конкретної особи за допомогою додаткової інформації, слід вважати інформацією особи, яку можна визначити⁸⁹. Так само, передбачення та висновки про особу належать до «особистих даних», якщо вони пов'язані з унікальними ідентифікаторами, або можна іншим чином встановити особу, якої такі дані стосуються.

Один із ключових принципів ЗРЗД — принцип «обмеження мети», який зобов'язує, щоб усі компанії, які збирають і оброблюють персональні дані, чітко зазначали мету обробки даних із самого початку, щоб вони зберігали записи про таку мету та чітко зазначали її в інформації про приватність, доступній особам, а також щоб вони використовували таку інформацію з новою метою лише за умови, що вона відповідає початковій меті, що особа надала свою згоду на таке використання, або що для цього є чітке законне підґрунтя⁹⁰.

ЗРЗД також встановлює високі стандарти згоди — під нею мається на увазі, що особа прийняла вільне, конкретне, поінформоване й однозначне рішення, яким вона чітко ствердно зазначає про свою згоду на обробку персональних даних, що її стосуються⁹¹. У ЗРЗД чітко вказано, що якщо обробка включає кілька цілей, особа має надати згоду на кожен

⁸⁵ С і Марпер проти Великої Британії», Заяви № 30562/04 і 30566/04, ЄСПЛ, 4 грудня 2008 р., доступ за адресою: <https://hudoc.echr.coe.int/eng?i=001-90051>

⁸⁶ Сатакуннан Марккінапорссі Ой та Сатамедія Ой проти Фінляндії, заява №931/13, ЄСПЛ, 27 червня 2017 р., пункт 137, доступ за адресою: <https://hudoc.echr.coe.int/eng#%7B%22itemid%22%3A%22001-175121%22%7D>.

⁸⁷ ЗРЗД, стаття 4(1)

⁸⁸ Там само

⁸⁹ ЗРЗД, преамбула, пункт 26.

⁹⁰ Див. ЗРЗД, статті 5(1)(б), 6(4) і 30, а також преамбулу, пункти 39 і 50.

⁹¹ ЗРЗД, стаття 4(1)

з них⁹², і що для забезпечення вільного висловлення згоди, обробка персональних даних не може мати легального підґрунтя у випадках, коли між контролером та особою наявний очевидний дисбаланс влади⁹³. На противагу вимозі вільного висловлення згоди, бізнес-модель на основі стеження робить згоду на обробку персональних даних та надання таких даних третім особам з маркетинговою та рекламною метою обов'язковою умовою використання своїх сервісів, що означає, що особа не може відмовитися або відкликати свою згоду так, щоб не бути виключеною з такого простору⁹⁴.

Нарешті, більшість експертів погоджуються, що приватність також є необхідним аспектом утворення та захисту простору, в якому ми конструємо свою ідентичність⁹⁵. Комітет ООН з прав людини визначає приватність, або особисту сферу, як «сферу життя людини, в якій він чи вона може вільно виражати свою ідентичність»⁹⁶. Це відображає думку, що наше відчуття власної ідентичності водночас соціально зумовлене та динамічне: ми проявляємо різні аспекти своєї особистості в різних контекстах, чи то з друзями, чи на роботі, чи на вулиці, і ці прояви постійно змінюються й адаптуються. Приватність дає нам змогу самостійно вирішувати, як ми хочемо, щоб інші нас бачили — і наша поведінка змінюється, коли за нами спостерігають, коли ми цього не хочемо. У цьому сенсі приватність є необхідною умовою автономії та здатності визначати власну ідентичність.

Люди, що перебувають під постійним наглядом, відчувають тиск бути схожими на інших. Ключова роль приватності у формуванні різних ідентичностей стимулює різноманіття культури. Багатшаровість ідентичностей часто є ключовою умовою для будь-якої меншини, що прагне жити, працювати та загалом існувати в іншій домінантній культурі. Наприклад, так можна охарактеризувати життя ЛГБТІ-людей, які живуть у середовищі, де одностатеві стосунки піддаються стигмі чи заборонені законом, також це може стосуватися ЛГБТІ-людей, які не живуть у такому середовищі, але в такому середовищі проживають члени їхньої родини⁹⁷. Крім того, це може стосуватися вразливих людей, залучених у тіньову економіку, таких як секс-працівників і працівниць⁹⁸.

Сам масштаб втручання бізнес-моделі Google і Facebook у наші приватні життя завдяки повсюдному й повсякчасному стеженню значно обмежив простір, у якому ми можемо визначати, хто ми. Право на приватність захищає нас від «намагань комерційних та

⁹² Див. ЗРЗД, статті 6(1)(а) та 7, а також преамбулу, пункт 32

⁹³ ЗРЗД, преамбула, пункт 43

⁹⁴ З такою «вимушеною згодою» триває юридична боротьба в рамках Загального регламенту про захист даних від імені організації «Нойб», що бореться за права споживачів: https://noyb.eu/wp-content/uploads/2018/05/pa_forcedconsent_en.pdf.

⁹⁵ Див., наприклад,, Аґре і Ротенбург (ред.), «Технологія і приватність: новий ландшафт», 1998; Джулі Е. Коен, 2013 р.

⁹⁶ Комітет ООН з прав людини, Куріель і Аурік проти Нідерландів (1994), комунікація №453/1991, пункт 10.2

⁹⁷ Див. Александр Дуст і Лукаш Шульц «Наші онлайн-«я»: соціальні, культурні та матеріальні контексти використання соцмереж геями в діаспорі», Social Media + Society, 2016 р., http://eprints.lse.ac.uk/87145/1/Szulc_Navigating%20online%20selves_2018.pdf

⁹⁸ Кашмір Гілл, «Як Facebook викриває секс-працівників і працівниць», Gizmodo, листопад 2017 р., <https://gizmodo.com/how-facebook-ousts-sexworkers-1818861596>

державних гравців зробити осіб та громади сталими, прозорими та передбачуваними»⁹⁹. Але сама природа таргетування, використання даних для висновків про детальні характеристики осіб, означає, що Google і Facebook визначають нашу ідентичність для решти світу, і часто це відбувається в контексті, що стосується наших прав. Це — втручання в наші приватні життя, що прямо суперечить нашому праву на самостійне розпорядження інформацією про себе та на визначення своєї ідентичності у приватній сфері.

Іншими словами, стеження в таких масштабах являє собою безпрецедентне втручання в право на приватність, яке не може бути сумісним із зобов'язаннями компаній дотримуватися прав людини. Наслідки виходять за межі втручання в усі аспекти нашого життя онлайн і насправді загрожують навіть нашому праву визначати, ким ми є в суспільстві як окремі особи.

Обіцянки дотримуватися приватності та нездатність це робити: історія

Нещодавно керівництво Google і Facebook визнало необхідність дотримуватися права на приватність у публічних заявах. У травні генеральний директор Google Сундар Пічаї опублікував колонку про приватність¹⁰⁰. У березні генеральний директор Facebook Марк Цукерберг оголосив, що його компанія змінить політику для кращого захисту приватності¹⁰¹, а в травні виголосив свою головну щорічну промову на фоні таблички «майбутнє — приватне»¹⁰².

В рамках цієї тенденції обидві компанії оголосили нові заходи, покликані дати користувачам і користувачкам змогу краще контролювати свою приватність на їхніх платформах¹⁰³. У листопаді Google оголосив, що запровадить жорсткіші обмеження даних, які надаються рекламодавцям через платформу рекламних аукціонів компанії, після того, як ірландський Офіс захисту даних розпочав розслідування обробки персональних даних в рамках роботи сервісу Google Ad Exchange¹⁰⁴. Гугл також представив нову функцію, що дозволяє користувачам і користувачкам видаляти інформацію про їхні координати (щоправда, лише після того, як така інформація зберігається принаймні три місяці)¹⁰⁵. Facebook почав впроваджувати інструмент, що дозволяє людям переглянути інформацію, якою інші додатки

⁹⁹ Джулі Е. Коен, 2013

¹⁰⁰ Сундар Пічаї, «Сундар Пічаї з Google: Приватність не має бути предметом розкоші», New York Times, 7 травня 2019 р.

¹⁰¹ Facebook, «Бачення соцмереж із фокусом на приватність», 6 березня 2019 р., <https://newsroom.fb.com/news/2019/03/vision-for-socialnetworking/>

¹⁰² Курт Вагнер і Селіна Ванг, «Власник Facebook Цукерберг закликає до приватності, але підтвердження неоднозначні», Bloomberg, 1 травня 2019 р.

¹⁰³ Обидві компанії також вказали на інструменти, які вони пропонують користувачам, щоб ті контролювали свої рекламні вподобання. Див. Google, «Керуйте тим, яку рекламу ви бачите», <https://support.google.com/accounts/answer/2662856>; Facebook <https://facebook.com/help/247395082112892>

¹⁰⁴ Google, «Додаткові кроки для захисту приватності користувачі та користувачки», 14 листопада 2019 р., <https://www.blog.google/products/admanager/additional-stepssafeguard-user-privacy>; Комісія з захисту даних Ірландії, «Комісія з захисту даних починає розслідування Google Ireland Limited», 22 травня 2019 р.

¹⁰⁵ Google, «Запуск функції автоматичного видалення історії місця перебування та даних про ваші дії», 1 травня 2019 р., <https://www.blog.google/technology/safety-security/automatically-delete-data>. Google також вказав, що працює над технологією інтегрованого навчання, див. <https://federated.withgoogle.com/>.

та сайти діляться з ним, та від'єднати ці дані від свого облікового запису (але не видалити їх повністю)¹⁰⁶.

Хоч це й може віщувати покращення практик дотримання приватності, численні коментатори скептично поставилися до думки, що Google і Facebook ґрунтовно змінять свою бізнес-модель та погляди, адже ці гіганти працюють завдяки стеженню¹⁰⁷. У липні 2019 року Федеральна комісія США з питань торгівлі досягла згоди з Facebook у питанні порушення приватності, відповідно до якої компанія мусить змінити свій підхід до питання приватності та погодитися на цілий ряд вимог та заходів контролю¹⁰⁸. Однак, як пояснюється у Розділі 4, ці зміни не торкаються самої бізнес-моделі компанії та не зменшують її шкоду для приватності людей в достатній мірі.

І Google, і Facebook вже понад десять років зазнають критики за свій підхід до питання приватності. У 2007 році перша спроба Facebook встановити нав'язливу рекламну функцію під назвою Beacon на своїй платформі зіткнулася з таким спротивом, що довелося її прибрати¹⁰⁹. Подібна негативна реакція спіткала і Google за рекламне таргетування відповідно до змісту електронних листів у Gmail, і в 2017 році компанія оголосила, що більше не буде сканувати листи¹¹⁰. Коли люди дізнаються про ту чи іншу форму стеження, вони зазвичай скаржаться, а компанії перепрошують за це — і все ж їхня бізнес-модель неухильно тяжіє до максимального стеження, як пояснюється вище.

Google і Facebook також відзначились у ситуаціях, коли вони вводили користувачів і користувачок в оману щодо приватності та рекламного таргетування. Ось кілька прикладів:

- Під час розробки Google Street View у 2010 році, фото-машини Google таємно зчитували приватні електронні листи та паролі з незахищених Wi-Fi-мереж¹¹¹;
- У 2018 році журналісти виявили, що Google не припиняє зберігати інформацію про координати, навіть якщо користувачі та користувачки відімкнули таку функцію. Після виходу публікації Google змінив опис цієї функції, але не відімкнув відстеження координат навіть після того, як користувачі та користувачки вимикали функцію

¹⁰⁶ Facebook, «Тепер ви бачите і контролюєте всі дані, якими додатки і сайти діляться з Facebook», 20 серпня 2019 р., <https://about.fb.com/news/2019/08/off-facebook-activity/>

¹⁰⁷ За висловлюванням Шошани Зубофф: «Як ми можемо очікувати, що компанії, економічне існування яких залежить від даних про поведінку, що вони добровільно припинять збирати дані? Це наче якби ми просили їх здійснити самогубство». Зубофф, «Таємниці капіталізму стеження», Frankfurter Allgemeine, березень 2016 р.; див. також, наприклад, Брюс Шнаер «Нова конституція приватності для Facebook», 8 березня 2019 р.; Кейсі Джонстон, «Facebook намагається нівелювати значення слова «приватність», The Outline, 1 травня 2019 р.; Джулія Керрі Вонг, «Моя безпека даних краща за вашу: генеральні директори IT-компаній підставляють одне одного, сперечаючись про приватність», 9 травня 2019 р.

¹⁰⁸ Facebook, Нова система захисту приватності, 24 липня 2019 р., <https://about.fb.com/news/2019/07/ftc-agreement/>

¹⁰⁹ The Register, «Facebook вимикає світло в Beacon», 23 вересня 2009 р.

¹¹⁰ Google, «З поширенням G Suite як корпоративного рішення, Gmail для користувачів та користувачки в Gmail в рамках G Suite для компаній стають тісніше пов'язані між собою», 23 червня 2017 р.

¹¹¹ Guardian (Велика Британія), «Google визнає, що збирав інформацію з Wi-Fi-мереж через машини Street View», 15 травня 2010 р., <https://www.theguardian.com/technology/2010/may/15/google-admits-storing-private-data>

«Історія місцезнаходження»¹¹². Зараз на Google очікує можливий судовий розгляд за позовом наглядового органу Австралії із забезпечення конкуренції¹¹³.

- На початку 2019 року журналісти виявили, що пристрої «розумний будинок» Google Nest мали вбудовані мікрофони, про які покупців не повідомляли¹¹⁴.
- Facebook визнав, що знав про порушення правил використання даних компанією політичного мікротаргетингу Cambridge Analytica за кілька місяців до того, як стався скандал (див. сіру рамку в Розділі 3)¹¹⁵.
- За допомогою додатку Facebook Research компанія раніше платила підліткам за те, щоб вони встановлювали додаток, який відстежує все, що вони роблять на телефоні¹¹⁶.
- Facebook також визнав, що проводив поведінкові експерименти над групами людей — наприклад, підштовхував певні групи виборців голосувати, або покращував (чи погіршував) настрої користувачів і користувачок, показуючи їм різні пости у стрічці новин¹¹⁷.

Доступ держав до сховищ даних Google і Facebook

«Пам'ятайте, що будь-які особисті дані, які зберігає Facebook чи Android, — це дані, до яких намагатимуться отримати доступ уряди з усього світу і які намагатимуться викрасти злодії».

Тім Бу, 2019¹¹⁸

Окрім прямих наслідків бізнес-моделі на основі стеження для прав людини, існує також ризик непрямих наслідків через зв'язок корпоративного стеження з державним. Органи державної влади, такі як розвідка, правоохоронні та імміграційні органи все більше намагаються отримати доступ до даних ІТ-компаній¹¹⁹. Сховища даних про людей, які

¹¹² Associated Press, «Google роз'яснює політику відстеження місця перебування», серпень 2018 р., <https://www.apnews.com/ef95c6a91eeb4d8e9dda9cad887bf211>

¹¹³ Австралійська комісія з конкуренції та прав споживачів, «За наявною інформацією, Google створив у користувачі та користувачки помилкове уявлення про збір і використання даних про місце перебування», 29 жовтня 2019 р., <https://www.accc.gov.au/media-release/google-allegedly-misled-consumers-on-collection-and-use-of-location-data>

¹¹⁴ The Verge, «Google стверджує, що вбудовані в Nest мікрофони «не мали бути таємницею», лютий 2019 р., <https://www.theverge.com/circuitbreaker/2019/2/20/18232960/google-nest-secure-microphone-google-assistant-built-in-security-privacy>

¹¹⁵ Guardian (Велика Британія), «Facebook визнає, що побоювання щодо Cambridge Analytica виникли ще до того, як про це повідомила преса», 22 березня 2019 р., <https://www.theguardian.com/uk-news/2019/mar/21/facebook-knew-of-cambridge-analytica-data-misuse-earlier-than-reported-court-filing>

¹¹⁶ Джош Констін, «Facebook визнає, що 18% користувачі та користувачки дослідницької шпигунської програми були підлітками, а не <5%, TechCrunch, 28 лютого 2019 р., <https://techcrunch.com/2019/02/28/facebook-research-teens/>

¹¹⁷ Christian Science Monitor, «Експеримент Facebook із кнопкою «Я проголосував/-ла»: похвальний крок чи пропаганда?», листопад 2014 р.; Guardian (UK), «Facebook розкриває експеримент зі стрічкою новин, покликаний контролювати емоції», червень 2014 р.

¹¹⁸ Тім Бу, автор «Торгівців увагою», «Як капіталізм зрадив приватність», New York Times, 10 квітня 2019 р., <https://www.nytimes.com/2019/04/10/opinion/sunday/privacy-capitalism.html>

¹¹⁹ Див. наприклад «CNBC, США, Велика Британія» підписують першу в історії угоду про доступ до даних ІТ-компаній, таких як Facebook і Google», жовтень 2019 р., <https://www.cnbc.com/2019/10/04/us-uk-sign-agreement-to-access-data-from-tech-companies-like-facebook.html>; Дженніфер Лінч, «Sensorvault від Google може

зібрали Google і Facebook, дали б органам державної влади чудову можливість доступу до надзвичайно цінних персональних даних, які було б дуже важко зібрати в інший спосіб.

Сама по собі бізнес-модель за своєю природою містить ризик, що Google і Facebook могли б стати учасниками нав'язливого, незаконного цифрового стеження з боку держави або таргетування людей таким чином, що це становить порушення їхніх прав. Хоча такий ризик наявний для будь-якої компанії, яка збирає значні обсяги персональних даних, бізнес-модель Google і Facebook мотивує ці компанії збирати й утримувати максимальні обсяги даних, щоб збільшити прибуток, що серйозно підвищує ризик.

Інформація про масове стеження, яку повідомив викривач, який раніше працював в Агентстві національної безпеки США, Едвард Сноуден, продемонструвала, як органам розвідки вдавалося отримати доступ до інформації IT-компаній. Документи про розвідку США, які оприлюднив Сноуден у 2013 році, розкрили, як розвідка США та Великої Британії проводить стеження за людьми на масовому рівні — і як компанії, зокрема Yahoo, Google і Microsoft, змушені були виконувати таємні накази і передавати дані про своїх користувачів і користувачок¹²⁰. Агентству національної безпеки також вдалося обійти захист Google і Yahoo та отримати доступ до центрів зберігання та обробки даних цих компаній¹²¹.

Після заяв Сноудена IT-компанії посилили використання шифрувальних технологій, щоб захистити дані користувачів і користувачок, і почали створювати юридичні перепони, щоб відмовляти урядам у вимогах надати дані, зокрема посилаючись на накази Уряду США про секретність, згідно з якими компанії не мають права відповідати на певні запити про інформацію¹²². І Google, і Facebook — члени Коаліції з реформування урядового стеження і виступають за реформу законів і практик, що врегулювали б урядове стеження¹²³. Це похвальні кроки, однак вони не допомагають вирішити проблему в корені, а саме — те, що бізнес-модель на основі стеження мотивує масштабний збір і обробку даних, які, в свою чергу, значно розширюють можливості державного стеження за населенням.

Права людини в Google і Facebook

Відповідно до міжнародних норм у сфері прав людини, Google і Facebook повинні проводити перевірку, щоб визначити потенційні та фактичні наслідки їхньої бізнес-моделі на конкретні права людини, включно з правом на приватність та свободою висловлювань,

повідомити поліцію, де ви були», квітень 2018 р., <https://www.eff.org/deeplinks/2019/04/googles-sensorvault-can-tellpolice-where-youve-been>

¹²⁰ Юен МакАскілл та Домінік Раш, «Документи Сноудена розкривають ключову роль компаній у зборі даних Агентства національної безпеки», Guardian (Велика Британія), листопад 2013 р. <https://www.theguardian.com/world/2013/nov/01/nsa-data-collection-tech-firms>

¹²¹ Бартон Геллман та Ашкан Сольтані, «Агентство національної безпеки має таємний зв'язок із центрами даних Yahoo і Google по всьому світу, за документами Сноудена», The Washington Post, жовтень 2013 р. https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centersworldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

¹²² Washington Post, «Google кидає виклик ордеру США про мовчання, посилаючись на Першу поправку», 18 червня 2013 р.

¹²³ Реформа урядового стеження, принципи, <https://www.reformgovernmentsurveillance.com/principles/>

та вживати заходів для покращення ситуації¹²⁴. Разом з тим, оскільки збір, аналіз та монетизація даних — настільки ключовий елемент їхньої бізнес-моделі, який має настільки серйозний та поширений вплив на право на приватність та настільки суперечить можливості користуватися цим правом, то IT-гіганти повинні також оцінювати, чи їхня бізнес-модель взагалі може поєднуватися з їхнім зобов'язанням поважати права людини.

Google і Facebook вже давно засвідчили свою повагу до права на приватність і свободу висловлювань, приєднавшись до Глобальної мережевої ініціативи (Global Network Initiative)¹²⁵. Однак масштаб ГМІ означає, що вона не розглядає загрози для інших прав, окрім права на приватність і на свободу висловлювань, а також насамперед зосереджується на тому, як компанії відповідають на запити урядів щодо даних.

Через участь у ГМІ обидві компанії мають кожні два роки проходити незалежну оцінку відповідних внутрішніх систем, політик і процедур. Останню таку оцінку було опубліковано в липні 2016 року, і в ній вказано, що обидві компанії відповідають Принципам ГМІ, які ґрунтуються на міжнародно визнаних законах і стандартах у сфері прав людини¹²⁶.

Amnesty International не може перевірити цю оцінку, оскільки процес оцінювання конфіденційний. Однак ГМІ заявляє, що процес такого оцінювання включає огляд систем, політик і процедур компанії, а також оцінку кількох конкретних прикладів, які узгоджує сама компанія¹²⁷. Увага до конкретних прикладів може вказувати на те, що процес не включає комплексної оцінки того, наскільки ефективно компанія впроваджує ці політики та процедури на практиці, зокрема виявляючи наслідки своєї діяльності для прав людини та усуваючи негативні наслідки. Процес також може не зважати на те, чи такі компанії, як Google і Facebook, проводять належну перевірку, щоб визначити та ліквідувати негативні наслідки самої своєї бізнес-моделі. Таким чином, ця оцінка, ймовірно, не включає ті аспекти, про які йдеться у цьому дослідженні, а саме — чи може бізнес-модель на основі стеження взагалі бути сумісною з дотриманням прав людини, враховуючи, що за своєю природою вона вже суперечить трьом ключовим елементам права на приватність¹²⁸.

Amnesty International запитала в Google і Facebook, чи враховує правозахисна перевірка компаній системні та поширені наслідки їхньої бізнес-моделі для прав людини, зокрема для

¹²⁴ Ranking Digital Rights проводить детальну оцінку компаній-лідерів у сфері інтернету, мобільних послуг і телекомунікації щодо виконання ними взятих на себе зобов'язань і політик, що впливають на свободу висловлювань і приватність інтернет-користувачів та користувачкив по всьому світу. Див. Індекс корпоративної підзвітності 2019 від Ranking Digital Rights, <https://rankingdigitalrights.org/index2019>. RDR зараз розширює методологію, щоб включити шкоду, пов'язану з політиками і практиками таргетованої реклами, а також використанням та розвитком алгоритмічних систем прийняття рішень

¹²⁵ Див. також принципи штучного інтелекту від Google <https://ai.google/principles> та декларацію про права людини <https://about.google/human-rights/>

¹²⁶ ГМІ, оцінки компаній 2015/2016, July 2016, <https://globalnetworkinitiative.org/2015-2016-company-assessments/>

¹²⁷ ГМІ, оцінки компаній, <https://globalnetworkinitiative.org/company-assessments/>

¹²⁸ У нинішньому процесі оцінки ГМІ ставить запитання, яку належну перевірку виконують компанії, щоб виявити потенційні загрози для права на свободу висловлювань і приватність, пов'язані з конкретними продуктами, ринками, придбаннями чи бізнес-зв'язками, але при цьому не оцінюється бізнес-модель компанії загалом. Див. ГМІ, оцінки компаній 2018/2019, Додаток I: запитання, що ставляться в процесі оцінки, <https://globalnetworkinitiative.org/wp-content/uploads/2019/03/GNI-2018-Appendix-I.pdf>

права на приватність, як згадується вище. На зустрічі з Amnesty International Google заявив, що проводить правозахисну перевірку свого бізнесу. Facebook надіслав детальний лист у відповідь (див. Додаток), але не відповів на це конкретне запитання.

3. Масштабна аналітика даних: додаткові ризики для прав людини

«Стеження — це просто процес спостереження, але що воно зробило з суспільством, правда?.. Що відбувається, коли немає закутків, де можна мати інакші погляди або так чи інакше експериментувати з самовираженням? На що це схоже? Це насправді лише форма контролю над суспільством... рух до конформізму... Саме слово «стеження» недостатньо агресивне, щоб це описати.

Джулія Ангвін, 2018¹²⁹

Платформи Google і Facebook функціонують на основі передових систем аналізу даних. Їхні алгоритми розроблені таким чином, щоб показувати користувачу «доречний» контент (а доречність ці компанії вираховують на основі зібраних даних) — як «органічні» пости, так і рекламні оголошення. Наприклад, алгоритми, за якими працюють Google-пошук та стрічка новин Facebook, постійно навчаються на великих обсягах даних користувачів і користувачок у різних цілях, зокрема щоб спрямовувати користувачу ту чи іншу рекламу, налаштовувати результати пошуку, рекомендувати новий контент і заохочувати користувачів і користувачок створювати новий контент та взаємодіяти з наявним. Для цього системи «оптимізують» результат, використовуючи складні, багаторазові алгоритмічні процеси, які виявляють кореляції та роблять логічні висновки на основі даних користувачів і користувачок¹³⁰.

Все частіше виявляється, що такі алгоритмічні системи, в свою чергу, можуть призвести до серйозних негативних наслідків для прав людини, зокрема приватності, свободи висловлювань, а також права на рівність та права не бути дискримінованим/-ою¹³¹. В деяких випадках такі наслідки викликає безпосередньо сама технологія компанії, в інших випадках, ці інструменти можуть використовувати інші гравці — таким чином, що це шкодить правам. Ці наслідки значно зростають та погіршуються через сам лише масштаб Google і Facebook та домінуючу позицію, яку ці платформи займають.

В результаті цього шкода, яка виникає через вплив бізнес-моделі на основі стеження на приватність, поширюється так, що наслідки передбачити неможливо. Наприклад, на рівні окремої людини, хтось може поділитися лише незначними, нібито невинними даними, наприклад, натиснути, що щось «подобається». Але коли такі дані збираються, їх можна

¹²⁹ Джулія Ангвін у розмові з Тревлором Паґленом, «Кінець довіри», випуск 54, McSweeney's Quarterly Concern and the Electronic Frontier Foundation, с. 55, <https://www.eff.org/document/end-trust-0>.

¹³⁰ «Системи оптимізації використовують логіку операційного контролю, що зосереджується на результаті, а не на процесі... ми називаємо системами оптимізації системи, які відстежують і маніпулюють поведінкою та середовищем користувачів та користувачки за логікою оптимізації». Ребека Овердорф, Богдан Кулинич, Еро Балса, Кармела Тронсозо, Седа Гюрзес, «Технології захисної оптимізації», серпень 2018 р., <https://arxiv.org/abs/1806.02711>.

¹³¹ Див. різні приклади, що наводяться у «Сценаріях загроз для прав людини: таргетована реклама» від Ranking Digital Rights, лютий 2019 р., <https://rankingdigitalrights.org/wp-content/uploads/2019/02/Human-Rights-Risk-Scenarios-targeted-advertising.pdf>; а також в публікації «Алгоритми, машинне навчання й автоматичне прийняття рішень», липень 2019 р., https://rankingdigitalrights.org/wp-content/uploads/2019/07/Human-Rights-RiskScenarios_-algorithms-machine-learning-automated-decision-making.pdf

використати, щоб показувати чітко таргетовану рекламу, політичні оголошення та пропаганду, або щоб заволодіти увагою людей і заохотити їх все більше користуватися платформою.

УВКПЛ заявило, що аналітична потужність технологій на основі даних створила середовище, яке «несе ризик для осіб та громад, який важко переоцінити»¹³².

Зростання персоналізації, профайлінгу та мікротаргетингу

Передові технології аналітики даних — основа бізнес-моделі Google і Facebook, і саме вони забезпечують економічну потужність цих компаній. У 2018 році Facebook заявив, що одна з технологій машинного навчання, на яких працює платформа, робить 200 трильйонів передбачень на день¹³³. Системи алгоритмів слугують на користь бізнес-моделі у два способи: по-перше, вони допомагають чітко таргетувати рекламу, а по-друге, вони максимально збільшують взаємодію користувачів і користувачок із платформою. Як пояснюється в наступних розділах, обидві цілі несуть в собі серйозні ризики для прав людини¹³⁴.

Збір даних дозволяє Facebook і Google показувати людям надзвичайно точно налаштовану рекламу на основі складної комбінації їхніх характеристик, зокрема координат, віку, гендеру, інтересів і поведінки. Як пояснюється в Розділі 1, ці характеристики логічно виводяться та передбачаються за допомогою складних алгоритмічних моделей компанії. Здатність Google і Facebook надавати рекламодавцям можливість робити дуже точні передбачення та «мікротаргетинг» на цільову аудиторію збільшує прибуток цих компаній від реклами.

Є величезна кількість компаній та інших гравців, які створюють складні екосистеми таргетованої реклами. Однак завдяки тому, що Google і Facebook мають самодостатнє поєднання величезних обсягів даних у сховищах, їхні платформи надзвичайно популярні, вони контролюють основні потоки даних і, відповідно, можуть розвивати найбільш новаторські інструменти машинного навчання та моделі передбачень, ці компанії займають цілком панівне положення на ринку цифрової реклами.

Водночас із використанням аналітики даних та реклами, Facebook і Google також використовують алгоритми, щоб персоналізувати платформу для кожного користувача та кожної користувачки, а отже, «збільшити взаємодію» зі своїми продуктами, утримуючи користувачів і користувачок на своїй платформі настільки довго, наскільки це можливо¹³⁵.

¹³² УВКПЛ, «Право на приватність у цифрову добу», 3 серпня 2018 р., А/НRC/39/29, пункт 16.

¹³³ Facebook, «Запуск PyTorch 1.0 for для досліджень і виробництва, травень 2018 р., <https://engineering.fb.com/ai-research/announcingpytorch-1-0-for-both-research-and-production>

¹³⁴ Ranking Digital Rights, ««Сценарії загроз для прав людини: таргетована реклама», лютий 2019 р., та «Алгоритми, машинне навчання й автоматичне прийняття рішень», липень 2019 р.

¹³⁵ Facebook заперечує, що алгоритм стрічки новин побудовано таким чином, щоб максимізувати взаємодію користувачі та користувачки із контентом, і що «Справжня мета стрічки новин Facebook — надати людям контент, який буде їм найбільш цікавим». Див. відповідь Facebook у Додатку.

Іншими словами, ці платформи розробляються так, щоб викликати залежність¹³⁶. Це тісно пов'язано з бізнес-моделлю та прибутком компаній, бо що більше часу користувач чи користувачка проводить на платформі, то більше людей побачать рекламні оголошення і перейдуть за посиланнями в них, що в свою чергу надасть Google чи Facebook ще більше даних. Така схема підтримує функціонування бізнес-моделі, забезпечуючи постійний доступ до даних людей та підтримуючи майже-монополію цих платформ.

Вплив на думки та переконання

Як пояснюється в Розділі 2, приватність тісно пов'язана з ідеєю автономності, здатності будувати свою ідентичність без непроханого спостереження чи необґрунтованого впливу.

Однак поєднання алгоритмізованого рекламного таргетингу та персоналізованого змісту пошуку чи стрічки новин означає, що платформи Google і Facebook відіграють величезну роль у формуванні онлайн-досвіду людей та вирішенні того, яку інформацію ми бачимо. Це може вплинути на наші думки та переконання, сформувати їх чи змінити, а це може вплинути на нашу здатність робити вільний вибір. Крім того, алгоритми розроблені так, щоб якнайкраще підштовхувати людей до певних результатів на основі унікальних особистих характеристик тієї чи іншої людини. Техносоціологиня Зейнеп Туфекші описала ці платформи як «архітектуру переконання», які можуть маніпулювати та впливати на мільярди людей¹³⁷. Подібним чином колишній стратег реклами Google Джеймс Вільямс назвав це «перетворенням переконання на бізнес» і заявив, що ці «привернення та використання уваги» відволікають нас настільки, що ми не можемо чітко думати та досягати власних цілей.

Така здатність означає, що існує велика загроза, що ІТ-гіганти можуть безпосередньо завдавати шкоди праву на свободу думки, свободу совісті та віросповідання, а також свободі переконань та висловлювань за рахунок використання алгоритмічних систем¹³⁸. До того ж, вони можуть стати співучасниками порушення цих прав з боку інших гравців, які можуть отримати доступ до їхніх алгоритмів чи скористатися ними.

Міжнародне право у сфері прав людини не дозволяє будь-яких обмежень свободи думки та совісті або свободи дотримуватися чи звертатися до будь-яких релігійних вірувань чи переконань. Ці права захищаються безумовно, як і право мати власні погляди без стороннього втручання¹³⁹. Комітет ООН з прав людини зробив висновок, що право на свободу переконань може забезпечуватися лише за умови відсутності неналежного впливу

¹³⁶ ABC News, уривок із книги Джарона Ланьє «Десять причин видалити свої профілі у соцмережах просто зараз», червень 2018 р., <https://abcnews.go.com/Technology/book-excerpt-jaron-laniers-ten-arguments-deleting-social/story?id=56009512>.

¹³⁷ Зейнеп Туфекші, «Ми будуюмо антиутопію просто для того, щоб люди клікали по рекламі», TEDGlobal, вересень 2017 р., https://www.ted.com/talks/zeynep_tufekci_we_re_building_a_dystopia_just_to_make_people_click_on_ads/transcript?language=en

¹³⁸ Права, гарантовані ЗДПЛ, статтями 18, 19, Міжнародним пактом про громадянські та політичні права, статтями 18 і 19

¹³⁹ Див. Рада ООН з прав людини, «Коментар загального порядку №22: право на свободу думки, совісті та релігії» (стаття 18), 30 липня 1993 р., CCPR/C/21/Rev/1/Add/4, пункт 3; і Комітет ООН з прав людини, «Коментар загального порядку №34, стаття 19: свобода думки і висловлювань», CCPR/C/GC/43, 12 вересня 2011 р., пункт 3.

при формуванні поглядів, ідеологій та переконань особи¹⁴⁰. Спеціальний доповідач ООН з просування та захисту права на свободу висловлювань підкреслив, що «перетин технологій та індивідуального підбору контенту піднімає цілком нові питання про види переконання чи впливу, які можуть вважатися втручанням у право формувати думку¹⁴¹», а також відзначив, що «компаніям слід принаймні забезпечувати користувачів і користувачок значущою інформацією про те, як вони розробляють та впроваджують критерії підбору та персоналізації контенту на своїх платформах, а також інформацією про політики та процеси визначення соціальних, культурних чи політичних упереджень при розробці відповідних систем штучного інтелекту»¹⁴². Комітет міністрів Ради Європи також застеріг, що «високоточні, підсвідомі та персоналізовані рівні алгоритмічного переконання можуть серйозно вплинути на когнітивну автономність окремих осіб та їхнє право формувати власну точку зору та приймати незалежні рішення»¹⁴³.

Є чимало прикладів на підтвердження того, як такі платформи можна використовувати, щоб з граничною точністю таргетувати рекламу та впливати на думки та переконання людей. Такий таргетинг стає можливим саме завдяки бізнес-моделі Google і Facebook, що ґрунтується на стеженні. Академічні дослідження показали, що штучний інтелект вже здатен з більшою точністю виявляти ознаки депресії за постами в Instagram, ніж це зробили б люди, аналізуючи ті самі пости¹⁴⁴. Facebook також повідомив рекламодавцям, що може визначити, коли підлітки почуваються «невпевненими», «нікчемними» чи їм треба «підвищити впевненість у собі»¹⁴⁵. У відповідь на звіт Facebook сказав, що не дозволяє таргетинг на основі емоційного стану людей¹⁴⁶, однак цей момент лише підкреслює великі можливості Facebook і те, як їх ними можна зловжити, щоб нав'язати щось людям, коли вони найбільш вразливі.

Ще один приклад — проект Google «Метод редирект» (метод перенаправлення), який використовує платформу компанії AdWords (зараз вона називається Google Ads), щоб зменшити рівень радикальності потенційних прихильників ісламістського тероризму¹⁴⁷. Один коментатор успішно скористався тим самим інструментом — який розміщено онлайн

¹⁴⁰ Йонг Джо-Канг проти Республіки Корея, комунікація Комітету ООН з прав людини №878/1999, 16 липня 2003 р. (CCPR/C/78/D/878/1999)

¹⁴¹ Девід Кей, Звіт Спеціального доповідача з просування та захисту прав на свободу думки і висловлювань перед Генеральною асамблеєю ООН, 29 серпня 2018 р., A/73/348, пункт 24. (Девід Кей, 2018)

¹⁴² Девід Кей, 2018, пункт 26. Як сказано вище, Facebook вжив заходів у цьому напрямку, зокрема запровадив інструменти, щоб надати користувачам «більше інформації про те, що вони бачать на Facebook, та більше контролю над цим». Див. відповідь Facebook в Додатку.

¹⁴³ Комітет Міністрів Ради Європи, Декларація про маніпулятивні здатності алгоритмічних процесів, лютий 2019 р., https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b

¹⁴⁴ Йоганнес С. Ейхстедт, Роберт Дж. Сміт, Райна М. Мерчант, Лайл Г. Унґар, Патік Кратчлі, Деніел Преюцюк-П'єтро, Девід А. Еш та Г. Ендрю Шварц, «Мова Facebook передбачає медичну депресію», жовтень 2018 р. <https://www.pnas.org/content/115/44/11203>.

¹⁴⁵ The Australian, «Facebook адресує рекламу «невпевненим в собі» дітям, травень 2017 р., <https://www.theaustralian.com.au/business/media/facebook-targetsinsecure-young-people-to-sell-ads/news-story/a89949ad016eee7d7a61c3c30c909fa6>.

¹⁴⁶ Facebook, «Коментарі про дослідження і таргетування реклами», квітень 2017 р., <https://newsroom.fb.com/news/h/comments-on-research-and-adtargeting/>

¹⁴⁷ «Метод редирект», <https://redirectmethod.org/>

у вільному доступі — щоб спонукати людей на межі самогубства подзвонити на лінію підтримки¹⁴⁸. З цього очевидно, що таку «соціальну інженерію» цілком можна використати, щоб вплинути на думки та переконання людей, і це можуть робити як самі ці компанії, так і інші гравці. Хоча в цих прикладах такий вплив використовувався з начебто позитивною метою, ці інструменти так само легко можна було б застосувати й у шкідливий для наших прав спосіб, особливо, якби вони використовувалися на масштабному рівні.

Масштабна прихована маніпуляція

Право на приватність є «невід’ємною умовою реалізації права на свободу висловлювань»¹⁴⁹, а отже, нищення «особистої сфери» через Google і Facebook прямо і непрямо впливає на розвиток вільного обміну думками.

Свобода висловлювань — це колективне право, яке дозволяє людям як соціальній групі шукати та отримувати інформацію та «озвучувати колективні погляди»¹⁵⁰. За самою своєю природою алгоритмічні системи впливають на людей як групу, а також на індивідуальному рівні¹⁵¹. Коли можливості впливу та переконання застосовуються в масштабах платформ, що контролюються Facebook і Google, ці компанії можуть впливати на погляди великих груп чи сегментів населення, а цим можуть скористатися інші гравці.

Бізнес-модель на основі стеження створила архітектуру, яка не лише радикально зменшила й обмежила «приватну сферу», але й водночас ізолювала людей одне від одного, оскільки кожна людина отримує свій цілком персоналізований досвід в інтернеті, якнайточніше підлаштований під цю людину за допомогою висновків та припущень про неї на основі алгоритмів¹⁵². Це уможливорює масштабні маніпуляції.

Найяскравіший приклад того, як здатність Google і Facebook таргетувати людей з високою точністю можна використати на шкоду, — це застосування цих інструментів у політичному контексті. Найбільш відомий такий випадок — скандал з компанією Cambridge Analytica (див. рамку нижче). Ті самі механізми й інструменти переконання, що застосовуються для реклами, можна використати для маніпуляції політичними поглядами людей¹⁵³.

Використання так званого мікротаргетингу для донесення політичних ідей може також

¹⁴⁸ Патрік Берлінкет, «Я використав рекламу Google для соціальної інженерії. В мене вийшло», липень 2019 р. <https://www.nytimes.com/2019/07/07/opinion/google-ads.html>

¹⁴⁹ Звіт Спеціального доповідача з просування та захисту права на свободу думки і висловлювань, Франка Ля Рю, 17 квітня 2013 р., A/HRC/23/40, пункт 24.

¹⁵⁰ Звіт Спеціального доповідача з просування та захисту права на свободу думки і висловлювань, Франка Ля Рю, 20 квітня 2010 р., A/HRC/14/23, пункт 29.

¹⁵¹ «Профіль не просто визначає характеристики окремих суб’єктів даних, вони конструюються за принципом контрастування з іншими суб’єктами даних у наборі». Ліліан Едвардз і Майкл Віл, «Раб алгоритму? Чому «право на пояснення» — не та форма поновлення прав, яка вам, ймовірно, потрібна, 16 Duke Law & Technology Review 18, 2017, с. 35, <https://ssrn.com/abstract=2972855> (Едвардз і Віл, 2017)

¹⁵² Наприклад, дослідження Web Foundation щодо підбору контенту в стрічці новин виявило, що «алгоритм розміщує кожного користувача в окрему, індивідуалізовану версію того, що має бути громадським місцем обміну інформацією». Див. Web Foundation, «Невидимий підбір контенту», 2018, с. 5 http://webfoundation.org/docs/2018/04/WF_InvisibleCurationContent_Screen_AW.pdf

¹⁵³ Tactical Tech дослідили та схематично зобразили інструменти й техніки індустрії політичних даних. Див. Tactical Tech, «Інструменти індустрії впливу», <https://ourdataourselves.tacticaltech.org/posts/influence-industry>

обмежити свободу висловлювань, «створюючи спеціально підібраний світогляд, недружній до плюралістичного політичного дискурсу»¹⁵⁴.

Використання мікротаргетингу для політичних кампаній є особливо проблемним через нестачу прозорості та нагляду за політичними повідомленнями та їхнім авторством. Це залишає політикам можливість використовувати «темну» політичну рекламу, при якій люди отримують ретельно відібрані повідомлення, які бачать лише вони, але при цьому не завжди зрозуміло, яка організація чи особа їх опублікувала, а також яку інформацію бачать й отримують інші люди.

Скандал із Cambridge Analytica

Cambridge Analytica була фірмою політичного аналізу даних, яка заявляла, що здатна впливати на цільову аудиторію, створюючи неповторно детальні особисті профілі та підганяючи політичну рекламу відповідно до цих профілів (ця техніка відома як психографічне таргетування)¹⁵⁵. Реклама ж самої Cambridge Analytica заявляла, що в компанії наявні профілі на майже 240 мільйонів американців та від 4 до 5 тисяч одиниць даних на кожного виборця¹⁵⁶.

У 2014 році Cambridge Analytica отримала доступ до даних Facebook-профілів за допомогою додатку під назвою thisisyourdigitallife (цетвоєцифровежиття), який розробив доктор Александер Коґан, професор психології Кембриджського університету. Коли користувачі та користувачки Facebook завантажували додаток, вони давали згоду на доступ додатку до своєї особистої інформації¹⁵⁷. Компанія доктора Коґана уклала з партнером компанії Cambridge Analytica угоду про збір інформації з Facebook¹⁵⁸.

Відповідно до тогочасної політики Facebook, додатки могли отримати доступ до інформації не лише про користувачів і користувачок, які напяму дали на це згоду, а й до персональних даних людей, які були «в друзях» у таких користувачів і користувачок¹⁵⁹. Відповідно, хоча поділитися інформацією з додатком Коґана погодились лише 270 000 користувачів і користувачок, Facebook пізніше підтвердив, що за допомогою додатку Cambridge Analytica було передано відомості про майже 87 мільйонів профілів на Facebook¹⁶⁰.

¹⁵⁴ Девід Кей, 2018, пункт 18

¹⁵⁵ Сью Гальперн, «Cambridge Analytica і небезпеки психографії», The New Yorker, <https://www.newyorker.com/news/news-desk/cambridge-analytica-and-the-perils-of-psychographics>

¹⁵⁶ BBC News, «Компанія-власниця Cambridge Analytica, SCL Elections, отримала штраф через дані», січень 2019 р.

¹⁵⁷ Facebook, «Призупинення доступу Cambridge Analytica та SCL Group до Facebook», березень 2018 р. <https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/>

¹⁵⁸ Керол Кедвалладр і Емма Ґрехем-Ґеррісон, «Викрито: Cambridge Analytica отримала 50 мільйонів профілів на Facebook внаслідок масштабного витоку даних», Guardian (Велика Британія), 17 березня 2018 р. <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-uselection>

¹⁵⁹ Комітет з цифрової політики, культури, медіа та спорту Палати громад Великої Британії, Проміжний звіт про дезінформацію та «фейкові новини», липень 2018 р., пункт 120

¹⁶⁰ Facebook, «Повідомлення про наші плани обмежити доступ до даних на Facebook», 4 квітня 2018 р., <https://newsroom.fb.com/news/2018/04/restricting-data-access/>

В кінці 2015 року газета «Guardian» повідомила, що Cambridge Analytica неправомірно використовувала персональні дані з Facebook для президентської кампанії кандидата Теда Круза¹⁶¹. У відповідь на це Facebook поставив вимогу, щоб Коган і Cambridge Analytica видалили ці дані¹⁶². Cambridge Analytica відповіли, що це буде зроблено, однак насправді у компанії залишався доступ до даних чи моделей, що ґрунтувалися на цих даних¹⁶³.

У 2016 році команда Дональда Трампа найняла Cambridge Analytica в рамках передвиборчої кампанії, і компанія використала ці психографічні профілі, щоб визначити цільову аудиторію цифрової реклами і змодельовати явку виборців. Аж у квітні 2018 року, після того, як газети «Observer» і «New York Times» опублікували матеріал про використання Cambridge Analytica даних з Facebook, Facebook почав зв'язуватися з 87 мільйонами користувачів і користувачок, які стали жертвами цього витоку даних¹⁶⁴.

Можна виділити три ключові аспекти скандалу, пов'язаного з Facebook. Перший — сумнозвісна слабка політика приватності даних, яка діяла у Facebook у той час, і завдяки якій Когану вдалося отримати доступ до особистої інформації не лише тих користувачів і користувачок соцмережі, які зайшли в додаток, а й усього кола спілкування кожного з них. Після цього Facebook довелося призупинити роботу тисяч додатків від близько 400 розробників, які могли отримати доступ до персональних даних користувачів і користувачок до 2014 року, коли компанія зменшила рівень доступу розробників¹⁶⁵. Відтоді Facebook ще більше обмежив обсяг даних, до яких можуть отримати доступ розробники додатків¹⁶⁶. По-друге, хоча Facebook і надіслав запит у Cambridge Analytica, щоб там видалили такі дані, в них не було змоги перевірити, чи Cambridge Analytica дійсно це зробила, що демонструє, наскільки складно втілювати на практиці навіть вже наявні політики. Третій аспект: навіть попри те, що Facebook було відомо про проблему принаймні з грудня 2015 року, компанія повідомила про це користувачів і користувачок, яких торкнувся витік даних, набагато пізніше — лише після того, як відбулося журналістське розслідування, що спричинило великий публічний скандал.

¹⁶¹ Гаррі Дейвіс, «Тед Круз використав фірму, що збрала дані про мільйони користувачів та користувачкив Facebook, які нічого не підозрювали», Guardian (Велика Британія), 11 грудня 2015 р., <https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data>

¹⁶² Facebook, Важкі запитання: повідомлення щодо Cambridge Analytica, 21 березня 2018 р., <https://newsroom.fb.com/news/2018/03/hard-questionscambridge-analytica>

¹⁶³ Пол Льюїс, Девід Пер і Алекс Герн, «Cambridge Analytica мала моделі даних Facebook протягом виборів у США», Guardian (Велика Британія), травень 2018 р., <https://www.theguardian.com/uk-news/2018/may/06/cambridge-analytica-kept-facebook-data-models-through-us-election>

¹⁶⁴ Метью Розенберг, Ніколас Конфессоре та Керол Кедвалладр, «Президентська кампанія Дональда Трампа 2016 року скористалася Cambridge Analytica», New York Times, 17 березня 2018 р.; Керол Кедвалладр і Емма Грехем-Гаррісон, «and Emma Graham-Harrison, Викрито: Cambridge Analytica отримала 50 мільйонів профілів на Facebook внаслідок масштабного витоку даних», Guardian (Велика Британія), 17 березня 2018 р.; CNBC, «Facebook тепер проінформує вас, якщо ваші дані було передано Cambridge Analytica», 9 квітня 2018 р.

¹⁶⁵ Facebook, «Нова інформація щодо нашого розслідування стосовно розробників додатків», 20 вересня 2019 р., <https://newsroom.fb.com/news/2019/09/an-updateon-our-app-developer-investigation/>. Згідно з відповіддю Facebook, надісланою до Amnesty та включеною в кінці звіту, «призупинення не обов'язково означає, що ці додатки становили загрозу для користувачів та користувачкив».

¹⁶⁶ Facebook, «Оновлення щодо API та важливі зміни», 25 квітня 2019 р., <https://developers.facebook.com/blog/post/2019/04/25/api-updates/>

Коли відгримів скандал, пов'язаний з Cambridge Analytica, Google і Facebook ввели більш сувору політику щодо політичної реклами¹⁶⁷, включно з заходами, спрямованими на чіткіше позначення того, хто платить за рекламу, та «бібліотеками реклами», що включали б політичну рекламу. Однак аналіз Privacy International показав, що цих заходів поки що було недостатньо, а ще вони неоднаково застосовуються в різних країнах, а отже, більшості користувачів і користувачок у світі «бракує значущої інформації про те, як рекламні оголошення спрямовуються через ці платформи»¹⁶⁸. Окремий аналіз, що провели дослідники Mozilla, також показав, що інструментів Facebook наразі не досить¹⁶⁹.

Сама залежність бізнес-моделі від побудови профілів та таргетування реклами означає, що цю здатність платформи і в майбутньому будуть використовувати треті особи, зокрема політичні гравці.

Максимальне збільшення взаємодії

Компанії зобов'язані поважати свободу висловлювань, і це включає висловлювання, які можуть вважатися образливими чи неприємними¹⁷⁰. Наприклад, Міжнародний пакт про громадянські та політичні права вимагає, щоб держави забороняли лише «будь-які висловлювання, що захищають національну, расову чи релігійну ненависть і є закликом до дискримінації, ворожості чи насильства». Інші форми висловлювання, навіть ті, що можуть когось шокувати чи образити, законом обмежувати не можна.

Однак використання алгоритмів для підбору контенту соцмереж та максимального утримування користувачів і користувачок на платформі може призвести до того, що Google і Facebook можуть активно пропагувати та підсилювати контент, що містить заклики до насильства, ненависть і дискримінацію. Ці платформи рекомендують та показують новий контент на основі непрозорих алгоритмічних процесів, щоб визначити, що змусить користувача найбільше взаємодіяти з контентом¹⁷¹. Оскільки люди більш схильні переходити за матеріалами, що мають сенсаційний характер або викликають емоційний

¹⁶⁷ Google, «Запроваджуємо новий звіт прозорості щодо політичної реклами», 15 серпня 2018 р., <https://www.blog.google/technology/ads/introducingnew-transparency-report-political-ads/>; Facebook, «Покращений спосіб дізнатися більше про рекламу на Facebook», 28 березня 2019 р., <https://newsroom.fb.com/news/2019/03/a-better-way-to-learn-about-ads/>

¹⁶⁸ Privacy International, «Соціальним мережам не вдається зробити рекламу прозорою для користувачів та користувачкив по всьому світу», 3 жовтня 2019 р., <https://privacyinternational.org/long-read/3244/social-media-companies-have-failed-provide-adequate-advertising-transparency-users>

¹⁶⁹ Mozilla, «API архіву реклами Facebook недостатньо», 29 квітня 2019 р., <https://blog.mozilla.org/blog/2019/04/29/facebook-ad-archive-api-is-inadequate/>

¹⁷⁰ Комітет ООН з прав людини, «Зауваження загального характеру №34, стаття 19: Свобода думки та висловлювань», CCPR/C/GC/43, 12 вересня 2011 р., пункт 11.

¹⁷¹ Див. наприклад, Алекс Мадригал, The Atlantic, «Як насправді працює алгоритм YouTube», листопад 2018 р., <https://www.theatlantic.com/technology/archive/2018/11/how-youtubes-algorithm-really-works/575212/>

резонанс, так звані «рекомендаційні системи» цих платформ можуть спрямувати користувача у так звану «кролячу нору» токсичного контенту¹⁷².

Колишня директорка Google з технологій Ніколь Вонг тепер визнає цю проблему, стверджуючи, що «Персоналізація, залученість... це те, що вас тут утримує, і зараз ми це чітко знаємо. Це надзвичайно обурює»¹⁷³. Марк Цукерберг визнає, що «згідно з нашими дослідженнями, де б ми не ставили межу дозволеного, що ближче цей контент до такої межі, то більше люди будуть із ним взаємодіяти в середньому — навіть якщо після цього вони повідомляють, що цей контент їм не подобається»¹⁷⁴.

Facebook стверджує, що «ми зосереджуємось на якості часу, проведеного на Facebook, а не на його кількості... Алгоритми Facebook надають перевагу постанам, які, за нашими передбаченнями, покладуть початок важливим розмовам»¹⁷⁵. Разом з тим, навіть представники самого Facebook визнають, що продукт викликає залежність не випадково. Наприклад, Роджер МакНемі, інвестор, що вклав гроші у Facebook ще на початку його існування та є радником Марка Цукерберга, цього року написав: «Бізнес-модель залежить від реклами, яка, у свою чергу, залежить від маніпулювання увагою користувачів і користувачок, щоб вони бачили більше рекламних постів. Один із найкращих способів захопити увагу — звернутися до обурення та страху, емоцій, які збільшують взаємодію з контентом»¹⁷⁶.

Спеціальний доповідач ООН з просування та захисту права на свободу висловлювань відзначив, що «вплив штучного інтелекту на пошукові механізми має величезні наслідки для поширення знань. Агрегатори контенту та новинні сайти... обирають, яку інформацію показувати, на основі не останніх чи важливих новин, а додатків зі штучним інтелектом, які передбачають інтереси користувачів і користувачок та новини, цікаві їм, на основі масштабних наборів даних. Як наслідок, штучний інтелект відіграє велику, але зазвичай приховану роль у формуванні споживання чи навіть намірів споживання інформації окремими особами»¹⁷⁷. Спеціальний доповідач також заявив, що «в системі, що працює на основі штучного інтелекту, поширення інформації та ідей регулюється непрозорими силами, пріоритети яких можуть суперечити принципам сприятливої обстановки для розмаїття медіа та незалежних голосів»¹⁷⁸.

¹⁷² Кевін Руз, «Як твориться YouTube-радикал», The New York Times, червень 2019 р.
<https://www.nytimes.com/interactive/2019/06/08/technology/youtube-radical.html>

¹⁷³ Recode Decode, «Всі запитання і відповіді: колишня юристка Google і заступниця директора США з технологій Ніколь Вонг», вересень 2018 р., <https://www.vox.com/2018/9/12/17848384/nicole-wong-cto-lawyer-google-twitter-kara-swisher-decode-podcast-full-transcript>

¹⁷⁴ Марк Цукерберг, «Схема управління контентом та забезпечення дотримання правил», листопад 2018 р., <https://www.facebook.com/notes/markzuckerberg/a-blueprint-for-content-governance-and-enforcement/10156443129621634/>

¹⁷⁵ Лист Facebook до Amnesty International – див. Додаток. Компанія також вказує на свої зусилля щодо зменшення «вірусності» мови ненависті та інші заходи з модерування контенту.

¹⁷⁶ Роджер МакНемі, «Я був ментором Марка Цукерберга. Я любив Facebook. Але я не можу мовчати про те, що відбувається», Time, 17 січня 2019 р., <https://time.com/5505441/mark-zuckerberg-mentor-facebook-downfall/>

¹⁷⁷ Девід Кей 2018, пункт 11.

¹⁷⁸ Девід Кей 2018, пункт 30.

Звісно, сенсаційність у мас-медіа — не нове явище, і воно не обмежується самим лише інтернетом. Але механізми рекомендацій контенту в соцмережах — дещо більше, ніж давно відома історія про те, що медіа-аудиторія реагує насамперед на негатив. Ці механізми можуть систематично надавати перевагу екстремальному контенту, такому, як теорії змови, мізогінія та расизм, щоб якнайдовше утримувати користувачів і користувачок у себе на платформі. Наприклад, одне академічне дослідження поширення негативного ставлення до біженців і біженок на Facebook виявило, що «злочини ненависті щодо біженців непропорційно зросли там, де люди більше користувалися Facebook у періоди інформаційних хвиль, негативно налаштованих до біженців»¹⁷⁹. Подібним чином, були також випадки, коли алгоритми платформи YouTube, що належить Google, призводили до різних негативних наслідків (див. рамку нижче).

Водночас із наданням переваги шкідливому контенту алгоритми цих платформ можуть також підривати свободу висловлювань чи вести до дискримінації, зменшуючи видимість певного контенту. Наприклад, ЛГБТІ-спільноти повідомляли, що алгоритм YouTube блокує чи зменшує видимість відео, зміст якого пов'язаний з ЛГБТІ, автоматично нав'язуючи вікові обмеження та «демонетизуючи» відео — це означає, що виробники такого контенту не можуть отримати прибуток від реклами¹⁸⁰. YouTube це заперечує, стверджуючи, що «компаніє не демонетизує ЛГБТІ-контент автоматично»¹⁸¹.

Практичний приклад: екосистема радикалізації на YouTube

Численні дослідження YouTube, які проводили науковиця Зейнеп Туфекші¹⁸², колишній інженер YouTube Ґійом Шасло¹⁸³, газета The New York Times¹⁸⁴ та інші, виявили підтвердження того, як алгоритм рекомендацій YouTube надає перевагу неправдивому й емоційно зарядженому контенту.

В теорії, образи та мова ненависті порушують політику YouTube. На практиці ж матеріали, які наближаються до цієї межі (або й перетинають її), ніхто не видаляє. Вони привертають багато уваги та приносять YouTube прибуток, оскільки завдяки їм користувачі та

¹⁷⁹ Карстен Мюллер і Карло Шварц, «Роздмухуючи полум'я ненависті: соцмережі та злочини на ґрунті ненависті», Варвickський університет, травень 2018 р., https://warwick.ac.uk/fac/soc/economics/research/centres/cage/manage/publications/373-2018_schwarz.pdf; Аманда Тауб і Макс Фішер, «Згідно з новим дослідженням, Facebook підлив олії у вогонь нападів на біженців у Німеччині», New York Times, 21 серпня 2018 р.

¹⁸⁰ Джулія Александер, «ЛГБТК-користувачі та користувачки YouTube подають в суд на YouTube за потенційну дискримінацію», The Verge, серпень 2019 р., <https://www.theverge.com/2019/8/14/20805283/lgbtq-youtuber-lawsuit-discrimination-alleged-video-recommendations-demonetization>

¹⁸¹ Там само

¹⁸² Зейнеп Туфекші, «YouTube, великий радикалізатор», The New York Times, березень 2018 р. <https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html>.

¹⁸³ Сайт Шасло, «Щоденні YouTube-рекомендації», намагається відстежувати рекомендації для понад тисячі каналів. Див. <https://algotransparency.org/>. Також див. «Як колишній інсайдер YouTube провів розслідування його секретного алгоритму», Guardian (Велика Британія), <https://www.theguardian.com/technology/2018/feb/02/youtube-algorithm-election-clinton-trump-guillaume-chaslot>.

¹⁸⁴ Макс Фішер і Аманда Тауб, «Як YouTube радикалізував Бразилію», New York Times, 11 серпня 2019 р., <https://www.nytimes.com/2019/08/11/world/americas/youtube-brazil.html>

користувачки довше залишаються на платформі, а отже, бачать більше реклами. Це, в свою чергу, приносить прибуток YouTube, оскільки компанія заробляє гроші на рекламодавцях залежно від того, скільки переглядів отримує рекламне оголошення. За словами самої компанії, 70% часу, проведеного користувачами та користувачками на платформі, генерує саме їхня система алгоритмізованих рекомендацій нового матеріалу¹⁸⁵.

Звіт дослідниці з аналітичного центру Data & Society Бекки Льюїс, що вийшов у 2018 році, описує, як механізм рекомендацій YouTube монетизує охоплення та «вплив» навіть тих авторів відео, які регулярно заявляють про свої шкідливі, зокрема расистські, погляди¹⁸⁶. У своєму дослідженні під назвою «Альтернативний вплив: транслюючи реакційне право на YouTube» Льюїс вимальовує схему праворадикальних «інфлюенсерів» у США, які використовують алгоритми YouTube, щоб отримувати вигоду від поширення дезінформації та мови ненависті. Вона показує, як поєднання алгоритму рекомендацій YouTube та соціальних практик праворадикальних користувачів і користувачок сервісу створює екосистему радикалізації, завдяки якій «користувачам і користувачкам надзвичайно легко натрапити на все більш екстремістський контент»¹⁸⁷. Особливу проблему, за її словами, це становить через те, наскільки популярним джерелом новин для молоді є YouTube¹⁸⁸. Її висновок: «Величезна мережа інфлюенсерів й інфлюенсерок на YouTube транслює реакційні ідеї молодим глядачам і глядачкам, а це робить їх більш радикальними»¹⁸⁹.

Цей алгоритм також живить неправдиву інформацію та чутки. Автоматично поєднуючи різні відео, які повторюють той самий неправдивий наратив, YouTube створює ілюзію, що та сама ідея повторюється в різних джерелах. Насправді ж цей нібито консенсус виникає винятково через алгоритм: за словами Дебори Дініз, активістки за права жінок, яка стала жертвою скоординованої онлайн-кампанії в Бразилії, «виникає відчуття, що глядач чи глядачка сам/-а виявляє зв'язок між різними відео, але насправді він виникає через систему»¹⁹⁰. Проблеми підтверджувального упередження й упередження популярності вже неодноразово фіксували в соцмережах¹⁹¹.

У відповідь на такі звіти YouTube оголосив — вже не вперше — зміни до алгоритмів рекомендації контенту на платформі, але станом на зараз ці зміни стосуються лише невеликого набору відео у США¹⁹². Компанію й досі жорстко критикують за те, що вона

¹⁸⁵ Там само

¹⁸⁶ Ребекка Льюїс, «Альтернативний вплив: транслюючи реакційне право на YouTube», Data & Society, вересень 2018 р., <https://datasociety.net/output/alternative-influence/>

¹⁸⁷ Там само

¹⁸⁸ Звіт посилається на дослідження дослідницького центру «П'ю», згідно з яким, понад 90% дорослих віком від 18 до 24 років користуються YouTube: http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/pi_2018-03-01_social-media_0-01/.

¹⁸⁹ Ребекка Льюїс, <https://twitter.com/beccalew/status/1042054175201185792>

¹⁹⁰ Макс Фішер і Аманда Тауб, «Як YouTube радикалізував Бразилію», New York Times, 11 серпня 2019 р.

¹⁹¹ Джованні Лука Чампалья, Філіппо Меншер, «Упередження роблять людей вразливими до дезінформації в соцмережах», The Conversation, 21 червня 2018 р., <https://www.scientificamerican.com/article/biases-make-people-vulnerable-to-misinformation-spread-by-socialmedia/>

¹⁹² YouTube, «Продовжуємо працювати над покращенням рекомендацій на YouTube», 25 січня 2019 р., <https://youtube.googleblog.com/2019/01/continuing-our-work-to-improve.html>

дозволяє монетизувати образливий контент¹⁹³. Однак генеральний директор YouTube заперечує припущення, «що ми неохоче вживаємо заходів щодо проблематичного контенту, бо він приносить прибуток нашому бізнесу»¹⁹⁴. Google заявив, що YouTube продовжує поліпшувати функцію рекомендацій¹⁹⁵.

Дискримінація

Іще одна серйозна загроза таргетованої реклами та профайлінгу (побудови профілів осіб на основі даних), які слугують підґрунтям бізнес-моделі Google і Facebook, — те, що показ відібраного контенту окремим людям чи групам людей може посилити дискримінацію з боку приватних компаній, або ж і з боку самих платформ, що порушує критичний принцип, що всі люди повинні мати рівний доступ до прав людини¹⁹⁶. Недискримінація, а також рівність перед законом, становлять базовий загальний принцип захисту прав людини¹⁹⁷.

Сама мета профайлінгу — розрізнати людей на основі їхніх особистих характеристик, переконань і поведінки. Вже були випадки, коли таргетинг з боку рекламодавців і політичних партій з використанням платформ Facebook і Google (тобто рішення про те, які групи включити, а які виключити) містив профайлінг людей за захищеними характеристиками — зокрема «люди до 18 років»¹⁹⁸, «належить до кількох культур»¹⁹⁹, «цікавиться державною зрадою»²⁰⁰, «цікавиться Йозефом Геббельсом»²⁰¹, «дохід нижче

¹⁹³ YouTube, «Суворіший погляд на образи онлайн», 5 червня 2019 р.

<https://youtube.googleblog.com/2019/06/taking-harder-look-atharassment.html>

¹⁹⁴ YouTube, Сьюзан Войчицьки: «Зберігаючи відкритість завдяки відповідальності», серпень 2019 р.,

<https://youtube-creators.googleblog.com/2019/08/preserving-openness-through-responsibility.html>

¹⁹⁵ YouTube, «Чотири аспекти відповідальності», частина 1: «Видалення шкідливого контенту», 3 вересня 2019 р.,

<https://youtube.googleblog.com/2019/09/the-four-rs-of-responsibility-remove.html>

¹⁹⁶ Кріс Гілланд, «Расизм без зусиль», журнал Real Life, 15 жовтня 2018 р., <https://reallifemag.com/friction-free-racism/>

¹⁹⁷ Комітет ООН з прав людини, Коментар загального характеру №18: недискримінація, 10 листопада 1989 р., пункт 1.

¹⁹⁸ Facebook, «Щодо таргетингу за віком», <https://www.facebook.com/help/103928676365132> («Мінімальний вік для реєстрації на Facebook — 13, тож вся реклама спрямовується людям, яким принаймні 13 років»)

¹⁹⁹ ProPublica, «Facebook обіцяє заборонити рекламодавцям таргетувати рекламу за расою чи етнічним походженням. Знову», липень 2018 р. <https://www.propublica.org/article/facebook-promises-to-bar-advertisers-from-targeting-ads-by-race-or-ethnicity-again>

²⁰⁰ Guardian (Велика Британія), «Facebook позначає російських користувачів та користувачки як таких, що «зацікавлені в державній зраді», липень 2018 р., <https://www.theguardian.com/technology/2018/jul/11/facebook-labels-russian-users-as-interested-in-treason>

²⁰¹ Los Angeles Times, «Facebook вирішив, які користувачі та користувачки цікавляться нацистами, — і дозволяє рекламодавцям напряму таргетувати рекламу на них», лютий 2019 р., <https://www.latimes.com/business/technology/la-fi-tn-facebook-nazi-metal-ads-20190221-story.html>

середнього»²⁰², «цікавиться центрами допомоги людям із залежністю»²⁰³, «цікавиться абортами»²⁰⁴, «цікавиться білим геноцидом»²⁰⁵ або «сексуальна орієнтація»²⁰⁶.

Окремі випадки таргетингу необов'язково означають порушення прав: коли рекламодавці спрямовують рекламу споживачам на основі їхніх інтересів, це не зачіпає ніяких прав і свобод. Однак коли це використовується у контекстах, що безпосередньо впливають на права людини, зокрема економічні, соціальні та культурні права, надточне таргетування, яке для рекламодавців уможливляють Google і Facebook, саме по собі несе високу загрозу дискримінації.

Дискримінація давно заборонена рекламною політикою Facebook²⁰⁷. Однак журналісти та журналістки-розслідувачі довели, що рік за роком Facebook дозволяв рекламодавцям (які рекламували житло, вакансії або, що викликає ще більше занепокоєння, публікували політичну рекламу) спрямовувати рекламу на певні групи людей, і водночас виключати певні групи на підставі захищених характеристик, таких як етнічне походження та вік²⁰⁸. У цьому році Facebook довелося серйозно обмежити таргетування для реклами житла, вакансій та кредитів у США внаслідок юридичної угоди з правозахисними групами²⁰⁹. Зокрема, рекламодавці більше не можуть адресувати людям рекламу на такі теми на підставі віку, гендеру, конкретного району проживання чи будь-яких інтересів, що описують захищені характеристики чи пов'язані з ними. Однак ці заходи стосуються лише рекламодавців зі США, або тих, які публікують рекламу для аудиторії у США, а це означає, що люди з інших країн все ще можуть зазнавати дискримінації в цих сферах.

Що важливо, окрім ризику бути дискримінованими третіми сторонами через використання можливостей таргетингу Google і Facebook, алгоритмічні системи, які визначають, як

²⁰² Google, «Щодо демографічного таргетування», <https://support.google.com/google-ads/answer/2580383>

²⁰³ У 2018 році Facebook почав давати дозвіл на рекламу центрів боротьби з залежністю лише для сертифікованих організацій — але лише у США. Див. Facebook, «Обмеження реклами для центрів боротьби з залежністю та заставних зобов'язань», 9 серпня 2018 р., <https://www.facebook.com/business/news/restricting-ads-for-addiction-treatment-centers-and-bail-bonds>

²⁰⁴ Рекламна політика Google, «Охорона здоров'я та медикаменти», <https://support.google.com/adspolicy/answer/176031> (this category is not available in a number of countries.)

²⁰⁵ The Intercept, «Facebook дозволив рекламодавцям таргетувати рекламу користувачам, зацікавленим у «Білому геноциді» — навіть після масового вбивства у Піттсбургу», <https://theintercept.com/2018/11/02/facebook-ads-white-supremacy-pittsburgh-shooting/>. Зараз ця категорія вже не активна.

²⁰⁶ Можливість таргетувати користувачі та користувачки за сексуальною орієнтацією на Facebook була доступна до лютого 2019 р. BuzzFeed, «Facebook заблокував таргетування користувачі та користувачки за сексуальною орієнтацією», 21 березня 2018 р. <https://www.buzzfeednews.com/article/alexkantowitz/facebook-has-blocked-adtargeting-by-sexual-orientation>.

²⁰⁷ Рекламна політика Facebook, «Заборонений контент: практики дискримінації», https://www.facebook.com/policies/ads/prohibited_content/discriminatory_practices

²⁰⁸ Джулія Ангвін та Террі Перріс-мол., «Facebook дозволяє рекламодавцям виключати групи користувачі та користувачки за расою», 28 жовтня 2016 р., <https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race>

²⁰⁹ Facebook, «Більше зусиль, щоб запобігти дискримінації у сфері реклами житла, вакансій та кредитів», 19 березня 2019 р., <https://newsroom.fb.com/news/2019/03/protecting-against-discrimination-in-ads>; ACLU, «Резюме угод між правозахисниками та Facebook», 19 березня 2019 р., <https://www.aclu.org/other/summary-settlements-between-civil-rights-advocates-and-facebook>

рекламні оголошення показуються на платформах і самі можуть призвести до дискримінаційних наслідків — навіть тоді, коли самі рекламодавці підходять до таргетингу цілком нейтрально²¹⁰. Це збільшує ризик, що ІТ-гіганти можуть безпосередньо викликати дискримінацію через те, як їхні алгоритмічні системи показують рекламу — на підставі «доречності» або більш «цінним» користувачам. У березні 2019 року Департамент США з житлової політики та міського розвитку подав позов до Facebook про дискримінацію у сфері забезпечення житлом, зокрема через власну систему показу реклами на Facebook, заявивши, що механізми Facebook «працюють так само, як рекламодавець, який навмисне таргетує чи виключає користувачів і користувачок на основі захищеної характеристики»²¹¹. Facebook заперечив це припущення, сказавши, що «у Департаменту немає доказів чи підтверджень того, що наші системи штучного інтелекту дискримінують людей»²¹². За наявною інформацією, Департамент з житлової політики та міського розвитку також розслідує рекламні практики Google і Twitter²¹³.

²¹⁰ Мухаммед Алі, Пйотр Сапежинські, Міранда Боґен, Александра Корольова, Алан Міслав, Арон Піке, «Дискримінація через оптимізацію: як показ реклами у Facebook може привести до викривлених результатів», квітень 2019 р., <https://arxiv.org/abs/1904.02095>; Університет Карнегі-Меллон, «Ставимо під питання справедливість таргетування онлайн-реклами», липень 2015 р., <https://www.cmu.edu/news/stories/archives/2015/july/online-adsresearch.html>

²¹¹ Департамент США з житлової політики та міського розвитку проти Facebook, позов про дискримінацію, 28 березня 2019 р., https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf

²¹² Заява Facebook у ProPublica, «Департамент США з житлової політики та міського розвитку подає в суд на Facebook за дискримінацію у сфері забезпечення житлом і стверджує, що алгоритми компанії погіршили проблему», березень 2019 р., <https://www.propublica.org/article/hud-sues-facebook-housing-discrimination-advertising-algorithms>

²¹³ Washington Post, «Департамент США з житлової політики та міського розвитку переглядає рекламні практики Twitter і Google в рамках розслідування щодо дискримінації у сфері забезпечення житлом», 28 березня 2019 р., <https://www.washingtonpost.com/business/2019/03/28/hud-charges-facebook-with-housing-discrimination/>

4. Концентрація влади — перешкода для підзвітності

«У світі програмного забезпечення, особливо у випадку платформ, це ринки, на яких переможець отримує все».

Білл Ґейтс, співзасновник Microsoft²¹⁴

За допомогою бізнес-моделі на основі стеження, за якою працюють Google і Facebook, цим компаніям вдалося встановити майже абсолютний контроль над основними каналами, які люди використовують для взаємодії з цифровим світом й онлайн-спільнотою. Таким чином влада цих компаній сягнула небачених досі пропорцій. Ще ніколи не було приватних гравців, які виступають посередниками та встановлюють пріоритети в передачі інформації понад двом мільярдам користувачів і користувачок у численних країнах.

У зосередженні влади в руках цих компаній є кілька аспектів. Пол Неміц, головний радник при Європейській комісії, стверджує, що унікальна концентрація влади в руках технічних гігантів включає чотири ключові елементи, які слід розглядати комплексно: фінансову владу, яка дозволяє їм впливати на політику та ринки; владу над інфраструктурою демократії та дискурсом; владу над особами, що ґрунтується на профайлінгу, і використання цих знань у власних інтересах компаній; а також лідерську позицію в інноваціях, пов'язаних зі штучним інтелектом²¹⁵.

Ця сконцентрована влада тісно пов'язана з наслідками бізнес-моделі Google і Facebook для прав людини. Знищення права на приватність онлайн відбулося насамперед через те, що критично важливі онлайн-сервіси опинилися під контролем компаній, які залежать від стеження. Разом з тим, компаніям вдалося встановити цю панівну позицію саме через те, що дохід від реклами був для них важливішим за приватність та інші права.

Ця ситуація не лише погіршила наслідки діяльності цих платформ для прав людини, а також створила ситуацію, в якій дуже важко притягнути ці компанії до відповідальності, а тим, чий права було порушено — знайти спосіб ефективно їх захистити.

Стеження як плата за доступ до інтернету

Доступ до інтернету вже давно визнають критичним фактором прав людини в цифрову епоху. У 2011 році Спеціальний доповідач ООН з питань свободи висловлювань визнав, що «унікальна, революційна природа інтернету не лише дає особам змогу користуватися правом на свободу думки та висловлювань, а й уможливорює користування цілою низкою інших прав і сприяє загальному поступу суспільства»²¹⁶. У 2016 році Рада ООН з прав людини

²¹⁴ The Verge, «Білл Ґейтс каже, що його «найбільша в житті помилка» — те, що Microsoft програв Android», червень 2019 р.

²¹⁵ Пол Неміц, Головний радник при Європейській комісії (від власного імені), «Конституційна демократія та технології в добу штучного інтелекту», жовтень 2018 р. В аналізі йдеться про владу Google, Facebook, Microsoft, Apple і Amazon.

²¹⁶ Франк Ла Рю, Спеціальний доповідач з просування та захисту права на свободу думки і висловлювань, звіт для Ради ООН з прав людини, 16 травня 2011 р., UN Doc A/HRC/17/27

наголосила на важливості «застосування комплексного правозахисного підходу в наданні та розширенні доступу до інтернету», вказавши, що потрібно докладати зусиль для відкритості, доступності та якості інтернету²¹⁷.

Роль Google і Facebook як «посередників» у взаємодії з цифровим світом (як пояснюється в Розділі 1) означає, що вони серйозно впливають на те, як люди користуються своїми правами людини онлайн. Більшість інтернет-користувачів і користувачок дійсно послуговуються саме сервісами цих двох компаній. Ці платформи стали невід'ємною частиною користування правами людини онлайн і щодня їхнє використання сприяє свободі висловлювань, праву на свободу мирних зібрань та об'єднань та іншим правам²¹⁸.

Разом з тим, домінуюча позиція платформ цих компаній означає, що інтернетом фактично неможливо користуватися, при цьому не «погоджуючись» на їхню бізнес-модель, що ґрунтується на стеженні. «Мережеві ефекти» (які описано нижче) ведуть до того, що люди не можуть просто так покинути соцмережі, де спілкуються всі їхні друзі та рідні. Люди, які зареєструвалися на платформах, коли вони значно більше поважали приватність (див. нижче) — або перш ніж їх придбали Google і Facebook — тепер стикаються з несправедливим вибором: залишити сервіс, від якого вони залежать, чи погодитися на стеження. У деяких країнах Facebook став синонімом інтернету, а смартфони в усьому світі переважно працюють на мобільній ОС Android, що належить Google. Навіть людям, які не користуються жодним із цих сервісів, дуже важко використовувати інтернет так, щоб їхні дані не отримали ці дві компанії²¹⁹.

Це створило парадоксальну ситуацію, в якій люди, які хочуть отримати доступ до інтернету та вільно користуватися своїми правами людини онлайн, часто змушені коритися системі, яка ґрунтується на втручанні у право на приватність у безпрецедентних масштабах, і яка має настільки ж масштабні наслідки для інших прав, зокрема права а свободу висловлювань та права не бути дискримінованим. Ця ситуація різко відрізняється від твердження Ради ООН з прав людини про важливість «правозахисного підходу в наданні та розширенні доступу до інтернету»²²⁰. У червні 2019 року група експертів ООН ще раз підтвердила, що «Цифровий простір не є нейтральним. На рівні його фізичної архітектури, регулювання й використання, різні групи в ньому функціонують на користь власним інтересам. Однак його розвиток має ґрунтуватися на принципах міжнародного права у сфері прав людини»²²¹.

²¹⁷ Рада ООН з прав людини, «Просування, захист і використання прав людини в інтернеті», червень 2016 р., UN Doc A/ HRC/32/L.20

²¹⁸ «У цифрову добу використання прав на мирне зібрання та об'єднання стало досить сильно залежним від приватних компаній, юридичні зобов'язання, політики, технічні стандарти, фінансові моделі й алгоритми яких можуть впливати на ці свободи». Клеман Ньялетсоссі Вуль, Спеціальний доповідач ООН про свободу мирних зібрань та об'єднань.

²¹⁹ Джулія Ангвін, «У пошуках приватності, безпеки та свободи у світі безжального стеження», 2014 р.; Кашмір Гілл, «Прощавай, Велика п'ятірка», Gizmodo, січень 2019 р.

²²⁰ Рада ООН з прав людини, «Просування, захист і використання прав людини в інтернеті», червень 2016 р., UN Doc A/ HRC/32/L.20

²²¹ УВКПЛ, «Експерти ООН наголошують на зв'язку між цифровим простором і правами людини на зустрічі в Тунісі», 13 червня 2019 р. www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24696

Зосередження влади погіршує наслідки

Все більша влада Google і Facebook як посередників при взаємодії людей з цифровим світом стала головною причиною знищення онлайн-приватності. Аналіз розвитку цих компаній неодноразово показував, що вони поступово збільшували обсяг і рівень стеження паралельно зі зростанням їхнього контролю над основними каналами доступу до інтернету та зниженням популярності будь-яких серйозних альтернатив²²².

На початку їхньої діяльності, коли Google і Facebook функціонували на висококонкурентних ринках, вони не ставили повсюдне стеження умовою використання їхніх послуг. Згідно з політикою Facebook, що діяла тоді, «ми не використовуємо і не будемо використовувати cookie-файли для збору приватної інформації про будь-якого користувача»²²³. В першій версії політики приватності Google зазначалося, що компанія передавала інформацію про користувачів і користувачок рекламодавцям, але «ми говоримо лише про наших користувачів і користувачок загалом, а не про окремих осіб» — що дуже відрізняється від нинішньої моделі, коли реклама стала надзвичайно персоналізованою і таргетованою²²⁴.

Перехід цих компаній від початкового етапу, коли вони більше дотримувалися приватності, до нинішньої бізнес-моделі, що ґрунтується на повсюдному стеженні, відбувався поступово. Google зробив останній крок до повного переходу на таку модель у 2016 році, коли він змінив свою політику приватності, уможлививши поєднання даних з рекламної мережі DoubleClick (пізніше перейменованої на Google Marketing Platform) з персональними даними, зібраними з інших платформ компанії²²⁵. Це означало, що тепер компанія могла напряму адресувати рекламу особам, яких можна було ідентифікувати на основі надзвичайно особистої інформації. Журналістка Джулія Ангвін, яка займається темою приватності даних, прокоментувала, що Google таким чином «тихо стер критичну межу приватності»²²⁶. Facebook приблизно те ж саме зробив у 2014 році, оголосивши, що буде використовувати дані веб-перегляду для таргетованої реклами²²⁷.

Компаніям вдалося зробити цей остаточний крок, бо вони вже зайняли панівну позицію на ринку. Початкова бізнес-модель цих компаній доводить, що на більш конкурентному ринку користувачі та користувачки б не мирилися з настільки сильним втручанням у їхню

²²² Див., наприклад, Зубофф, 2018; Діна Срінівасан «Боротьба з монополією Facebook: шлях монополіста до нав'язливого стеження попри те, що споживачі прагнуть приватності», 16 Berkeley Bus. L.J. 39, 2019 р.

²²³ Facebook, Політика приватності Facebook (2004), на яку посилаються доктор Ліза Ловдал Ґормсен і доктор Хосе Томас Янос у «Антиконкурентних нахилах Facebook у стратегіях», червень 2019 р. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3400204 (Gormsen and Llanos, 2019)

²²⁴ Google, Політика приватності, червень 1999 р., <https://policies.google.com/privacy/archive/19990609?hl=en&gl=ZZ>

²²⁵ Google, Політика приватності, червень 2016 р., <https://policies.google.com/privacy/archive/20160325-20160628?hl=en&gl=ZZ>

²²⁶ Джулія Ангвін, «Google тишком скасував заборону на відстеження в інтернеті з можливістю ідентифікації особи», ProPublica, 21 жовтня 2016 р., <https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking>

²²⁷ AdAge, «Facebook планує використовувати історію веб-переглядів для таргетування реклами», червень 2014 р., <https://adage.com/article/digital/facebook-web-browsing-history-ad-targeting/293656>

особисту сферу і перейшли б на інші сервіси. А тепер компанії можуть собі дозволити порушувати право на приватність, бо у людей немає іншого вибіру, окрім згоди²²⁸.

Порушення прав людини сприяють концентрації влади

Водночас бізнес-модель на основі стеження має вбудовану тенденцію збільшувати домінування та масштаб самих платформ, які працюють на її основі, а отже, порушення приватності та інших прав також допомогло зосередити владу в руках Google і Facebook. Отримання все більшого обсягу даних допомогло цим компаніям збільшити контроль над тим, як люди користуються інтернетом, контролю настільки потужного, що в умовах бізнес-моделі з більшим дотриманням приватності це не стало б можливим.

Перший аспект — це явище під назвою «мережевий ефект»: що більше користувачів і користувачок є в певній платформі, то більш цінною вона стає як для них самих, так і для інших. Онлайн-платформи та бізнес-модель, на якій вони працюють, за самою своєю природою дуже схильні до мережевих ефектів. Багато користувачів і користувачок почали користуватися Facebook, бо там були їхні друзі, рекламодавці перейшли на YouTube, бо там найбільша аудиторія. Виникає ефект снігової кулі, коли що більшою стає платформа, то більше люди від неї залежать і то міцніше вона може закріпити свою позицію — через що користувачам і користувачкам стає складніше покинути платформу, а конкурентам — запропонувати альтернативу.

Отримання й аналіз даних у цій бізнес-моделі також призводить до специфічних мережевих ефектів, що ґрунтуються на даних²²⁹. Накопичення великих обсягів даних дозволяє компанії краще тренувати моделі машинного навчання й алгоритми, які створюють поведінкові передбачення. У свою чергу, ці функції передбачення використовуються, щоб утримувати людей на платформі, що генерує ще більше даних та підтримує контроль над потоками даних. Кращі функції передбачення також збільшують дохід від реклами, підвищуючи вартість платформи та владу компанії на ринку.

Ця закільцьована система в поєднанні з традиційними мережевими ефектами стала невід'ємною частиною швидкого зростання масштабу та влади цих платформ, зробивши Google і Facebook беззаперечними лідерами в цифровому світі. За нинішнього швидкого переходу до «інтернету речей», аналітика даних і штучний інтелект стають центром економіки. Сховища даних Google і Facebook та їхній контроль над передовими технологіями штучного інтелекту та машинного навчання ще більше зміцнить їхнє домінування. Технології машинного навчання від Google і Facebook — TensorFlow і PyTorch

²²⁸ «Платформи онлайн-комунікації... можна порівняти з комунальними послугами, в тому сенсі, що споживачі відчують, що не можуть без них обійтися, тож вони мало що можуть зробити окрім того, щоб просто прийняти їхні умови. Надавачі цих послуг зараз мало вмотивовані щось робити з проблемами неналежного використання даних чи онлайн-загрозами, зокрема загрозами для суспільства», — комітет Палати лордів Великої Британії щодо комунікацій та регулювання в цифровому світі, березень 2019, пункт 45. Facebook не погодився з цим висновком, заявивши, що «ми знаємо, що якщо не будемо захищати дані людей, то втратимо їхню довіру». Див. відповідь Facebook на резюме звіту Amnesty International у Додатку.

²²⁹ Ґормсен і Янос, 2019

відповідно — вже стали основними інструментами, якими послуговуються розробники штучного інтелекту²³⁰.

Ці компанії також змогли використати переваги, які вони отримали за рахунок збору даних — зокрема фінансову вигоду — щоб активно перешкоджати розвитку альтернативних сервісів. Вони роблять це у кілька способів: «підв'язуючи» один сервіс до іншого, користуючись домінуванням в одній сфері, щоб підвищити домінування в іншій²³¹, знижуючи рейтинг сервісів від потенційних конкурентів на власних платформах (наприклад, у пошуковій видачі)²³² та придушуючи компанії, які пропонують схожі послуги чи такі, що можуть стати потенційними конкурентами — для цього вони їх або копіюють, або просто відразу ж купують компанію²³³. Ця схема настільки добре відома, що венчурні капіталісти в Кремнієвій долині називають це «вбивчою зоною» Google і Facebook²³⁴: йдеться про сферу економіки, в якій конкуренти не можуть закріпити хоч якусь позицію, і єдина життєздатна бізнес-модель для нової компанії на ринку — щоб її придбав Google або Facebook.

Влада перешкоджає корпоративній підзвітності

Дисбаланс між багаторівневою владою технічних гігантів, таких як Google і Facebook, що описується вище, та здатністю урядів ефективно їх контролювати — яскравий приклад «прогалин у врядуванні» між «масштабом та впливом економічних сил і гравців та здатністю суспільств впоратися з негативними наслідками». Такі прогалини Спеціальний представник ООН з бізнесу та прав людини Джон Раді назвав «глибинною причиною» викликів для прав людини, що постають внаслідок глобалізації²³⁵.

Внаслідок того, скільки детальних даних Google і Facebook вдалося зібрати за допомогою своїх платформ і сервісів, які пронизують майже всі аспекти сучасного життя, виникла величезна інформаційна асиметрія між компаніями з одного боку та урядами й інтернет-користувачами та користувачками з іншого. Шошана Зубофф стверджує, що «капітал приватного стеження закріпив асиметрію знання на безпрецедентному рівні. Вони знають все про нас, ми майже нічого не знаємо про них»²³⁶.

²³⁰ Джефф Гейл, «Яка технологія глибокого навчання розвивається найшвидше?», KDnuggets, квітень 2019 р., <https://www.kdnuggets.com/2019/05/which-deep-learning-framework-growing-fastest.html>

²³¹ Європейська комісія, «Боротьба з монополіями: Комісія накладає на Google штраф у розмірі 4,34 мільярди євро за нелегальні практики з мобільними телефонами Android, покликані посилити домінування пошукової системи Google», 18 липня 2018 р., http://europa.eu/rapid/press-release_IP-18-4581_en.htm

²³² Європейська комісія, «Боротьба з монополіями: Комісія накладає на Google штраф у розмірі 2,42 мільярди євро за використання домінуючої позиції пошукової системи для здобуття нелегальної переваги власним сервісом порівняльної купівлі», 27 червня 2017 р., http://europa.eu/rapid/press-release_IP-17-1784_en.htm. Див. також «Виступаючи проти Google», The New York Times, 20 лютого 2018 р., www.nytimes.com/2018/02/20/magazine/the-case-against-google.html

²³³ Див., наприклад: Wired, «Не можеш створити — купи: мапа найбільших придбань Google», вересень 2017 р.; Біллі Галлагер, «Імітатор: як Facebook намагався придушити Snapchat», Wired, лютий 2018 р.; New York Post, «Джерела повідомляють, що Facebook похвалився, що купив Instagram, щоб знищити конкуренцію», лютий 2019 р.

²³⁴ The Economist, «Американські технічні гіганти ускладнюють життя стартапам», 2 червня 2018 р.

²³⁵ Джон Раді, Спеціальний представник ООН з прав людини та транснаціональних корпорацій й інших приватних підприємств, звіт Раді ООН з прав людини, квітень 2008 р., A/HRC/8/5

²³⁶ https://www.democracynow.org/2019/3/1/age_of_surveillance_capitalism_we_thought

Швидкість, з якою платформи Google і Facebook так розрослися та їхня наявність у численних країнах означає, що державному регулюванню складно впоратися з наслідками діяльності цих компаній для прав людей²³⁷. Цю прогалину вже відкрито визнають керівні особи в Кремнієвій долині. Генеральний директор Microsoft Бред Сміт заявив: «Майже жодна технологія не залишалася настільки нерегульованою так довго, як цифрова технологія»²³⁸. Марк Цукерберг закликав до «більш активної ролі урядів та регуляторних органів», зокрема в контексті приватності даних²³⁹. У 2014 році колишній генеральний директор Google Ерік Шмідт і тодішній голова Google Ideas Джаред Коен заявили, що «онлайн-світ — це... найбільший нерегульований простір у світі»²⁴⁰. Сам Google говорить, що це «аксіоматично, що норми міжнародного права відстають від швидкості технологічного прогресу»²⁴¹.

Хоча органи влади, відповідальні за захист даних, конкуренцію та сплату податків, вжили немало заходів з регулювання великих технологічних компаній, поки що їм не вдалося усунути мотивацію до використання бізнес-моделі на основі стеження.

Із нещодавніх гучних прикладів, у червні 2019 року Федеральна комісія США з питань торгівлі виписала Facebook рекордний штраф у 5 мільярдів доларів США та поставила низку вимог до компанії внаслідок розслідування скандалу з Cambridge Analytica²⁴². Хоча цей штраф — найбільша в історії санкція проти приватної компанії, він все одно незначний порівняно з річним обігом та прибутком компанії — що можна побачити вже з того, що після оголошення штрафу вартість акцій Facebook зросла²⁴³. Що ще більш важливо, рішення Комісії не вирішило питання з самою моделлю повсюдного стеження, профайлінгу на основі поведінки та таргетингу. У заяві комісара Федеральної комісії Рохіта Чопри про незгоду з таким рішенням сказано: «Угода, якої було досягнуто, ніяк не змінює структуру компанії чи її фінансову мотивацію, які й призвели до цих порушень. Вона також не

²³⁷ Див., наприклад, Комітет Палати лордів Великої Британії щодо комунікацій та регулювання в цифровому світі, березень 2019 р.: «Регулювання цифрового світу не встигає за його роллю в нашому житті»; Deloitte Insights, «Майбутнє регулювання», червень 2018 р., <https://www2.deloitte.com/us/en/insights/industry/public-sector/future-of-regulation/regulating-emerging-technology.html>; Даніель Малан, «Закон не може встигнути за новими технологіями. Ось як їх наздогнати», Світовий економічний форум, червень 2018 р., <https://www.weforum.org/agenda/2018/06/law-too-slow-for-newtech-how-keep-up>

²³⁸ NPR, «Президент Microsoft: На карту поставлено демократію. Врегулюйте роботу технічних гігантів», вересень 2019 р.

²³⁹ Марк Цукерберг, «Інтернету потрібні нові правила. Почнімо у цих чотирьох сферах», Washington Post, березень 2019 р.

²⁴⁰ Шмідт і Коен, «Нова цифрова доба», 2014 р.

²⁴¹ Google, інформація до подання в Управління об'єднаного верховного комісара з прав людини щодо приватності у цифрову добу, 2018 р.

²⁴² Федеральна комісія США з питань торгівлі: «Комісія накладає штраф у 5 мільярдів та широкі обмеження щодо приватності на Facebook», 24 липня 2019 р., <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions>

²⁴³ MIT Technology Review, «Facebook коштує навіть дорожче після того, як з'явилися новини про штраф у 5 мільярдів від Федеральної комісії», 15 липня 2019 р.

запроваджує будь-яких обмежень масового стеження, до якого вдається компанія, чи її рекламних тактик»²⁴⁴.

Однак зворотна реакція наростає: і регуляторні органи, і законодавці в різних юрисдикціях все більше прагнуть виступити проти панівної позиції Google і Facebook, насамперед за допомогою законодавства про конкуренцію та захист даних.

Google і Facebook вже зіштовхнулися з навалюю скарг, поданих після запровадження ЗРЗД в Європейському Союзі. Комісія захисту даних в Ірландії — де розташовані центральні офіси обох компаній в Європі — проводить кілька паралельних розслідувань діяльності обох компаній, зокрема в контексті аналізу поведінки та таргетованої реклами²⁴⁵. У січні 2019 року наглядовий орган із захисту даних у Франції виписав рекордний штраф компанії Google розміром у 50 мільйонів євро за порушення, зокрема нестачу дійсної згоди на персоналізацію реклами²⁴⁶.

У США і Google, і Facebook — об'єкти численних антимонопольних розслідувань, зокрема їх проводять Департамент юстиції, Федеральна комісія з питань торгівлі, Юридичний підкомітет Палати представників Конгресу та дві окремі групи державних прокурорів²⁴⁷. У 2018 році, в Каліфорнії прийняли поки що найбільш прогресивний закон про приватність, Акт про приватність споживачів Каліфорнії, який надав мешканцям штату нові права на те, щоб знати, яку персональну інформацію збирають компанії та передають третім сторонам, і можливість відмовитися від продажу такої інформації²⁴⁸.

У вересні 2019 року комісарку ЄС з питань конкуренції Маргрете Вестагер повторно призначили на посаду. В неї є чималий досвід роботи з цифровою політикою та регулюванням²⁴⁹, що свідчить про намір врегулювати діяльність технічних гігантів, особливо після кількох серйозних антимонопольних рішень, які Комісія прийняла щодо компаній із Кремнієвої долини²⁵⁰. За межами США та Європи, Австралійська комісія з конкуренції опублікувала великий звіт про владу Google і Facebook, а державні органи з питань

²⁴⁴ Федеральна комісія США з питань торгівлі, Заява незгоди комісара Рохіта Чопри, щодо Facebook, Inc. Файл комісії №1823109, 24 липня 2019 р.

²⁴⁵ див. Щорічний звіт Комісії з захисту даних, 25 травня — 31 грудня 2018 р., «Розпочато розслідування щодо міжнародних IT-компаній», с. 50; «Комісія з захисту даних починає розслідування Google Ireland Limited, травень 2019 р., <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-opens-statutory-inquiry-google-ireland-limited>

²⁴⁶ Commission Nationale de l'Informatique et des Libertés (CNIL), «Обмежений комітет CNIL накладає фінансову санкцію в розмірі 50 мільйонів євро на GOOGLE LLC, 21 січня 2019 р. Google подав апеляцію.

²⁴⁷ Марсі Гордон і Метт О'Браєн, Associated Press, «З наближенням федерального розслідування окремі штати відкривають нові справи проти Facebook і Google», 6 вересня 2019 р. <https://www.apnews.com/5d4d10e28b4841c8a3a723095d4c0d16>

²⁴⁸ Акт про приватність споживачів Каліфорнії (CCPA), 2018, <https://oag.ca.gov/privacy/ccpa>

²⁴⁹ Wall Street Journal, «Комісарка ЄС, що боролася з технічними гігантами, обрана на другий термін», 10 вересня 2019 р.

²⁵⁰ Наприклад, Комісія оштрафувала Google на 4,34 мільярди євро за нелегальне використання мобільної ОС Android для «укріплення домінування власної пошукової системи», а на 1,49 мільярдів євро — за «неналежне використання лідерської позиції» в рекламі в онлайн-пошуку. Google подав апеляцію на обидва рішення.

конкуренції чотирьох із п'яти країн BRICS опублікували початковий звіт про цифрові ринки²⁵¹.

Історичне рішення, яке прийняв німецький орган з питань конкуренції щодо Facebook у лютому 2019 року, слугує прикладом того, як підхід, який поєднує захист даних і забезпечення конкуренції водночас, може дійсно похитнути глибинні причини бізнес-моделі на основі стеження. Правила, які забороняють Facebook зводити дані з різних платформ, наприклад, WhatsApp і Instagram, без згоди користувачів і користувачок, напрямку підважує здатність компанії користуватися своїм контролем над цими платформами²⁵² — однак дія рішення поки що призупинена регіональним судом, поки розглядається апеляція, подана Facebook²⁵³.

Ця тенденція вказує на те, що епоха саморегулювання технічних гігантів може добігати кінця, і дуже ймовірно, що завдяки поєднанню заходів на забезпечення виконання законодавства та прийняття нових законів урядовий нагляд за ІТ-компаніями посилиться. У цих зусиль є потенціал забезпечити, щоб Google і Facebook виконували своє зобов'язання дотримуватися прав людини. Але уряди повинні зробити все можливе, щоб майбутнє регулювання ІТ-індустрії відповідало зобов'язанням держав за міжнародним правом захищати осіб та громади від шкідливого впливу діяльності корпорацій, зокрема за рахунок «ефективних політик, законодавства, регулювання та вирішення в судовому порядку»²⁵⁴.

Корпоративне лобіювання

Один зі способів, якими Google і Facebook намагаються послабити регулювання, — використання своїх ресурсів для масштабного корпоративного лобіювання. Важливо відзначити, що ці компанії лобіюють широкий спектр питань, пов'язаних з бізнесом, і не всі кошти, які Google і Facebook витрачають на лобіювання, впливають на права людини. Разом з тим, ті великі суми, які ці компанії витрачають саме на це демонструють їхню владу та політичний вплив. Наприклад, Google витратив понад 8 мільйонів євро на лобіювання в ЄС у 2018 році, а Facebook — понад 3,5 мільйони євро²⁵⁵. Щоб було з чим порівняти — Google

²⁵¹ Комісія з конкуренції та прав споживачів Австралії «Щоб вжити заходів на подолання домінування цифрових платформ, потрібні комплексні, динамічні реформи», 26 липня 2019 р., <https://www.accc.gov.au/media-release/holistic-dynamic-reforms-needed-to-address-dominance-of-digital-platforms> ; Адміністративна рада економічного захисту Бразилії (CADE) «CADE опублікувала звіт про цифрову економіку», вересень 2019 р., http://www.cade.gov.br/cade_english/press-releases/cade-releases-report-on-digital-economy-during-the-vi-brics-competition-conference

²⁵² Федеративне бюро забезпечення конкуренції в Німеччині (Bundeskartellamt), «Bundeskartellamt забороняє Facebook поєднувати дані користувачів з різних джерел: додаткова інформація», 7 лютого 2019 р., https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook_FAQs.pdf

²⁵³ Герберт Сміт Фрігіллз, «Історичне рішення Федеративного бюро забезпечення конкуренції щодо Facebook призупинено через апеляційний розгляд», 27 серпня 2019 р., <https://hsfnotes.com/crt/2019/08/27/german-fcos-landmark-facebook-decision-suspended-on-appeal>

²⁵⁴ Керівні принципи ООН щодо бізнесу і прав людини, Керівний принцип 1

²⁵⁵ Див. Реєстр прозорості ЄС: профіль Google, <http://ec.europa.eu/transparencyregister/public/consultation/displaylobbyist.do?id=03181945560-59>; профіль Facebook, <http://ec.europa.eu/transparencyregister/public/consultation/displaylobbyist.do?id=28666427835-74>

того року витратив на лобіювання в ЄС більше грошей, ніж будь-яка інша компанія — наступними йдуть Microsoft, Shell і Facebook²⁵⁶. Google і Facebook лобіювали проти прийняття Загального регламенту захисту даних (ЗРЗД), який став обов'язковим до виконання в усіх країнах-членах ЄС у 2018 році²⁵⁷.

Ці компанії ще більше витрачають на лобіювання в уряді США. Центр гнучкої політики, позапартійна громадська організація, що відстежує витрати на лобіювання у США, заявляє про те, що Google витратив 21,2 мільйони доларів на лобіювання в уряді США у 2018 році (що майже на 17,6% більше за суму, витрачену в попередньому році)²⁵⁸. ІТ-компанії також фінансують чимало аналітичних центрів, щоб ті підтримували їхні аргументи²⁵⁹. ІТ-компанії лобіюють як для того, щоб уникнути потенційних антимонопольних заходів, так і для просування потенційного федерального законодавства, яке б нівелювало ефективні закони про приватність, що діють на рівні окремих штатів. Вони також боролися проти прийняття й цих ініціатив на рівні штату, в тому числі Акту про приватність споживачів Каліфорнії та Акту про приватність біометричної інформації штату Іллінойс²⁶⁰.

Крім того, це лобіювання не обмежується Європою і США. За інформацією газети «The Guardian», внаслідок витоку документів Facebook цього року стало відомо про «засекречену глобальну операцію з лобіювання, що спрямована на сотні законодавців і регуляторних органів, щоб збільшити вплив по всьому світу, зокрема у Великій Британії, у США, в Канаді, в Індії, у В'єтнамі, в Аргентині, у Бразилії, в Малайзії та в усіх 28 країнах ЄС^{261 262}.

²⁵⁶ Statista, «Компанії, що найбільше витрачають на лобіювання в ЄС», 29 квітня 2019 р.,

<https://www.msn.com/en-us/finance/news/the-companiesspending-the-most-on-eu-lobbying/ar-BBWoSWM>

²⁵⁷ Див., наприклад, Лора Каялі, «За лаштунками боротьби Facebook з європейським регулюванням», Politico, 23 січня 2019 р., <https://www.politico.eu/article/inside-story-facebook-fight-against-european-regulation/>

²⁵⁸ Див. Центр гнучкої політики, «Профілі компаній-лобістів»: Google, <https://www.opensecrets.org/lobby/firmsum.php?id=D000022008&year=2018>; Facebook,

<https://www.opensecrets.org/lobby/clientsum.php?id=D000033563&year=2018>

²⁵⁹ Лі Фенг, «Аналітичні центри з питань приватності, що фінансуються з Кремнієвої Долини, намагаються зруйнувати захист приватності споживачів на рівні штатів в окрузі Колумбія», The Intercept, 16 квітня 2019 р.: <https://theintercept.com/2019/04/16/consumer-privacy-laws-california/>

²⁶⁰ Див., наприклад, Канг і Вогель «ІТ-гіганти збирають армію з лобіювання», NYT та Фенг, «Аналітичні центри з питань приватності...», The Intercept, квітень 2019 р.

²⁶¹ Щодо Акту про приватність споживачів Каліфорнії, див. Лора Магоні та Деніел Столлер, «Google та інші ІТ-компанії прагнуть послабити історичний закон про приватність даних у Каліфорнії», Los Angeles Times, 4 вересня 2019 р., <https://www.latimes.com/business/story/2019-09-04/google-and-other-tech-companies-attempt-to-water-down-privacy-law>. Щодо Акту про приватність біометричної інформації штату Іллінойс, див., напр., Расселл Брандом, «Законодавці, яких підтримує Facebook, намагаються розправитись із законом про приватність», The Verge, 10 квітня 2018 р., <https://www.theverge.com/2018/4/10/17218756/facebook-biometric-privacy-lobbying-bipa-illinois>

²⁶² Керол Кедвалладр і Данкан Кемпбелл, «Викрито: Facebook займається лобіюванням проти законів про приватність даних по всьому світу», The Guardian, 2 березня 2019 р., <https://www.theguardian.com/technology/2019/mar/02/facebook-global-lobbying-campaign-against-data-privacy-laws-investment>

У відповідь на цей звіт Google вказав на наявність відкритого переліку третіх сторін, які компанія фінансує, та відкрити інформацію про лобювання, яке здійснює²⁶³. Facebook заявив, що дотримується усіх відповідних законів та інструкцій при здійсненні лобювання²⁶⁴.

Перешкоди для поновлення в порушених правах

Масштаб Google і Facebook також створює цілком нові перешкоди для осіб, яким потрібна можливість ефективно поновити свої права після того, як їхні права було серйозно порушено внаслідок бізнес-моделі, що ґрунтується на стеженні²⁶⁵. Частково ця ситуація виникає саме через ті виклики, які алгоритмічні системи створюють для доступу до поновлення прав.

Серйозну проблему становить те, що дотримання нинішніх норм захисту даних не забезпечується. Навіть у Європі з її порівняно сильним режимом захисту даних регуляторні органи не мають достатньо ресурсів чи експертизи, щоб належним чином розслідувати порушення та переслідувати порушників²⁶⁶. Крім того, приватні особи рідко відстоюють свої права через «недостатні знання про свої права, складні процедури, високу вартість судової тяганини та замалу фінансову вигоду при індивідуальному розгляді справи»²⁶⁷. Закони, що захищають дані, зміцніли по всьому світу, але належне забезпечення дотримання цих законів залишається непростим²⁶⁸.

Одна з п'яти базових форм поновлення людини в правах, що було порушено — відновлення прав, тобто повернення до тієї ситуації, яка існувала до того, як було вчинене порушення. Але в контексті корпоративного стеження та масового збору даних, таке відновлення може бути практично неможливим. УВКПЛ чітко заявляє, що «Наслідки порушення приватності важко скасувати... Те, наскільки легко зберігати, передавати, використовувати з іншою

²⁶³ Google, «Наші принципи та стандарти ведення бізнесу», <https://www.google.com/publicpolicy/transparency/>, і «Профспілки та членські групи», https://services.google.com/fh/files/misc/trade_association_and_third_party_groups.pdf

²⁶⁴ Див. відповідь Facebook у Додатку нижче.

²⁶⁵ Право на ефективне поновлення прав було визнано в рамках різноманітних міжнародних і регіональних договорів й інструментів про права людини, а також визнається правилом традиційного міжнародного права. Див., напр., Статтю 8 Загальної декларації прав людини, Статтю 2 (3) Міжнародного пакту про громадянські та політичні права, Статтю 2 Міжнародного пакту про економічні, соціальні та культурні права.

²⁶⁶ Див., напр., Reuters, «Європейські регулятори: ми не готові до нового закону про приватність», травень 2018 р., <https://uk.reuters.com/article/us-europe-privacy-analysis/european-regulators-were-not-ready-for-new-privacy-law-idUKKBN1I915X>; Агентство ЄС з фундаментальних прав, «Доступ до засобів відновлення права на захист даних у країнах-членах ЄС», 2013 р., с. 46, https://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies_en.pdf

²⁶⁷ Нойб, «Втілюючи приватність у життя», 2017, с. 8, https://noyb.eu/wp-content/uploads/2017/11/concept_noyb_public.pdf

²⁶⁸ Consumers International, «Стан правил із захисту даних у різних країнах світу», травень 2018 р., с. 5, <https://www.consumersinternational.org/media/155133/gdpr-briefing.pdf>; Privacy International, «Ключі до захисту даних», серпень 2018 р., с. 7, <https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf>

метою та зводити дані та профілі, впливає на постійність цифрових даних, що означає, що особа може зіткнутися з новими та тривалими ризиками для її прав у майбутньому»²⁶⁹.

Доступ до інформації про те, як діяльність компанії впливає на права людей, конче необхідний, щоб люди могли заявляти про поновлення своїх прав у випадку їхнього порушення з боку корпорацій²⁷⁰. Однак інформаційна асиметрія між Google і Facebook з одного боку і користувачами та користувачками інтернету — з іншого, а також непрозорість процедур збору, обробки та передачі даних, означає, що приватні особи часто навіть не можуть дізнатися, чи було порушено їхні права, і якщо так, то як²⁷¹. Прикладом слугують дані Facebook, якими скористалася Cambridge Analytica: академік Девід Керролл протягом двох років намагався отримати свої дані від цієї компанії, але йому це не вдалося. Якби журналісти-розслідувачі не викрили цю проблему, Керролл навіть не знав би, що його дані було використано неналежним чином²⁷².

Спеціальний доповідач ООН з питань свободи висловлювань вказав, наскільки системи штучного інтелекту загалом часто впливають на право осіб ефективно поновлювати свої права²⁷³. Інформування осіб ускладнене, оскільки вони «не усвідомлюють масштабу, охоплення чи навіть існування алгоритмічних систем, які впливають на їхні права». Ця відсутність прозорості ще більше ускладнюється через те, що алгоритми компаній постійно адаптуються та змінюються, і навіть розробники таких систем не завжди можуть пояснити, як вони досягли того чи іншого результату²⁷⁴.

І нарешті, через природу алгоритмічних наслідків у масштабах систем Google і Facebook, яка сама по собі є колективною, намагатися досягти поновлення у правах на індивідуальному рівні складно. Системи поновлення в правах зазвичай не розраховані на ситуації настільки великого, обширного масштабу²⁷⁵. Як наголошують експерти з цифрових прав та технологій Ліліан Едвардз і Майкл Віл, «способи поновлення у правах у сфері захисту даних за задумом ґрунтуються на індивідуальних правах... в той час як шкода від використання алгоритмів зазвичай виникає через те, як системи класифікують чи стигматизують групи людей»²⁷⁶.

²⁶⁹ УВКПЛ, «Право на приватність у цифрову добу», А/НRC/39/29, 2018, пункт 56

²⁷⁰ Amnesty International, «ТОВ Несправедливість: корпоративні порушники прав людини і поновлення прав», 2014, с. 157

²⁷¹ «Проект з прав людини, великих даних і технологій», Університет Есекса, подання УВКПЛ щодо права на приватність у цифрову добу, 2018, с. 8

²⁷² Wired, «Невідступна боротьба однієї людини, щоб отримати свої дані від Cambridge Analytica», січень 2019 р., <https://www.wired.com/story/one-mans-obsessive-fight-to-reclaim-his-cambridge-analytica-data/>

²⁷³ Девід Кей, 2018, пункт 40

²⁷⁴ AI Now Institute, Щорічний звіт, 2017, с. 30 https://ainowinstitute.org/AI_Now_2017_Report.pdf

²⁷⁵ Berkman Klein Center for Internet & Society, «Штучний інтелект і права людини: можливості та ризики», с. 55, https://cyber.harvard.edu/sites/default/files/2018-09/2018-09_AIHumanRightsSmall.pdf

²⁷⁶ Едвардз і Віл, 2017, с. 22

Висновки та рекомендації

Поширення бізнес-моделі на основі стеження призвело до ситуації, коли дві компанії — Google і Facebook — контролюють архітектуру стеження в небачених досі масштабах. Ця система охоплює цілі континенти та впливає принаймні на третину населення світу. В нинішній формі бізнес-модель на основі стеження несумісна з правом на приватність та становить серйозну загрозу цілому спектру прав людини.

На практиці ж, питання, розглянуті в цьому звіті, стосуються не лише Google і Facebook. Бізнес-модель на основі стеження слугує не лише інтересам цих компаній-лідерів ринку. Вона слугує підґрунтям роботи численних компаній: рекламодавців, брокерів даних, стартапів та нетехнічних компаній, які хочуть розвинути чи змінити свій бізнес таким чином, щоб заробити на персональних даних. Модель, яку випробували Google і Facebook, стала взірцем для інтернету, і вона проникає в наші домівки, офіси та на вулиці за допомогою «інтернету речей».

І все ж, що б не казали звичайним користувачам, інтернет не мусить залежати від стеження. Серйозні порушення приватності, свободи висловлювань та інших прав людини не є невід'ємною частиною технологій, за якими працює інтернет, а лише тієї бізнес-моделі, що зайняла панівну позицію на ринку. Google і Facebook обрали таку бізнес-модель саме через те, що це був найшвидший спосіб розвитку компаній. Тепер стало очевидним, що їхній вибір має серйозні наслідки для прав людини.

Через масштаб та складність загроз для прав людини, що пов'язані з бізнесом на основі стеження, рішення повинні бути структурними та філігранно поєднаними. Щоб знайти їх, потрібні будуть подальші розслідування, аналіз та міждисциплінарні міркування найрізноманітніших сторін — технологів, академіків, громадянського суспільства, політичних експертів та розробників політик. Вже існує чималий корпус академічних досліджень та активна міждисциплінарна спільнота, що працює над цими питаннями.

Загрози такої бізнес-моделі для приватності фіксуються вже давно. Двадцять років тому, коли лише закладалися підвалини цієї системи, захисники приватності попереджали про ризики індивідуалізованої побудови онлайн-профілів та потребу в юридичних запобіжниках. У 2000 році директор Центру інформації про електронну приватність Марк Ротенбург сказав Сенату США: «Ми попереджали [рік тому], що саморегулюванню не вдасться захистити приватність і що громадськість негативно поставиться до плану компанії формувати профілі інтернет-користувачів і користувачок»²⁷⁷.

Однак зараз з'явилася серйозна можливість нарешті впоратись із проблемою. Враховуючи негативне ставлення громадськості до влади ІТ-гігантів у місцях, де ці компанії займають найбільшу частину ринку, очевидно, що жорсткіше урядове регулювання не за горами. Ризик полягає в тому, що будь-яке регулювання інтернету повинно впроваджуватись надзвичайно обережно, щоб не зашкодити свободі висловлювань та іншим правам.

²⁷⁷ Марк Ротенбург, «Про інтернет-приватність і профайлінг», Свідчення перед Комітетом з торгівлі Сенату США, червень 2000 р., <https://epic.org/privacy/internet/senate-testimony.html>. Згадується компанія рекламних технологій DoubleClick, яку пізніше придбав Google.

Важливо, щоб новий регуляторний режим, в якій би формі він не був, ґрунтувався на дотриманні прав людини і був спрямований на боротьбу з наслідками, які бізнес-модель, що ґрунтується на стеженні, неодмінно спричиняє для прав людини. У короткостроковій перспективі потрібно терміново забезпечити виконання нинішньої регуляторної політики, враховуючи поширені й системні порушення законів про захист даних.

Міжнародні права та стандарти у сфері прав людини вже чітко вказують на обов'язок держав та відповідальність приватних компаній вживати негайних, ефективних заходів для захисту та дотримання (те чи інше, залежно від ситуації) права на приватність. У 2016 році Рада ООН з прав людини розробила набір кроків, які повинні зробити уряди для зміцнення та захисту прав людини та невід'ємних свобод онлайн. Зокрема, йшлося про те, що держави повинні «прийняти, впровадити та, де необхідно, реформувати закони, регуляторні акти, політики та інші заходи, що стосуються персональних даних та захисту приватності онлайн»²⁷⁸.

Жоден підхід не спрацює сам по собі. Недостатньо просто встановити більш жорсткі обмеження відстеження та використання персональних даних, якщо не буде заходів, спрямованих на вирішення ситуації з концентрацією даних — і влади — в руках Google і Facebook. Водночас ті численні політики, представники регуляторних органів і публічні інтелектуали, які пропонують «роздробити» технічних гігантів, насправді не розв'яжуть проблеми систематичних порушень прав людини, якщо не підтримуватимуть також заходи, які системно підходять до зміни самої бізнес-моделі, що ґрунтується на стеженні.

Цей звіт — спроба подивитися на цю проблему з правозахисної перспективи та вказати на потенційні рішення.

Рекомендації для держав

- Уряди мають вжити заходів, щоб доступ і використання необхідних цифрових послуг й інфраструктури — зокрема тих, які надають Google і Facebook — не залежали від повсюдного стеження. Для цього потрібно буде впровадити і/або забезпечити виконання законодавства, яке гарантуватиме людям право відмовитися від стеження з боку рекламодавців та інших третіх сторін.
- Перш за все потрібно не допускати, щоб компанії робили доступ до своїх послуг залежним від того, щоб люди «погоджувалися» на збір, обробку чи передачу своїх персональних даних з метою маркетингу чи реклами.
- Урядам слід впровадити та забезпечити виконання сильних законів про захист даних, що ґрунтувалися б на дотриманні прав людини та відповідали б добре відомим принципам захисту даних. Ці закони повинні обмежувати кількість та обсяг персональних даних, які можна збирати, суворо обмежувати мету, з якою компанії можуть обробляти такі дані, і забезпечувати захист висновків та припущень про осіб, які робляться на основі збору та обробки персональних даних. Також вони повинні

²⁷⁸ Рада ООН з прав людини, «Просування, захист і використання прав людини в інтернеті», червень 2016 р., UN Doc A/ HRC/32/L.20

вимагати, щоб компанії відразу ж чітко повідомляли користувачам і користувачкам про мету збору персональних даних, і щоб вони не обробляли ці дані таким чином чи з такою метою, які були б несумісні з дотриманням прав людини.

- Уряди також повинні забезпечити, щоб у дійсно незалежних національних інституцій із захисту даних було достатньо ресурсів й експертизи, щоб глибоко розслідувати порушення з боку Google, Facebook та інших великих ІТ-компаній та застосовувати санкції за такі порушення. Також вони повинні забезпечити ефективні механізми компенсації на індивідуальному та колективному рівнях.
- Порадившись із незалежними технічними експертами та з групами, яких це безпосередньо стосується, уряди мають впровадити регулювання, яке б передбачило нагляд за розробкою та впровадженням алгоритмічних систем, щоб забезпечити юридичну відповідальність компаній за ризики для прав людини, що пов'язані з такими системами, включно з негативними наслідками, що виникають через оптимізаційні рішення таких систем. Особливо це важливо для систем такого масштабу і з таким рівнем впливу, як у платформ Google і Facebook.
- Уряди повинні юридично зобов'язати ІТ-компанії проводити правозахисну перевірку, щоб визначити наслідки для прав людини від їхньої діяльності та вжити заходів на стримування таких наслідків, зокрема ризиків та порушень, пов'язаних із їхніми алгоритмічними системами чи таких, що впливають із самої бізнес-моделі.
- Уряди повинні прийняти державну політику у сфері інтернету, яка була б спрямована на забезпечення загального доступу та дотримання прав людини. До неї також належать заходи, які змінили б ринок та нівелювали мотивацію використовувати бізнес-моделі, що ґрунтуються на стеженні.
- Уряди повинні впровадити чи забезпечити дотримання нормативних стандартів, щоб переконатися, що люди можуть на практиці обирати більш приватні альтернативи бізнес-моделей на основі стеження. Сюди також належать заходи для забезпечення здатності сервісів до взаємодії, а не просто перенесення даних, щоб люди могли вільно переходити від одного сервісу до іншого без наслідків для кола спілкування.
- Уряди повинні гарантувати доступ до ефективних заходів на виправлення наслідків від порушень прав людини, пов'язаних з функціонуванням ІТ-компаній, де б не виникали такі наслідки, включно з наслідками, що виникають через функціонування дочірніх компаній, як національних, так і іноземних.
- Уряди повинні заохочувати, поширювати та вкладати кошти у впровадження ефективних програм цифрової освіти, які б допомогли розуміти свої права, включно з правом ефективно захищатися від будь-яких порушень у сфері захисту даних, приватності та інших прав людини при доступі до цифрових сервісів.

Рекомендації для компаній

- Google, Facebook та інші ІТ-компанії, діяльність яких залежить від нав'язливого корпоративного стеження з метою отримання даних, повинні знайти спосіб перейти до бізнес-моделі, яка б не порушувала прав людини. Перш за все, ці компанії повинні переконатися, що їхні політики та процедури правозахисної перевірки проводяться таким чином, щоб включити системні та масштабні наслідки їхніх бізнес-моделей для

прав людини, особливо права на приватність, та прозоро комунікувати, як вони визначили ці наслідки, а також будь-які конкретні ризики, і що вони зробили для виправлення ситуації.

- ІТ-компанії повинні утриматися від лобіювання послаблення стандартів захисту даних та законодавства про приватність, коли таке послаблення збільшує ризик порушення прав людини. Поважаючи права людини, ці компанії зобов'язані не заважати державам виконувати свої правозахисні зобов'язання.
- ІТ-компанії повинні вжити заходів, щоб виправити будь-які порушення прав людини, до яких вони призвели чи учасниками яких стали внаслідок своєї діяльності.

Додаток: Лист від Facebook

Шановні Таня і Джо,

Дякуємо за можливість відповісти на коротке резюме вашого майбутнього звіту про права людини та бізнес-модель Facebook. Ми цінуємо можливість співпраці з Amnesty International з цих важливих питань, однак, при всій повазі, не можемо погодитися з вашим висновком, що наші практики несумісні з принципами прав людини.

Як і багато інших онлайн-компаній, Facebook існує за рахунок продажу реклами. Це дає змогу мільярдам людей у всьому світі підтримувати зв'язок і самовиражатися, як ніколи раніше. Сама Amnesty International користувалася з цієї можливості: організація використовувала Facebook-рекламу та інші продукти Facebook, щоб донести інформацію до прихильників, зібрати кошти та працювати над втіленням своєї місії.

Саме наша бізнес-модель дозволяє нам надавати важливу послугу, яка дозволяє людям користуватися своїм фундаментальним правом — мати голос (свободу висловлювань) та мати змогу встановлювати зв'язок одне з одним (свобода об'єднань і зібрань). Саме тому нас розчарувало, що внесок, який Facebook зробив у розвиток прав людини (і правозахисних організацій) не згадується у «короткому резюме», яким ви з нами поділилися. Є численні приклади того, як люди використовували Facebook саме для просування прав людини по всьому світу. Як компанія, ми поважаємо права людини, включно з правом на приватність. Ми давно включені до Глобальної мережевої ініціативи (ГМІ), і ця участь, а також дотримання нами стандартів врядування, приватності та свободи висловлювань, які викладено в Принципах та Посібнику впровадження ГМІ, демонструють цю повагу. Як ви знаєте, ці стандарти ґрунтуються на Керівних принципах ООН щодо бізнесу і прав людини, Загальній декларації прав людини та Міжнародному пакті про громадянські та політичні права. Ми проходимо незалежну оцінку того, як ми дотримуємося своїх зобов'язань як члени ГМІ кожні два роки.

Для Facebook зараз важливий момент в контексті прав людини. Ми нещодавно поінформували свій персонал та керівництво про проблеми з правами людини та видали нову версію Цінностей стандартів спільноти, яка прямо посилається на принципи прав людини. Ми залучені в численні масштабні оцінки впливу на права людини, а також збираємося запустити один з найцікавіших експериментів, пов'язаних з правами, в цьому десятиріччі — Наглядову раду Facebook. Враховуючи нещодавно висловлену нашим керівництвом заяву про дотримання принципу свободи висловлювань та значні нові ініціативи для правозахисників, можете не сумніватися, що ми ще чимало всього зробимо для прав людини.

Зараз для нашої компанії також важливий момент у контексті приватності. Наш надійний процес перевірки, в який залучена група експертів з усієї компанії, які перевіряють нові продукти та зміни в приватності наявних продуктів, стане ще сильнішим в рамках впровадження угоди, якої ми досягли з Федеральною комісією з питань торгівлі. Ця угода

вимагає безпрецедентного рівня підзвітності та запроваджує жорсткіші стандарти контролю, ніж для будь-якої іншої компанії в нашій галузі.

Ми цінуємо можливість відповісти на резюме, яке ви надіслали, але глибоко стурбовані тим, що воно містить низку неточностей і помилкових припущень, найсерйозніші з яких ми викладемо тут:

1. **Бізнес-модель Facebook і «стеження».** Опис бізнес-моделі Facebook — яка включає продаж реклами, щоб безкоштовно надавати послуги, — як «стеження» нівелює ключову різницю між послугами, на які люди добровільно підписуються, та урядовим стеженням, яке і являє собою втілення безпідставного втручання в особисте чи сімейне життя, недоторканність житла і таємницю кореспонденції, про яке йдеться у Статті 17 Міжнародного пакту про громадянські та політичні права.
2. **Збір даних.** Ми не збираємо «максимально можливий обсяг даних про людей» і не робимо припущень про сексуальну ідентичність, риси характеру чи сексуальну орієнтацію особи. Насправді ми вимагаємо від людей лише надати інформацію про їхнє ім'я, вік, гендер та контактну інформацію, коли вони реєструються на Facebook. У нас немає доступу до змісту електронних листів користувачів і користувачок.
3. **Не-користувачі та користувачки.** Як і інші компанії, які забезпечують технологіями інші сайти та додатки, ми можемо отримувати інформацію про людей, які не є користувачами та користувачками Facebook, коли вони використовують такі сайти та додатки. Так працює інтернет. Ми не використовуємо інформацію про тих, хто не є нашими користувачами та користувачками, щоб створювати профілі людей.
4. **Наскрізний доступ.** Частина нашого бачення забезпечення можливості надсилати повідомлення з одного додатку в інший — наскрізне шифрування. Це означає, що ми збираємо менше даних про людей, а не більше, як стверджується в резюме.
5. **Соціальні плагіни.** Ми не зберігаємо даних з соціальних плагінів (таких, як кнопка «Подобається») в формі, яка дозволяє визначити користувача, якщо це не є необхідним для безпеки чи запобігання шахрайству.
6. **Free Basics.** Метою проекту Free Basics було не «отримати доступ до нових джерел даних». Free Basics не зберігає інформації про те, що роблять люди, або про контент, який вони переглядають в будь-якому сторонньому сервісі, який надається через Free Basics.
7. **Участь користувачів і користувачок.** Наша стрічка новин не розробляється таким чином, щоб «максимізувати участь користувачів і користувачок». Мета стрічки новин — показувати людям контент, який вони вважають найцікавішим і найбільш доречним. Ми зосереджуємось на якості часу, проведеного на Facebook, а не на його кількості.
8. **Дискримінація і прозорість.** У резюме не згадуються ті численні зміни, які ми запровадили в нашій рекламній системі, щоб запобігати дискримінації — зміни, які ще не запровадила жодна інша компанія. Facebook — далеко не єдине місце, де рекламодавці публікують рекламні оголошення про житло, роботу та кредити, і ми внесли радикальні зміни в те, як така реклама демонструється на нашій платформі. Багато із сегментів за інтересами, які згадуються в резюме, також вже було видалено.

Прозорість — важлива частина нашої роботи над цим питанням, і ми полегшили доступ до всієї реклами, що опублікована на Facebook, незалежно від того, чи ця реклама демонструється вам безпосередньо.

9. Розробники додатків. Резюме також не згадує роботу, яку ми провели, щоб обмежити неправомірне використання інформації про людей, яке трапилося в ситуації з Cambridge Analytica. Припущення, висловлене в резюме, що ми нещодавно призупинили співпрацю з 10 000 розробників через те, що підозрювали неправомірне використання даних, не відповідає дійсності.
10. Робота з правоохоронними органами. Замість того, щоб «робити внесок» у нелегальне стеження з боку уряду, ми активно йому протидіємо, ретельно вивчаючи кожен запит на інформацію, який ми отримуємо, щоб переконатися, що він відповідає нашим правилам, відповідному законодавству та міжнародним стандартам у сфері прав людини.

Ви можете відзначити, що наші процедури виходять далеко за межі мінімальних стандартів, викладених в останньому посібнику ООН з цього питання, «Право на приватність у цифрову добу». Ми сподіваємося, що ця інформація, а також додатковий контекст, наведений нижче, допоможуть вам переглянути свої аргументи щодо стеження, приватності та пропорційності при подальшій роботі над звітом.

Ми цілком свідомі того, що Facebook в минулому помилявся, але готові регулярно покращувати свої послуги і враховувати відгуки людей, які ними користуються. Ми з радістю продовжимо спілкування з вами щодо цього звіту та важливих питань, які в ньому піднімаються.

З повагою,

Стів Саттерфілд

Директор з приватності та публічної політики

Бізнес-модель Facebook та практика поводження з даними

Ваше резюме характеризує бізнес-модель Facebook як таку, що «ґрунтується на стеженні». Ми категорично не згодні з таким описом.

По-перше, важливо зауважити, що ніхто не зобов'язаний реєструватися в Facebook. Рішення користуватися нашими додатками абсолютно добровільне та особисте. Вибір людини використовувати Facebook і те, як ми збираємо, отримуємо чи використовуємо інформацію, — про що ми відкрито повідомляємо користувачів і користувачок — ніяк не може порівнюватися до примусового (і часто незаконного) стеження та прослуховування з боку

уряду, які й становлять безпідставне втручання в особисте чи сімейне життя, недоторканність житла і таємницю кореспонденції, про яке йдеться у статті 17 Міжнародного пакту про громадянські та політичні права.

По-друге, на відміну від того, що висловлено у вашому резюме, бізнес-модель Facebook не працює на основі збору даних про людей. Як і багато інших інтернет-компаній, Facebook працює за рахунок продажу реклами. Як ви справедливо зазначаєте, ми не продаємо дані, ми продаємо рекламу. Це дозволяє нам пропонувати сервіс, який дає змогу всім користуватися фундаментальними правами людини — мати голос (свобода висловлювань) і підтримувати зв'язок (свобода об'єднань та зібрань).

Хоча використання даних, які ми збираємо й отримуємо, — важлива частина показу ефективної реклами, припущення, що наша бізнес-модель полягає у прагненні збирати «якомога більше інформації про людей», є невірним. Збір даних не є кінцевою метою для Facebook — це спосіб, у який ми надаємо доречні та корисні послуги людям й організаціям. Єдині дані, які люди повинні надати, реєструючись на Facebook — ім'я, вік, гендер та контактна інформація. Ми також даємо людям змогу виражати інші гендерні ідентичності, окрім «чоловік» і «жінка».

З часом, коли люди користуються нашими продуктами, ми можемо отримувати додаткові дані (наприклад, сторінки, які вподобала людина, на які пости та на яку рекламу вона реагує), і ці дані допомагають нам надавати користувачам і користувачкам контент та послуги, які для них цікавіші, наприклад, визначати, які пости та рекламні оголошення відображаються вище у стрічці новин.

Вид даних, які ми збираємо й отримуємо від людей, відображено в резюме помилково. Ми не читаємо зміст електронних листів людей, а також не робимо здогадок про сексуальну ідентичність, риси характеру чи сексуальну орієнтацію людей. Ми також не використовуємо для таргетування реклами зміст повідомлень людей.

По-третє, критично важливо згадати про цілий спектр засобів контролю над даними, які ми збираємо, які ми надаємо людям. Ми даємо їм потужні важелі, за допомогою яких вони можуть вирішити, що їм підходить. Тому ми й пропонуємо такі інструменти як «Перегляд інформації про вас», «Рекламні вподобання» та «Чому я бачу цю рекламу?», над вдосконаленням яких ми постійно працюємо. Ми також нещодавно почали запуск нового способу, яким користувачі та користувачки можуть контролювати свої дії за межами Facebook та від'єднати цю інформацію від їхніх облікових записів. Ці інструменти забезпечують безпрецедентний рівень прозорості та контролю і значно перевищують мінімальні вимоги, визначені в абзаці 30 останнього документу ООН на цю тему, «Право на приватність у цифрову добу». Наше регулярне впровадження подібних інструментів захисту приватності спростовує думку, висловлену в резюме, що «Facebook може дозволити собі порушувати приватність». Навпаки, ми знаємо, що якщо не будемо захищати дані людей, то втратимо їхню довіру.

Як сказано вище, дані дозволяють нам показувати людям кориснішу рекламу. Це не лише створює кращий досвід для самих користувачів і користувачок; це також конче важливо для

мільйонів малих компаній, у яких є доступ до тих самих потужних інструментів, що й у великих компаній, що дозволяє їм донести інформацію про себе до людей, які з більшою ймовірністю зацікавлені в їхніх продуктах, послугах чи проблемах, якими вони займаються. Ефективність, яку дані привносять у рекламу, допомагає компаніям та іншим організаціям по всьому світу рости та піднімати важливі питання, включно зі свободою об'єднань і зібрань, правом на свободу висловлювань та політичної участі та, звісно, правом на розвиток.

Думка, висловлена в резюме, що наше прагнення зробити наші сервіси повністю сумісними дозволить нам збирати більше даних про людей, абсолютно не відповідає дійсності. Як пояснив наш генеральний директор Марк Цукерберг, наше бачення майбутнього функціонування наших сервісів включає наскрізне шифрування — що означає, що ми отримуватимемо менше даних про людей, а не більше. Наскрізне шифрування означає, що у нас не буде змоги отримати доступ до змісту повідомлень людей з рекламною метою — чи з будь-якої іншої причини.

Варто також зазначити, що Facebook вже не зберігає дані з соціальних плагінів (таких, як кнопка «Подобається») з ідентифікаторами користувача чи пристрою, окрім як для безпеки та захисту від шахрайства. Ті обмежені дані, які ми зберігаємо для розслідувань, пов'язаних із безпекою і шахрайством, зберігаються в окремих таблицях, доступ до яких контролюється, щоб ми були впевнені, що лише працівники, що працюють над питаннями безпеки, можуть отримати доступ до такої інформації. Як тільки розслідування завершується, ми видаляємо дані, окрім випадків, коли ми визначили, що відбулося порушення, і потрібно вжити подальших заходів для захисту наших продуктів і користувачів і користувачок.

Хоча ми дійсно можемо отримувати інформацію про людей без облікових записів Facebook, коли вони використовують сайт чи додаток із соціальним плагіном (чи іншою технологією Facebook), ми не створюємо профілі людей, які не є нашими користувачами та користувачками.

Характеристика нашого сервісу Free Basics у звіті не цілком відповідає дійсності. Декларація про приватність Free Basics чітко пояснює, що цей сервіс не є «вправою зі збору даних». Навпаки, Free Basics захищає приватність людей завдяки сильним запобіжникам, наявним у сервісі. Що найважливіше, Free Basics не зберігає інформацію про те, що люди роблять чи який контент переглядають у будь-якому сторонньому сервісі. Натомість, щоб надавати доступ до цих сервісів без стягнення плати за мобільні дані, Free Basics тимчасово зберігає лише доменні імена чи назви сторонніх сервісів, які було відвідано, після чого інформація зводиться чи інакшим чином позбавляється ідентифікаторів. Free Basics залишається важливим інструментом надання більшій кількості людей доступу до інтернету та дає можливість бути на зв'язку людям по всьому світу.

Покращення взаємодії людей зі стрічкою новин

Резюме від Amnesty припускає, що наші алгоритми розроблені таким чином, щоб просувати сенсаційний контент, бо люди з більшою ймовірністю з ним взаємодіють, що не відповідає

дійсності. Справжня мета стрічки новин Facebook — надати людям контент, який буде їм найбільш цікавим. Ми зосереджуємося на якості часу, проведеного на Facebook, а не на його кількості. Оскільки розмір стрічки новин користувача обмежений, алгоритми Facebook надають перевагу постам, які, за нашими передбаченнями, покладуть початок важливим розмовам — зокрема постам від близьких друзів, членів родини, а також сторінок, з якими користувачі та користувачки часто взаємодіють. Такий контент має перевагу над публічним, таким як пости від компаній, брендів і медіа.

Ми також вжили заходів для обмеження поширення контенту, який було створено для того, щоб зібрати якомога більше реакцій на Facebook, але який при цьому призводить до негативних чи шкідливих наслідків для користувачів і користувачок. Наприклад, ми запровадили системи, які визначають і зменшують поширення такого контенту, як так звані «приманки взаємодії», неправдива інформація, фейкові новини та клікбейт. Ми також наполегливо — і успішно — працювали над зменшенням вірусного поширення мови ненависті та іншого ворожого контенту в багатьох країнах, де існує ризик насильства.

Крім того, ми віримо в те, щоб користувачі та користувачки мали якомога більше інформації про те, що вони бачать у Facebook, і якомога більше контролю над цим, зокрема у стрічці новин. У березні 2019 р. ми оголосили нову ініціативу з підвищення прозорості «Чому я бачу цей пост», яка вперше дає користувачам і користувачкам доступ до рейтингової інформації про кожен пост у їхній стрічці. У нас також є інструменти, які дозволяють користувачам і користувачкам ще більше персоналізувати свою стрічку новин, зокрема перегляд постів у хронологічному порядку та можливість відображати пости від конкретної сторінки чи людини вгорі стрічки новин.

Заходи для запобігання дискримінації та підвищення прозорості

Один з наших головних пріоритетів — захист людей від дискримінації на Facebook. Наша рекламна політика вже давно забороняє дискримінацію, і ми вимагаємо від усіх рекламодавців засвідчити згоду з нашою політикою недискримінації, перш ніж напускати рекламу на Facebook.

Зараз ми вносимо фундаментальні зміни в те, як на Facebook відображається реклама про забезпечення житлом, вакансії та можливості кредитування. Ми не дозволяємо рекламодавцям таргетувати таку рекламу на підставі віку, гендеру, району проживання чи будь-яких інтересів, що вказують на захищені характеристики. Ці зміни повністю вступлять у дію в кінці 2019 року; вони є наслідком наших угод із потужними організаціями захисту громадянських прав та думок, висловлених експертами з громадянських прав. Ці угоди також включають у себе наше зобов'язання співпрацювати з правозахисною спільнотою та іншими експертами, щоб вивчати потенційні упередження алгоритмів, які ми (як і інші гравці на ринку) використовуємо, щоб показувати людям цікавий їм контент і рекламу.

Навіть до укладення угоди ми вже внесли зміни в нашу рекламну систему, яку рекламодавці використовують, щоб обирати аудиторію для реклами. Ми видалили тисячі категорій, які могли б потенційно бути пов'язаними з захищеними характеристиками. Наш перегляд опцій вибору аудиторії триває весь час і відбувається на основі відгуків від зовнішніх експертів.

Ми також створюємо нову секцію нашої Бібліотеки реклами, яка допоможе людям шукати та переглядати всі наявні рекламні оголошення із забезпечення житлом у США за локацією, обраною рекламодавцем, незалежно від того, чи ця людина входить в аудиторію, обрану рекламодавцем. Ми запровадимо подібні можливості для вакансій та реклами кредитів у США наступного року.

Ці зусилля з підвищення прозорості — продовження нашої роботи з запровадження високих стандартів прозорості політичної та іншої реклами на Facebook. Зокрема, ми маємо намір боротися з так званою «темною рекламою», про яку ви пишете. Ми продовжуємо працювати над забезпеченням прозорості та цінуємо відгуки, які отримали від організацій, вказаних у вашому звіті.

Потенційне неправомірне використання даних платформи Facebook розробниками сторонніх додатків

Ситуація з Cambridge Analytica виникла в контексті дій стороннього розробника — Александра Коґана — який порушив політику Facebook, продаючи дані Facebook третій стороні, Cambridge Analytica. Коли нам стало відомо про цю проблему, ми швидко вжили заходів, щоб розслідувати її, і отримали підписане свідоцтво від Коґана, Cambridge Analytica та інших, що вони видалили відповідні дані. У 2018 році з'явилася інформація про те, що Cambridge Analytica, можливо, не видалила дані, отримані від Коґана.

Ми визнаємо, що ситуація з Cambridge Analytica становила порушення довіри, і ми вжили заходів для того, щоб це не повторилося в майбутньому. До них належить:

- Зменшення кількості видів даних, якими люди можуть ділитися з розробниками додатків;
- Недопущення передачі нових даних Facebook додатку, яким користувач чи користувачка не користується понад 90 днів;
- Посилення нашого процесу оцінки додатків, вимагаючи, щоб більше додатків пройшли попередню оцінку, перш ніж вони зможуть просити користувачів і користувачок поділитися з ними інформацією;
- Розслідування діяльності додатків, які мали доступ до значного обсягу користувацької інформації, перш ніж ми змінили платформу у 2015 році, унеможлививши передачу інформації про друзів стороннім додаткам, а також
- Призупинення доступу розробників, які не співпрацюють з таким розслідуванням, і навіть судові розгляди.

В контексті цього розслідування ваш звіт вказує, що «десять тисяч... додатків було призупинено через потенційно неправомірне використання даних». Це не відповідає дійсності. Як ми повідомили в останньому оновленні з цього розслідування (яке вже торкнулося мільйонів додатків), ми призупинили доступ десятків тисяч додатків від близько 400 розробників. Призупинення не обов'язково означає, що ці додатки становили загрозу для користувачів і користувачок. Багато з них не були в роботі, а натомість ще тестувалися, коли ми їх призупинили. Розробники часто тестують численні додатки, які потім вирішують

не запускати. І в багатьох випадках ми призупинили роботу додатків через те, що розробники не відповіли на наші інформаційні запити.

Ви справедливо вказуєте, що таке розслідування складне, але помилково вважати, що ми не маємо достатньо інструментів, щоб визначити розробників, які порушили нашу політику, і вжити відповідних заходів. Ми зобов'язуємося вживати серйозних заходів — у тому числі подавати в суд на розробників, як ми це вже нещодавно робили.

Нарешті, завдяки нашій новій угоді з Федеральною комісією з питань торгівлі, ми маємо ще один набір вимог контролю за розробниками додатків на нашій платформі. Розробники повинні будуть щорічно засвідчувати згоду з нашими політиками. Будь-які розробники, які не виконуватимуть ці вимоги, будуть притягнуті до відповідальності.

Захист приватності у зв'язку з запитами від правоохоронних органів

Facebook розкриває інформацію про облікові записи у відповідь на правомірні легальні запити, відповідно до наших умов користування, відповідних законів та міжнародних стандартів у сфері прав людини. Оскільки ми серйозно ставимося до захисту даних наших користувачів і користувачок, ми ретельно розглядаємо кожен запит, щоб переконатися, що він відповідає цим вимогам. Коли ми вважаємо, що вимоги не виконані, ми відмовляємося надавати дані і, якщо необхідно, подаємо апеляцію на запит у суді. Ми це робили, зокрема, коли уряд, що подавав такий запит, перевищував свої повноваження при подачі запиту, або коли ми мали підстави вважати, що такий запит не відповідає міжнародним стандартам у сфері прав людини.

Ми відкрито оприлюднюємо інформацію про те, як ми забезпечуємо дотримання наших Стандартів спільноти і як ми реагуємо на інформаційні запити від урядових структур у наших регулярних Звітах про прозорість. На них варто звернути увагу.

Співпраця з урядовцями щодо важливих політичних питань

Як сказано у нашій щорічній декларації про політичну участь, рішення у сфері публічної політики можуть мати значні наслідки для людей, які використовують наші сервіси, та для подальшого розвитку нашої компанії. Facebook регулярно співпрацює з членами уряду для обговорення різних політичних питань, а також щоб поділитися інформацією про наші продукти та послуги. Таким чином ми забезпечуємо дотримання усіх відповідних законів та інструкцій. Всі працівники Facebook, включно із зовнішніми консультантами, які спілкуються з урядовцями для обговорення політичних питань від нашого імені, проходять навчання про етичні стандарти, які вимагаються при такій взаємодії.

Amnesty International — це глобальний рух за права людини. Коли несправедливість трапляється з однією людиною, це стосується нас усіх.

[Наші контакти](#)

[Долучіться до розмови](#)

Гіганти стеження:

Як бізнес-модель Google та Facebook несе загрозу правам людини

Google і Facebook допомагають людям з усього світу бути на зв'язку і надають мільярдам людей необхідні послуги. Щоб брати значущу участь в економічному та суспільному житті та щоб користуватися своїми правами людини, у наш час люди потребують доступу до інтернету — і тих інструментів, які надають Google і Facebook.

Але попри справжню цінність послуг, які вони надають, за платформи Google і Facebook доводиться платити чималу ціну. Щоб мати змогу користуватися своїми правами онлайн, люди змушені миритися з постійним стеженням як в інтернеті, так і в реальному світі, зокрема через прилади, що мають доступ до інтернету. Бізнес-модель Google і Facebook, що ґрунтується на стеженні, за своєю природою несумісна з правом на приватність та ставить під загрозу ряд інших прав, зокрема свободу переконань і висловлювань, свободу думки, право на приватність і право не бути дискримінованим/-ою.

Урядам слід вжити позитивних заходів на зменшення шкоди від бізнес-моделі на основі стеження — прийняти такі політики у сфері цифрових технологій, які б забезпечували загальний доступ та змогу користуватися правами людини та знижували чи ліквідували нав'язливе стеження з боку корпорацій. Також варто впровадити структурні реформи, яких було б достатньо для відновлення довіри до інтернету як такого. Google і Facebook, а також інші ІТ-компанії, повинні покінчити з повсюдним стеженням і перейти на бізнес-модель, яка передбачає дотримання прав людини.