

УДК 340+342.7+330.1

DOI <https://doi.org/10.32849/2663-5313/2019.6.43>**Юлія Разметаєва,**

канд. юрид. наук,

асистент кафедри теорії і філософії права

Національного юридичного університету імені Ярослава Мудрого

ТЕОРЕТИЧНІ АСПЕКТИ ЗОБОВ'ЯЗАНЬ БІЗНЕСУ У СФЕРІ ПРИВАТНОСТІ: ВИКЛИКИ ЦИФРОВОЇ ЕПОХИ

Стаття присвячена зобов'язанням бізнесу у сфері прав людини, зокрема щодо права на приватність в умовах цифрової епохи. Досліджуються зміни у приватності, які стосуються колективного характеру, цифрового сліду, зсуву фокусу комунікації, а також основні точки її вразливості перед діяльністю компанії. Розглядаються обов'язкові та добровільні стратегії дотримання приватності, що можуть базуватися на економічному інтересі та глобальному стандарті.

Ключові слова: права людини, сучасна концепція прав людини, право на приватність, зобов'язання бізнесу, діяльність бізнесу, інформаційні відносини, інформаційні технології, цифрова епоха, цифровий слід.

Постановка проблеми. Сучасна концепція прав людини змінюється під впливом розвитку світу, як і право в цілому. Особливо це помітно останніми роками, оскільки інформатизація суспільства значно прискорює всі соціальні перетворення. На передній план виходять такі потужні гравці, як національні та транснаціональні корпорації, міжнародні організації та структури громадянського суспільства, які серйозно впливають на реалізацію та захист прав осіб. Тому гучніше звучать голоси тих, хто говорить про горизонтальний вимір прав, розширення кола їх носіїв та адресатів, а також необхідність перегляду зобов'язань у сфері прав людини [1; 2; 3]. Однією із суттєвих проблем є зіткнення права на приватність (або прайвесі) та інтересів бізнесу у цифровому світі.

Коли журналістка Дж. Дюпортейл надіслала запит з вимогою надати доступ до всіх зібраних про неї даних до Tinder, найпопулярнішого у світі додатку для знайомств, то у відповідь вона отримала документ на 800 сторінок [4]. Там було все: всі лайки у Facebook і фотографії в Instagram (навіть ті, що були опубліковані після видалення зв'язків між акаунтами), освіта та вік чоловіків, які її цікавили, скільки разів контактувала з кимось, коли і де вела листування з кожним, музичні та гастрономічні смаки та багато інших відомостей. Вона виявила, що корпорація-власник Tinder знає її краще, ніж друзі та рідні. Такі випадки змушують розмірковувати над тим, чи залишилася взагалі якась приватність у нашому новому світі, де віртуальне життя зливається з реальним?

І відповідь може бути такою: приватність не втрачена, але вона змінює форму.

Аналіз останніх досліджень і публікацій з цієї теми. Концепція прайвесі і без новітніх викликів досить суперечлива. Визначення самого права містять спектр розумінь – від недоторканості приватного життя особи, яке охоплює фізичну та душевну недоторканість, та захищеної індивідуальності до можливості поділитися інформацією із самостійно обраними особами, права бути залишеним у спокої, контролю над персональною інформацією тощо. Так, відомий дослідник проблематики приватності В.О. Серьогін розглядає такі її розуміння, як право бути залишеним у спокої, обмежений доступ до себе, секретність, контроль над персональною інформацією, захищену індивідуальність, інтимність тощо [5, с. 107–140]. Синтетичні концепції приватності передбачають складну структуру: інформаційну, тілесну, комунікаційну, дислокаційну, приватність вираження [6, с. 43]. Важливим питанням для прав людини та збереження приватності у сучасному інформаційному суспільстві стає природа зобов'язань бізнесу у сфері прав. Висловлюються думки про те, що наявного регулювання не досить, система міжнародного права не є ефективною щодо корпорацій, національні стратегії не охоплюють цієї проблематики достатньою мірою. Так, Дж. Нокс, розглядаючи небезпеку для прав людини і потенційні обов'язки бізнесу, пише, що невідомо, чи слід вирішувати питання «через наявну систему горизонтального права прав людини, відповідно до якої більшість зобов'язань приватних суб'єктів виводяться опосередковано,

або ж систему слід модифікувати, щоб такі зобов'язання були прямими й безпосередніми, принаймні для корпорацій» [2, с. 47]. Набуває популярності концепція реалізації компаніями зобов'язань у сфері прав, заснована на стратегії «належної обачності». Як зазначається, вона може допомогти «вирішувати багатогранні проблеми, що виникають у світі, який швидко глобалізується, за відносної відсутності обов'язкового міжнародного права, що регулює як кібербезпеку, так і сферу перетину бізнесу та прав людини» [3, с. 860]. Вочевидь, що, незважаючи на моделі, пропоновані такими документами, як Керівні принципи ООН щодо бізнесу та прав людини (реалізація Рамкової програми Організації Об'єднаних Націй «Захист, повага і засоби захисту») та Керівні принципи ОЕСР щодо багатонаціональних підприємств (рекомендації для відповідального ведення бізнесу в глобальному контексті), а також зусилля Форуму ООН «Бізнес і права людини» та відповідних робочих груп, проблема зобов'язань компаній, зокрема щодо приватності, є далекою від вирішення.

Метою цієї статті є висвітлення змін у праві на приватність та пов'язаних правах людини в умовах цифрової епохи, у тому числі тих, що відбуваються під впливом діяльності компаній, а також тенденцій розвитку концепції зобов'язань бізнесу у сфері приватності та інших прав.

Виклад основного матеріалу дослідження. Що саме змінюється у приватності під впливом технологічних досягнень і діяльності бізнесу?

Багато з тих, хто читає цю статтю, користуються соціальними мережами, у тому числі викладає фотографії, позначаючи на них своїх знайомих, близьких і колег, додаючи місцезнаходження та змістовні теги. У разі зі спільними фото контроль над налаштуваннями приватності основні соціальні медіа дають тій особі, яка завантажує знімок. Отже, якщо ви завантажуєте фото, приміром, з конференції раніше за свою колегу, то контролюєте, хто побачить цей знімок. Своєю чергою колега може обрати такі налаштування, які дадуть змогу регулювати аудиторію публікацій або порядок позначення її на знімках, або ж звернутися до служби підтримки з вимогою видалити позначку чи навіть саме фото.

Отже, перша зміна – *приватність стає колективним явищем*. Відтепер приватна інформація – це не тільки те, що ви говорите чи розкриваєте про себе, а також те, що інші кажуть або розкривають про вас.

Активно обговорюючи вік цифрової згоди, тобто вік, коли ви можете бути досить

дорослим, щоб вести активне віртуальне життя, для вироблення спільного європейського законодавства уряди різних держав надавали пропозиції відліковувати його з 18 або 16 років. Корпорації прагнули відліковувати цей вік хоча б з 13 років [7]. Ця ситуація показує не тільки те, наскільки інтереси бізнесу у цифровому світі можуть розходитися з доктриною прав людини, але й те, наскільки сучасна реальність далеко відійшла від класичних теорій дієздатності та вікових обмежень діяльності осіб, яка може мати юридично значущі наслідки.

Дослідження щодо підлітків, соціальних мереж та приватності виявили, що лише 9% підлітків були стурбовані стороннім доступом до своїх даних на Facebook, але 80% їхніх батьків висловили високу стурбованість [8]. У Великобританії широко обговорювалися юридичні наслідки випадку, у якому 14-річний хлопець надіслав оголене селфі дівчині через Snapchat, програму, яка видаляє прямі повідомлення протягом 10 секунд [9]. Проте перш ніж світлина зникла, дівчина зберегла її на власному телефоні, а потім відправила іншим учням. Згідно з місцевими правилами, інцидент був зареєстрований поліцією. І дані цього хлопця будуть зберігатися в поліцейській базі даних щонайменше 10 років. Ця інформація також може бути розкрита майбутнім роботодавцем, якщо він захоче, приміром, працювати з дітьми.

Отже, друга зміна у приватності під впливом технологічних досягнень і діяльності бізнесу – це *довгий цифровий слід*. Ви можете забути, яку приватну інформацію розкривали колись, ви можете більше не відчувати зв'язок з тією людиною, якою колись були, мати іншу ідентичність, але багато відомостей про вас залишаються збереженими у цифровій формі та можуть бути доступними роки потому.

Знакова справа про цифрове забуття, яка була розглянута Судом Європейського Союзу за зверненням іспанського громадянина Mario Costeja Gonzalez, який знайшов через пошук Google за своїм ім'ям відомості 16-річної давнини про банкрутство та аукціон нерухомості, пов'язані з його старими боргами [10], поклала початок новій судовій практиці та регулюванню, а також визнанню права бути забутих. У наведеній справі Суд ЄС дійшов висновку, що корпорації, які збирають особисту інформацію для отримання прибутку, мають прибрати посилення за запитом особи, тому що фундаментальні права переважають над комерційними інтересами, а в окремих випадках також і над публічними інтересами щодо доступу до інформації. Однак право бути забутих,

на яке посилався суд, має досить обмежене застосування, і до того ж бізнес-структури не палають бажанням поступатися прибутком заради належної поваги до прав людини та здійснювати пошук дорогих технічних рішень, особливо там, де правове поле вкрито туманом невизначеності.

Приватність є правом людини і гарантією людської гідності, важливим способом захисту ідентичності, підтримки особистої безпеки та сприяння свободі вираження поглядів. І розглядається вона, як правило, в контексті приватних думок або дій особи або у зв'язку з її взаємодією з іншими. Проте люди вже довіряють багато приватного життя не живим співбесідникам, а своїм пристроям. Ідея смартфона – це ідея цифрового продовження самого себе, а залежність від подібних пристроїв буде лише посилюватися.

Отже, третя зміна, яка відбувається під впливом технологічних досягнень і діяльності бізнесу, – це *зсув фокусу комунікації у приватності*, коли взаємодія здійснюється не лише між людиною, але й між людиною та пристроєм.

Які головні вразливості права на приватність перед діяльністю бізнесу?

По-перше, застосування технологічних досягнень для вторгнення до приватного життя, стеження та збирання персональних даних і поведінкових реакцій. Так, 5 вересня 2017 року Велика палата ЄСПЛ винесла рішення щодо права на приватність особистої кореспонденції на робочому місці [11]. Заявник був звільнений після того, як декілька разів використав обліковий запис Yahoo Messenger (який попросив створити роботодавець), щоб відповідати не лише на запити клієнтів. Внутрішні норми роботодавця прямо забороняли особисте використання всіх засобів, включаючи комп'ютери та доступ до Інтернету. Роботодавець інформував заявника про те, що протягом 8 днів спостереження за повідомленнями було встановлено, що він використовував Інтернет в особистих цілях. Згодом був представлений 45-сторінковий протокол повідомлень, який включав листування заявника з братом та нареченою, у тому числі досить інтимні повідомлення. І хоча він знав, що йому не дозволено використовувати робочі комп'ютери з особистих причин, роботодавець не повідомив йому, що веде стеження за повідомленнями. Велика палата ЄСПЛ вирішила, що держави-члени мають позитивний обов'язок щодо ст. 8 Конвенції про захист прав людини і основоположних свобод, а національні органи влади мають забезпечити, щоб роботодавець вжив заходів для моніторингу кореспонденції «адекватними та достатніми» гарантіями проти зловживань.

По-друге, накопичення великого обсягу інформації та обмін нею, особливо в діяльності транснаціональних корпорацій. Ми нерідко бачимо у ЗМІ повідомлення, що внаслідок вдалої хакерської атаки чи упущеної вразливості було вкрадено мільйони даних користувачів, серед яких можуть бути не лише паролі та імена, але й номери кредитних карт. Зустрічаємо таргетовану рекламу. Починаємо набирати запит у пошукачі і бачимо підказку – слово або фразу, які нам потрібні, або ні – хто може бути впевнений? Наприклад, мобільна операційна система Android, YouTube та Google Inc. належать до Alphabet груп, що значно розширює охоплення користувачів і вплив на них, а також накопичення інформації в одних руках. Користувачі при цьому можуть навіть не підозрювати про зв'язки між названими компаніями.

По-третє, використання необізнаності людей і прогалин у правовому регулюванні (а вони дуже великі просто через бурхливий розвиток інформаційних технологій). Ключові висновки рейтингу дотримання цифрових прав уже декілька років поспіль надають підтвердження неадекватності розкриття приватної інформації компаніями. Крім того, обробка інформації користувачів є непрозорою. Незрозуміло, як і чому наша інформація збирається, зберігається та використовується. У 2017 році оцінки найпопулярніших компаній серед Інтернет та мобільних компаній розподілилися так: Google (65%), Microsoft (62%) та Yahoo! (58%), тоді як найнижчою оціночною є компанія Baidu (13%), Mail.ru (22%) та Tencent (22%). У 2018 році 17 з 22 ключових компаній покращили показники принаймні в одній з галузей, однак їхні режими збереження приватності залишаються далекими від ідеальних [12].

Якими мають бути обов'язки бізнесу в сфері прав людини, зокрема щодо права на приватність?

Поки що ні на глобальному, ні на національному чи локальному рівнях немає консенсусу стосовно того, чи мусить бізнес мати прямі міжнародні зобов'язання щодо прав людини. Наводяться аргументи, що добровільні ініціативи можуть прокласти шлях до змін, проте не дають певних перспектив захисту, і, відповідно, корпорації можуть ігнорувати їх без будь-яких юридичних наслідків. Разом із тим введення обов'язків для бізнесу стикається з низкою проблем. Обговорення таких зобов'язань здійснюється, зокрема, в межах неурядових ініціатив, а також у межах мандату Міжурядової робочої групи ООН з розробки проекту «Міжнародний юридично обов'язковий документ» з питань бізнесу та прав людини.

Інша площина дискусії розглядає питання: чи має обов'язковий документ стосуватися лише транснаціональних корпорацій як специфічних бізнес-структур або поширюватися на всі типи компаній. Зокрема, наводяться аргументи, що документ має охопити і національні підприємства, щоб не допустити зловживань у сфері прав людини. При цьому особлива увага має приділятися транснаціональним корпораціям, наприклад, у таких питаннях, як екстериторіальна юрисдикція та відповідальність материнських компаній.

Так, законодавство Європейського Союзу в сфері захисту приватності вже накладає значно більші обов'язки на компанії. Підприємства мусять мати можливість продемонструвати, що вони впровадили технічні та організаційні заходи, які показують, як вони розглядають та об'єднують дані у процесах обробки, що вони знають, якою інформацією володіють і де зберігають [13]. Недотримання може привести до максимального штрафу у розмірі 20 тис. євро.

Однак фактичне притягнення компаній до відповідальності стикається з низкою проблем, зокрема, коли йдеться про діяльність транснаціональних корпорацій та особливості національних правових систем.

Режими збереження приватності виглядають по-різному в різних державах. І суміш державного сектору, приватного сектору та технологічних інструментів, що використовуються для вирішення проблем приватності, значно відрізнятиметься. Водночас раніше розмежовані регуляторні юрисдикції стають все більш взаємозалежними. Тож у потенційному регулюванні треба враховувати як ці регуляторні розбіжності, так і глобалізований ринок.

Виникає справедливе питання: для чого це потрібно бізнесу – дотримуватися прав людини і, зокрема, стандартів щодо права на приватність?

Відповідь проста – економічний інтерес. У цифрову епоху в умовах поведінкової економіки та персоналізації для компаній стає важливим збереження довіри користувачів, наявність позитивного рейтингу й соціального капіталу. Крім того, ідея про те, що єдиним зобов'язанням компанії є максимізація прибутку вже не переважає над іншими ідеями. Якщо бізнес хоче, щоб клієнти почувалися добре, коли купують і використовують послугу або товар, і знову поверталися до конкретної компанії, він приділяє увагу правам людини. Якщо бізнес хоче залишатися конкурентоздатним та розвиватися, зважаючи на новітні вимоги та тренди, його довгострокові інтереси включають необхідність діяти відповідально.

До того ж бізнес може навіть надавати додатковий захист приватності або забезпечувати вищий рівень захисту порівняно з державними структурами, втілювати кращі практики у сфері прав людини, займаючи вигідну нішу першовідкривача на ринку.

Висновки

Якими мають бути стратегії поведінки та моделі зобов'язань бізнесу щодо права на приватність?

По-перше, *нам потрібне глобальне партнерство для вирішення проблем захисту прав людини у цифрову епоху*. І законодавство, і практика мають бути пристосованими до технологічних змін та враховувати:

1. Інноваційні способи, за допомогою яких можуть бути здійснені серйозні порушення приватності.

2. Необхідність балансування приватності з іншими правами людини та основними суспільними цінностями.

3. Режими застосування будь-яких засобів захисту, насамперед правового, та відшкодування за вторгнення до приватності.

По-друге, *нам потрібно виробляти глобальний стандарт приватності, який буде спиратися на розуміння того, що у цифровому світі є первинна приватна інформація, а також вторинна і поведінкова приватна інформація*.

Ми так влаштовані, що не відчуваємо приватні дані. Нам необхідно побачити роздруківку у 800 сторінок, доторкнутися до неї, щоб осягнути масштаб проблеми. Крім того, розумні очікування у сфері приватності мали б ґрунтуватися на таких налаштуваннях конфіденційності за замовчуванням, які за потреби можна розширити, а не звужити.

Глобальний стандарт має врахувати, що приватність може бути порушена як у спосіб вторгнення до усамітнення, наприклад фізичного втручання до приватного простору, спостереження, прослуховування або запису приватної діяльності особи, так і у спосіб маніпуляцій з приватною інформацією, особливо її викривлення, розголошення, безстрокового зберігання.

По-третє, *ми маємо поєднати добровільні та обов'язкові стратегії*. І закликати до широкої громадської дискусії про те, що таке приватність і якого її захисту очікують носії прав людини. Така дискусія має виходити за рамки обговорення «національної безпеки» і підійматися на глобальний рівень. Чим активніше ми зустрічаємо нові виклики, враховуючи уроки з попереднього досвіду, тим більше шансів, що інформаційні технології стануть джерелами добробуту та можливостей, а не загрозами приватності.

Список використаних джерел:

1. Алексі Р. Теорія дискурсу і права людини. *Філософія права і загальна теорія права* / пер. з англ. С.І. Максимова, О.О. Уварової. 2013. № 1. С. 73–98.
2. Knox J.H. Horizontal Human Rights Law. *The American Journal of International Law*. 2008. Vol. 102. No. 1. P.1–47.
3. Shackelford S.J. Human Rights and Cybersecurity Due Diligence: A Comparative Study. *University of Michigan Journal of Law Reform*. 2017. Vol. 50. No. 4. P. 859–885.
4. Duportail J. I asked Tinder for my data. It sent me 800 pages of my deepest, darkest secrets. *The Guardian*. 26 Sep 2017. URL: https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold?CMP=Share_iOSApp_Other.
5. Сербюгін В.О. Право на недоторканість приватного життя у конституційно-правовій теорії та практиці : монографія. Харків : Вид-во «Фінн», 2010. 608 с.
6. Разметаєва Ю.С. Приватність в інформаційному суспільстві: проблеми правового розуміння та регулювання. *Науковий вісник УЖНУ. Серія «Право»*. Вип. 37. Т. 1. 2016. С. 43–46.
7. Gibbs S. EU agrees draft text of pan-European data privacy rules and agencies. *The Guardian*. 16 Dec 2015. URL: <https://www.theguardian.com/technology/2015/dec/16/eu-agrees-draft-text-pan-european-data-privacy-rules>.
8. Teens, Social Media and Privacy. The Pew Research Center's Internet & American Life Project, by Madden M., Lenhart A., Cortesi S., Gasser U., Duggan M., Smith A., Beaton M. 21 May 2013. URL: <https://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/>.
9. Sexting boy's naked selfie recorded as crime by police. *BBC News*. 3 September 2015. URL: <http://www.bbc.com/news/uk-34136388>.
10. Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014), ECLI:EU:C:2014:317.
11. Barbulescu v. Romania, application no. 61496/08, 2017. ECHR.
12. The Ranking Digital Rights 2018. Corporate Accountability Index. 20 May 2019. URL: <https://rankingdigitalrights.org/index2018/>.
13. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Стаття посвячена обов'язкам бізнесу в сфері прав людини, в частині, стосовно права на приватність в умовах цифрової епохи. Вивчаються зміни в приватності, стосовно колективного характеру, цифрового сліду, зміщення фокусу комунікації, а також основні точки її уязвимості перед діяльністю компаній. Розглядаються обов'язкові та добровільні стратегії дотримання приватності, які можуть базуватися на економічному інтересі та глобальному стандарті.

Ключевые слова: права людини, сучасна концепція прав людини, право на приватність, обов'язки бізнесу, діяльність бізнесу, інформаційні відносини, інформаційні технології, цифрова епоха, цифровий слід.

The article is devoted to the obligations of business in the field of human rights, in particular, regarding the right to privacy in the digital era. The changes in privacy related to its collective nature, digital footprints, the shift of the focus of communication, as well as the main points of its vulnerability in accordance to the activities of companies are examined. The mandatory and voluntary privacy policies that can be based on economic interest and a global standard are considered.

Key words: human rights, modern concept of human rights, right to privacy, business obligations, business activities, informational relations, information technology, digital age, digital footprint.