Круглий стіл

"Налагодження співпраці стейкхолдерів в процесі інтеграції України в Єдиний цифровий ринок ЄС"

21 квітня 2021 року

ПРЯМУЄМО РАЗОМ

МІЖНАРОДНИЙ ФОНД ВІДРОДЖЕННЯ

Комітет цифрової трансформації

European Media Platform

Зміст

ПРЯМУЄМО РАЗОМ
МІЖНАРОДНИЙ ФОНД ВІДРОДЖЕННЯ
Комітет цифрової трансформації
European Media Platform

Матеріал підготовлено за підтримки Європейського Союзу та Міжнародного Фонду «Відродження» в межах грантового компоненту проєкту EU4USociety . Матеріал відображає позицію авторів і не обов'язково відображає позицію Міжнародного фонду «Відродження» та Європейського Союзу».

ПРЯМУЄМО РАЗОМ
МІЖНАРОДНИЙ ФОНД ВІДРОДЖЕННЯ
Комітет цифрової трансформації
European Media Platform

Огляд ринку електронних довірчих послуг

Лілія Олексюк

Вступ

У червні 2018 року в рамках круглого столу «Довіра та безпека в цифровій економіці» у Національному університеті «Києво-Могилянська академія» під егідою Української сторони Платформи громадянського суспільства Україна-ЄС та Української національної платформи Форуму громадянського суспільства Східного партнерства в рамках виконання проекту «Посилення участі громадськості у створенні та імплементації цифрового порядку денного України та гармонізації цифрових ринків з ЄС та країнами СхП» було презентовано інформаційно-аналітичний огляд сфери електронних довірчих послуг[1]. З того часу Закон України «Про електронні довірчі послуги»[2], що імплементує європейський Регламент eIDAS[3] був прийнятий.

Опис ринку

Міністерство цифрової трансформації України (Мінцифри) - головний орган у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері електронних довірчих послуг і виконує функції центрального засвідчувального органу.

Функції та повноваження центрального засвідчувального органу визначено у Статті 7 Закону України «Про електронні довірчі послуги», відповідно до якої Мінцифри:

- здійснює визначені законом повноваження у сферах електронних довірчих послуг та електронної ідентифікації:
- надає адміністративну послугу шляхом внесення юридичних осіб та фізичних осіб - підприємців, які мають намір надавати електронні довірчі послуги, до Довірчого списку;
- погоджує розроблені надавачами електронних довірчих послуг порядки синхронізації часу із Всесвітнім координованим часом (UTC);
- погоджує плани припинення діяльності кваліфікованих надавачів електронних довірчих послуг;
- приймає та зберігає документовану інформацію, сформовані сертифікати (у тому числі посилені, кваліфіковані) відкритих ключів, реєстри чинних, блокованих та скасованих сертифікатів відкритих ключів у разі припинення діяльності кваліфікованого надавача електронних довірчих послуг;
- розглядає пропозиції (зауваження) суб'єктів відносин у сфері електронних довірчих послуг щодо удосконалення державного регулювання сфери електронних довірчих послуг;
- надає суб'єктам відносин у сфері електронних довірчих послуг консультації з питань, пов'язаних з наданням електронних довірчих послуг;

[1] *https://vaibit.org.ua/trust-and-security-in-the-digital-economy/*

[2] *https://zakon.rada.gov.ua/laws/show/2155-19#Text*

[3] *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG*

- інформує відповідно до Закону України "Про електронні довірчі послуги" про обставини, які перешкоджають діяльності центрального засвідчувального органу;
- проводить оцінку стану розвитку сфери електронних довірчих послуг за результатами проведення аналізу інформації про діяльність постачальників електронних довірчих послуг та засвідчувального центру;
- забезпечує взаємне визнання українських та іноземних сертифікатів відкритих ключів та електронних підписів, що використовуються під час надання юридично значущих електронних послуг;
- здійснює інші повноваження у сферах електронних довірчих послуг та електронної ідентифікації, визначені законом;

Технічне та технологічне забезпечення виконання функцій центрального засвідчувального органу здійснюється адміністратором інформаційно-телекомунікаційної системи центрального засвідчувального органу - державним підприємством, яке належить до сфери управління Мінцифри (державним підприємством «ДІЯ»).

На сьогодні на ринку України послуги надають наступні кваліфіковані надавачі електронних довірчих послуг[4]:

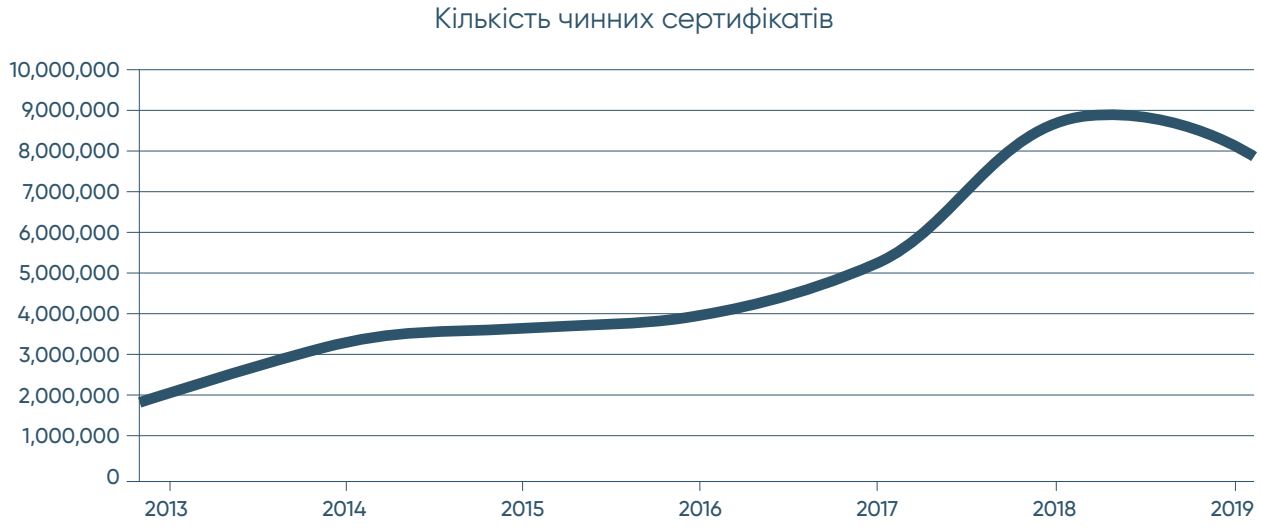
	Назва юридичної особи	Назва кваліфікованого надавача електронних довірчих послуг
1	АКЦІОНЕРНЕ ТОВАРИСТВО КОМЕРЦІЙНИЙ БАНК «ПРИВАТБАНК»	Кваліфікований надавач електронних довірчих послуг АЦСК АТ КБ «ПРИВАТБАНК»
2	Військова частина 2428	Кваліфікований надавач електронних довірчих послуг «Військова частина 2428» Державної прикордонної служби України
3	Генеральний штаб Збройних Сил України	Кваліфікований надавач електронних довірчих послуг «Центр сертифікації ключів Збройних Сил України»
4	Офіс Генерального прокурора	Кваліфікований надавач електронних довірчих послуг органів прокуратури України
5	Державна казначейська служба України	Кваліфікований надавач електронних довірчих послуг Державної казначейської служби України
6	Державне підприємство «Оператор ринку»	Кваліфікований надавач електронних довірчих послуг «АЦСК ринку електричної енергії»
7	Державне підприємство «ДІЯ»	Кваліфікований надавач електроних довірчих послуг «ДІЯ»
8	Державне підприємство «Український інститут інтелектуальної власності»	Кваліфікований надавач електронних довірчих послуг Укрпатенту
9	Державне підприємство «Українські спеціальні системи»	Кваліфікований надавач електронних довірчих послуг Державного підприємства «Українські спеціальні системи»
10	Інформаційно-довідковий департамент ДПС	Кваліфікований надавач електронних довірчих послуг Інформаційно-довідкового департаменту ДПС
11	Міністерство внутрішніх справ України	Кваліфікований надавач електронних довірчих послуг – акредитований центр сертифікації ключів МВС України
12	Національний банк України	Кваліфікований надавач електронних довірчих послуг «Акредитований центр сертифікації ключів Національного банку України»

[4] *https://czo.gov.ua/ca-registry*

13	Акціонерне товариство «Державний ощадний банк України»	Кваліфікований надавач електронних довірчих послуг - центр сертифікації ключів акціонерного товариства «Державний ощадний банк України»
14	Акціонерне товариство «УкрСиббанк»	Кваліфікований надавач електронних довірчих послуг АТ «УКРСИББАНК»
15	Товариство з обмеженою відповідальністю «Алтерсайн»	Кваліфікований надавач електронних довірчих послуг АЦСК «eSign» ТОВ «Алтерсайн»
16	Товариство з обмеженою відповідальністю «Арт-мастер»	Кваліфікований надавач електронних довірчих послуг «MASTERKEY»
17	Товариство з обмеженою відповідальністю «Інтер-Метл»	Кваліфікований надавач електронних довірчих послуг «АЦСК ТОВ 'Інтер-Метл'»
18	Товариство з обмеженою відповідальністю «Центр сертифікації ключів «Україна»	Кваліфікований надавач електронних довірчих послуг ТОВ «Центр сертифікації ключів «Україна»
19	Філія «Головний інформаційно-обчислювальний центр» акціонерного товариства «Українська залізниця»	Кваліфікований надавач електронних довірчих послуг ЦСК АТ «УКРЗАЛІЗНИЦЯ»
20	Товариство з обмеженою відповідальністю «ДЕПОЗИТ САЙН»	Кваліфікований надавач електронних довірчих послуг «ДЕПОЗИТ САЙН»
21	Національний банк України	Кваліфікований надавач електронних довірчих послуг «Акредитований центр сертифікації ключів Національного банку України»
22	Акціонерне товариство «УКРСИББАНК»	Кваліфікований надавач електронних довірчих послуг АТ «УКРСИББАНК»
23	ПАТ «Альфа-Банк»	Кваліфікований надавач електронних довірчих послуг - Акредитований Центр сертифікації ключів АКЦІОНЕРНОГО ТОВАРИСТВА «АЛЬФА-БАНК»
24	АТ «КРЕДІ АГРІКОЛЬ БАНК»	Кваліфікований Надавач електронних довірчих послуг АТ «КРЕДІ АГРІКОЛЬ БАНК»
25	АКЦІОНЕРНЕ ТОВАРИСТВО «ПЕРШИЙ УКРАЇНСЬКИЙ МІЖНАРОДНИЙ БАНК»	Кваліфікований надавач електронних довірчих послуг АТ «ПУМБ»

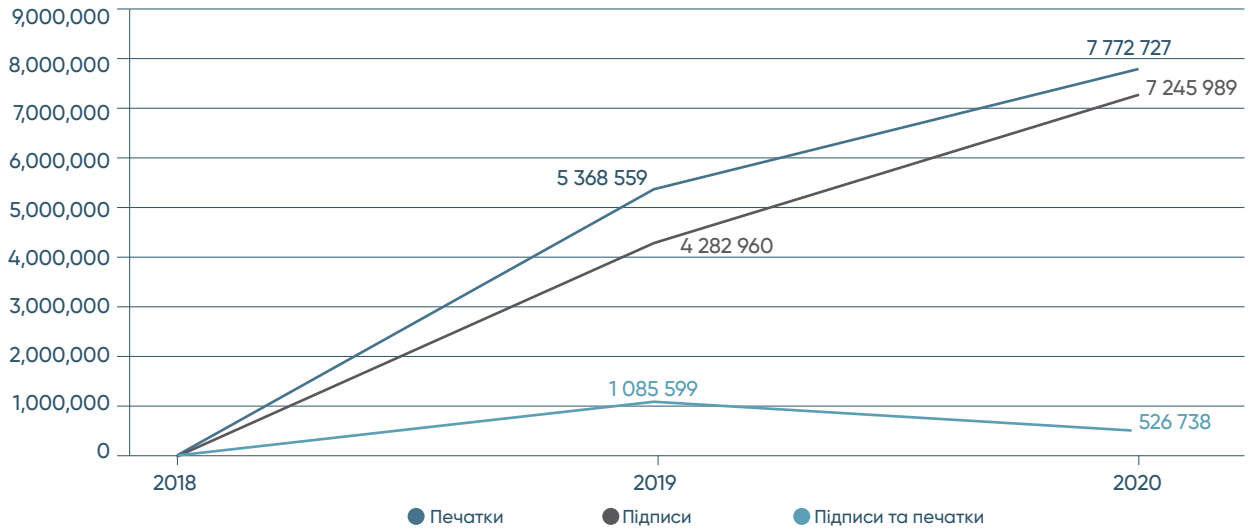
З них 15 – це публічний сектор, а 10 – приватні компанії. Таким чином, на ринку суттєво переважають державні кваліфіковані надавачі електронних довірчих послуг.

За час з 2013 по 2019 рік використання електронних довірчих послуг збільшується.



За останніми даними Мінцифри майже 4 млрд. разів українці скористалися електронним підписом за 2020 рік[5], а кількість сертифікатів збільшилась:

Динаміка виданих печаток/підписів/печаток та підписів разом за 2019-2020 роки



В даний час в Україні діє приблизно 7,8 мільйона сертифікатів, які активно використовуються.

Це відносно загальної кількості населення України приблизно 18,5 відсотка (якби теоретично, сертифікат був один на одну особу), без урахування дітей віком до 17 років - 33 відсотки (сьогодні, за даними Державної служби статистики, в Україні проживає 41,98 млн. осіб, у тому числі 7,58 дітей до 17 років).

Також на сьогодні в Україні використовуються eID (ідентифікатори) в даний час.

Послуга, яка надає ідентифікаційну інформацію, знаходиться тут https://id.gov.ua/.

Система інтегрує всіх постачальників послуг електронної ідентифікації: електронний підпис, BankID, MobileID.

Тут фізичні та юридичні особи можуть отримати доступ до державних електронних послуг.

Держава гарантує користувачам системи безпеку та захист персональних даних.

Як вже зазначено вище, на сьогодні існують декілька варіантів цифрової ідентифікації - ID карта, електронний підпис, BankID, MobileID.

ID карта — користувачі платять за послугу Державній міграційній службі[6]. Ця послуга стала доступною лише 5 лютого 2020 року, тому у відсотковому співвідношенні складає не більше 2%. Кількість зчитувачів для ID карта є недостатньою і, отже, майже не використовується.

Електронний підпис — користувачі платять кваліфікованим постачальникам електронних довірчих послуг, що зазначені в таблиці вище і складає 7,8 млн. сертифікатів.

[5] *https://bit.ly/3x9BtgC*

[6] *https://dmsu.gov.ua/faq/pasport-gromadyanina-ukrajni-id-kartka.html*

BankID – безкоштовна послуга, яку надає Національний банк України[7]. Цей спосіб електронної ідентифікації громадян за допомогою їх банківських реквізитів там, де їх обслуговують. Послуга надається Національним банком України і доступна лише клієнтам тих банків, які її підтримують. Список постійно оновлюється[8]. Коли користувач обирає свій банк, він перенаправляється для ідентифікації на веб-сайт власного банку. Отримавши логін, пароль, номер картки, система погоджується на передачу особистих даних клієнта, що дозволяє ідентифікувати його. Інформація, яка передається: ПІБ, дата народження, індивідуальний податковий номер (ІПН), адреса реєстрації, номер телефону, адреса електронної пошти, сканування паспорта та ІПН.

MobileID безкоштовно послугу могли надавати три найбільших мобільних оператора в Україні - Київстар, Vodafone, Lifecell .Це спосіб електронної ідентифікації громадян за допомогою мобільного оператора. Даний спосіб ідентифікації використовується лише якщо SIM-картка клієнта має електронний підпис. Щоб отримати таку SIM-карту, потрібно зв'язатися зі своїм постачальником послуг: обміняти наявну SIM-карту на нову та активувати її. На жаль, послуга не користується попитом за двох основних причин – в Україні жителі не бажають в ідентифікувати себе як користувачі мобільного зв'язку, друга – операторам так і не вдалось домовитись щодо застосування MobileID для надання публічних послуг.

Таким чином, на сьогодні активне застосування на ринку мають лише два види послуг – електронний підпис та BankID.

Нормативно-правове наближення

Ухвалений у 2018 році Закон України «Про електронні довірчі послуги» (далі – Закон) мав низку розбіжностей із Регламентом eIDAS, які необхідно буде з часом доопрацювати, особливо при бажанні України доєднатись до Єдиного цифрового ринку ЄС.

Правові підстави для укладення сторонами міжнародного договору, згідно з яким Україна зможе приєднатися до загальноєвропейської системи транскордонної електронної ідентифікації та автентифікації були переглянуті, і досягнуто домовленості про необхідність укладення такої угоди, що буде передувати відкриттю ринків. Особливу увагу слід звернути на те, що у Регламенті eIDAS та інших правових актах ЄС є багато положень (наприклад, принцип внутрішнього ринку, взаємне визнання, повідомлення про схеми електронної ідентифікації), які стануть актуальними та можуть застосовуватися лише після підписання згаданого міжнародного договору.

Регламент спрямований на публічний сектор (вони зобов'язані надати можливість зацікавленим особам використовувати засоби електронної ідентифікації, як це передбачено Регламентом eIDAS), тоді як українське законодавство застосовується як до державного, так і до приватного сектору (отже, це накладає обов'язок на ширшу групу осіб визнавати іноземних постачальників електронних довірчих послуг, і потребує широких консультацій).

Закон здебільшого відповідає розділу визначень Регламенту (який є підставою для подальшого регулювання), однак, не у всіх випадках. Визначення кваліфікованої електронної позначки часу та кваліфікованої електронної служби зареєстрованої доставки відсутні і потребують врегулювання.

[7] *https://id.bank.gov.ua/*
[8] *https://bit.ly/3sHwyjT*

Закон передбачає конкретну технологію та процеси, що використовуються у сфері електронних довірчих послуг (особисті та відкриті ключі, асиметричне криптографічне перетворення). Така відмінність повинна оцінюватися з точки зору принципу технологічної нейтральності, який визнаний в ЄС і який забезпечує доступність усіх технологічних рішень, якщо їм вдається досягти того самого або подібного результату. Існує імовірний ризик того, що такий конкретний опис технології або процесу, викладений в Законі може суперечити вищезазначеному принципу і потребує детальних досліджень.

Неодноразово як європейські, так і українські експерти звертали увагу на те, що Регламент eIDAS прямо вказує на необхідність дотримання належного рівня захисту персональних даних. З того моменту, коли Україна укладе відповідну міжнародну угоду з Європейським Союзом і вона стає частиною загальноєвропейської системи електронних довірчих послуг, вона повинна забезпечити, що GDPR вже є перенесеним в її законодавство і застосовується.

Є також необхідність встановити необхідний рівень надійності засобів електронної ідентифікації для іноземних постачальників електронних довірчих послуг.

Доопрацювання потребують механізми встановлення відповідальності щодо осіб, які завдають шкоди користувачам електронних довірчих послуг, хто має тягар доказування при доведенні злочинних намірів або недбалості постачальників послуг довіри.

Загальним правилом для постачальників електронних довірчих послуг має бути обов'язок інформувати ЦЗО, клієнтів та громадськість про порушення безпеки або втрати цілісності, що має значний вплив на надану послугу довіри або збережені в ній персональні дані, а також відсутні положення про управління ризиками.

Є питання досі до проведення процедур оцінки відповідності та їх необов'язковості в процесі отримання статусу кваліфікованого постачальника послуг довіри. Закон не регулює особливості зберігання даних.

Регламент eIDAS зазначає, що електронна відмітка часу не може бути відмовлена в юридичній дії та прийнятності як доказ у судовому процесі лише на тій підставі, що вона знаходиться в електронній формі або що вона не відповідає вимогам кваліфікованої електронної відмітки часу. Однак українське законодавство не передбачає положення про юридичні наслідки електронних відміток часу.

Питання електронної ідентифікації та автентифікації Законом врегульовано відповідно до Регламенту eIDAS. Але з метою підготовки до підписання міжнародного договору, українські органи влади мають не лише підготувати низку нових постанов Кабінету Міністрів України, що регулюють різні аспекти електронної ідентифікації та автентифікації, а мають виправити згадані неточності.

Нові плани ЄС та України

За період від ухвалення Закону в України з'явились амбітні плани щодо інтеграції до Єдиного цифрового ринку ЄС і на початку року був схвалений новий амбітний план, що передбачає оновлення законодавчої бази України[9].

Нещодавно був затверджений відповідний Спільний Робочий план співпраці між ЄС та Україною

[9] *https://thedigital.gov.ua/projects/yevrointegraciya*

щодо електронних довірчих послуг з перспективою укладення можливої угоди, яка повинна базуватися на наближенні до законодавства та стандартів ЄС[10]

За цей час і ЄС не стояв на місці і за час дії Регламенту eIDAS, як це зазвичай є з регулюванням, виявились певні окремі моменти, що потребують додаткового врегулювання.

У своїй Стратегії формування європейського цифрового майбутнього[11] Комісія зобов'язалась переглянути Регламент eIDAS, щоб підвищити його ефективність, поширити його застосування на приватний сектор та просувати надійні цифрові ідентичності для всіх європейців.

Регламент eIDAS, прийнятий у 2014 році, спрямований на підвищення довіри до електронних транзакцій на єдиному ринку, забезпечуючи:

- загальну систему взаємодії та взаємного визнання, яка дозволяє приватним особам та компаніям використовувати власні національні схеми електронної ідентифікації (eID) для автентифікації при доступі до державних послуг в інших державах-членах ЄС. Обов'язкове взаємне визнання повідомлених електронних посвідчень (eID) застосовується з 2018 року.
- нормативна база для розвитку європейського внутрішнього ринку електронних довірчих послуг (електронні підписи, електронні печатки, відмітки часу, послуги електронної доставки та автентифікація веб-сайтів), визнана за кордоном з таким самим правовим статусом, як традиційні паперові процеси. Ця нормативна база застосовується з 2016 року.

За допомогою eIDAS ЄС створив основи та передбачувану правову базу для людей, компаній (зокрема МСП) та державних адміністрацій для безпечного доступу до послуг та здійснення транзакцій в Інтернеті та за кордоном. Рішення eIDAS зменшують тяганину для громадян та створюють економію для бізнесу. Розгортання eIDAS означає більший рівень безпеки та підвищену зручність для будь-якої транскордонної діяльності в Інтернеті, яка вимагає довіреної ідентифікації, наприклад подання податкових декларацій, вступ до іноземного університету, дистанційне відкриття банківського рахунку, створення бізнесу в іншій державі-члені, автентифікація для здійснення Інтернет-платежів або надсилання заявок на тендер.

Як важливий елемент та механізм транскордонних цифрових державних послуг, Регламент eIDAS сприяє досягненню єдиного ринку. Визнання електронних ідентифікаторів в рамках eIDAS є ключовим фактором для транскордонного застосування принципу «один раз», одного з основних елементів Єдиного цифрового шлюзу.

Електронну ідентифікацію можна розглядати як цифровий еквівалент пред'явлення посвідчення особи або паспорта у фізичному світі. У цьому сенсі електронна ідентифікація є ключовим компонентом цифрової ідентичності, що також включає атрибути, посвідчення та атестації, такі як вік чи професійна кваліфікація, які не обов'язково ідентифікують особу, але дозволяють надавати послуги, що підлаштовуються під замовлення. У певних сферах, таких як державні послуги чи банківська справа, цифрова ідентичність повинна бути перевірена та засвідчена, щоб довести, що людина справді є такою, якою вона претендує.

В умовах гіперпов'язаної економіки цифрова ідентичність (digID) стає важливим фактором, що сприяє цифровим транзакціям. Потреба встановлювати особисті дані однозначно, точно, швидко та надійно не обмежується лише фізичними особами, а поширюється на юридичні

[10] *https://bit.ly/3tzadGr*

[11] *https://bit.ly/3sz9RhE*

особи, машини та пристрої. Сьогодні надання цифрової ідентифікації зазнає фундаментальних змін, оскільки такі організації, як банки, провайдери електронних комунікаційних послуг або великі онлайн-платформи, все частіше виступають у ролі постачальників ідентифікаційних даних, тоді як таке ринкове надання цифрової ідентифікації та автентифікації уникає регулювання.

Більше того, криза COVID-19 підкреслила необхідність швидкого надання всім європейським громадянам та підприємствам загальновизнаної цифрової ідентичності, що отримує довіру, та таких довірчих послуг, як eSignatures, щоб забезпечити безперервну безперервність бізнесу на Єдиному ринку, доступ до важливих та чутливих державні онлайнові служби, такі як електронне охорона здоров'я, електронний уряд та електронне правосуддя, а також пом'якшення ситуації проти шахрайства з особистими даними. Ця ініціатива допоможе прискорити цифровізацію з метою трансформації нової динаміки, пережитої під час кризи, у стійкий цифровий прогрес у державному та приватному секторі.

Регламент eIDAS запровадив першу транскордонну основу для довірених цифрових ідентифікаційних даних та довірчих послуг у 2014 році. Метою регламенту eIDAS є полегшення доступу всіх громадян ЄС до державних послуг по всьому ЄС за допомогою електронної ідентифікації (eID), виданої в їх рідна країна.

Незважаючи на безперечні досягнення, потенціал електронної ідентифікації та автентифікації в рамках eIDAS залишається недостатньо використаним. Сьогодні лише 15 з 27 держав-членів (~ 58% населення ЄС) пропонують своїм громадянам транскордонну електронну ідентифікацію згідно eIDAS[12]. Застосування цих засобів електронної ідентифікації та пропозиція публічних Інтернет-послуг, які можна використовувати з ними, є дуже нерівним у різних державах-членах. Не всі держави-члени пропонують електронні ідентифікатори та використання в приватному секторі, наприклад, для Інтернет-банкінгу або Інтернет-магазинів, як правило, неможливо, оскільки Регламент просто заохочує держави-члени надавати ІД-адреси приватним постачальникам онлайн-послуг, але дуже мало держав-членів запровадили це можливість. Безпечні та надійні ринкові рішення мали певний успіх, але не розширюються по всьому ЄС, оскільки працюють здебільшого в нерегульованому середовищі, не маючи юридичної визначеності та стимулів. Рішення основних соціальних платформ пропонують зручність, що відбувається ціною втрати контролю над розкритими персональними даними. Більше того, ці рішення від'єднані від перевіреної фізичної особи, що ускладнює пом'якшення шахрайства (наприклад, викрадення особистої інформації) та загрози кібербезпеки. Крім того, ця практика може викликати занепокоєння щодо ринкової сили та впливу на рівні умови, коли може розвиватися конкурентний ринок послуг, що розширює можливості користувачів, що надають цифрову ідентичність.

Як результат, сьогодні неможливо ідентифікувати в Інтернеті єдиний безпечний, зручний та надійний електронний ідентифікатор та захистити особисті дані так само, як за допомогою посвідчення особи або паспорта у фізичному світі. . Незважаючи на зростаючий попит, доступні рішення не підтримують ідентифікацію пристроїв, датчиків, моніторів для управління їх доступом до конфіденційних та нечутливих даних. Бізнес-можливості залишаються невикористаними, а безпечні витрати на ідентифікацію залишаються надмірними, наприклад, у банківській та фінансовій сферах, доки надійний державний електронний ідентифікатор не може широко та зручно використовуватися в приватному секторі та / або ринкові рішення не підтримуються нормативно-правовими актами.

Європейське рішення щодо ідентифікації, що дозволяє довіряти ідентифікацію громадян та

[12] *https://bit.ly/3n08K9A*

компаній у їх цифрових взаємодіях для доступу до державних або приватних онлайн-послуг (наприклад, електронної комерції), має бути цілком добровільним для користувачів дотримуватися та повністю захищати дані та конфіденційність. Анонімність Інтернету повинна забезпечуватися постійно, дозволяючи анонімну автентифікацію рішень анонімно, коли ідентифікація користувача не потрібна для надання послуги. Єдиний надійний європейський ідентифікатор, який може використовуватися як для державних, так і для приватних цифрових послуг, може сприяти цифровізації Єдиного ринку та забезпечити зручну можливість єдиного входу для тих, хто бажає ним користуватися. Попит на миттєві, безпечні та зручні операції в Інтернеті та еволюція кібер-ризиків обумовлюють інновації у рішеннях з цифрової ідентичності, де такі технології, як AI, IoT, аналітика, біометрія або мобільні телефони, перетинаються. Отже, ступінь, до якого ЄС спрямовується на інновації та регулювання цифрових ідентифікаційних даних, буде зміцнити технологічну автономію Європи та здатність європейського бізнесу конкурувати у глобальному масштабі.

Наявний досвід застосування eIDAS демонструє, що Регламент несе структурні недоліки, які обмежують його здатність ефективно підтримувати всеосяжну систему цифрових ідентифікаторів. Ці слабкі сторони пов'язані з принципом взаємного визнання за відсутності зобов'язання повідомляти національні схеми електронної ідентифікації та практичними труднощами в управлінні атрибутами (елементами персональної інформації), які можуть бути надійно розкриті третім особам, акцентом на громадськості сектора та відсутність можливості та / або стимулів для приватних сторін використовувати національні ІД. Ці та інші елементи, що обмежують ефективність eIDAS, є предметом постійної оцінки eIDAS і будуть представлені паралельно з переглядом.

Незважаючи на рамки eIDAS, національні правила щодо надання послуг цифрової ідентифікації залишаються фрагментованими або нерозробленими в усьому ЄС. Існуючі механізми добровільної координації між державами-членами, швидше за все, не забезпечать достатнього покращення. Європейська цифрова ідентичність, яка дозволяє простій, надійній, безпечній та доступній для всіх публічній системі громадянам ідентифікувати себе та обмінюватися інформацією, що стосується особистості, у цифровому просторі, може бути ефективно розроблена лише на рівні ЄС. Необхідність забезпечення транскордонного визнання системи цифрових ідентифікаційних даних у всіх державах-членах не може бути досягнута власними ініціативами держав-членів, які різняться за масштабами, амбіціями, технічною архітектурою, збереженими рішеннями та правовими механізмами, включаючи питання відповідальності та доступність використання приватним сектором. Індивідуальні рішення призводять до фрагментації Єдиного ринку та заохочують відвідування форуму постачальниками довірчих послуг, що призводить до нерівномірних пропозицій на шкоду діловим можливостям, пропонованим послугам та досвіду користувачів.

Фундаментальні зміни в загальному суспільному контексті передбачають перегляд Положення про eIDAS. Сюди входить різке збільшення використання нових технологій, таких як рішення на основі розподіленої книги, Інтернет речей, Штучний інтелект та біометрія, зміни в структурі ринку, коли мало хто з гравців зі значною ринковою владою все частіше виступає в ролі «воротарів» цифрової ідентичності, зміни у поведінці користувачів із збільшенням попиту на миттєву, зручну та безпечну ідентифікацію та розвиток законодавства ЄС про захист даних. Метою цієї ініціативи є, перш за все, забезпечити майбутню нормативно-правову базу для підтримки загальноєвропейської, простої, надійної та безпечної системи управління ідентифікаційними даними в цифровому просторі, що охоплює ідентифікацію, автентифікацію та надання атрибутів, облікових даних. та атестації. По-друге, ініціатива спрямована на створення універсального загальноєвропейського єдиного цифрового посвідчення особи.

Ці цілі можуть бути досягнуті шляхом капітального ремонту системи eIDAS, поширення eIDAS на приватний сектор, запровадження європейської цифрової ідентичності (EUid) на основі системи eIDAS або поєднання цих варіантів.

На сьогодні ЄС очікує на публікацію пропозицій до Регламенту eIDAS, тому більш широкий аналіз можна буде зробити лише після публікації.

Команда Мінцифри підготувала та опублікувала 24 лютого 2021 законопроєкт[13], що пришвидшить інтеграцію України до Єдиного цифрового ринку ЄС. Це наблизить українське законодавство до європейських вимог у сферах електронної ідентифікації та електронних довірчих послуг.

Проект акта розроблено відповідно до пункту 4 статті 1 Указу Президента України від 29 липня 2019 року № 558/2019 "Про деякі заходи щодо поліпшення доступу фізичних та юридичних осіб до електронних послуг", пункту 591 Плану законопроектної роботи Верховної Ради України на 2020 рік, затвердженого Постановою Верховної Ради України від 16 червня 2020 року № 689-IX, пункту 45 плану пріоритетних дій Уряду на 2020 рік, затвердженого розпорядженням Кабінету Міністрів України від 9 вересня 2020 року № 1133-р.

Метою прийняття акта є пришвидшення інтеграції України до Єдиного цифрового ринку Європейського Союзу, а також максимальне наближення положень національного законодавства до європейських вимог у сферах електронної ідентифікації та електронних довірчих послуг.[14]

Закон України "Про електронні довірчі послуги" спрямований на запровадження в Україні моделі та принципів надання електронних довірчих послуг, які застосовуються у Європейському Союзі, не руйнуючи систему взаємодії суб'єктів відносин у сфері електронного цифрового підпису, що склалась в Україні.

Водночас стрімкий розвиток інформаційних технологій, впровадження нових цифрових інструментів, спрямованих на спрощення доступу фізичних та юридичних осіб до електронних послуг, у тому числі транскордонних, а також нові виклики сьогодення, пов'язані з вжиттям заходів, спрямованих на запобігання поширенню на території України гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2, вимагають удосконалення нормативно-правового регулювання, зокрема у сферах електронної ідентифікації та електронних довірчих послуг.

У рамках домовленостей, досягнутих під час 22-го Саміту Україна – ЄС, Українська Сторона та Сторона Європейського Союзу розробили (а у січні 2021 року – погодили) спільний робочий план співпраці між Європейським Союзом та Україною щодо електронних довірчих послуг з перспективою укладення можливої угоди, яка повинна базуватися на наближенні до законодавства та стандартів Європейського Союзу (лист Представництва Європейського Союзу в Україні від 20 січня 2021 року). Пунктом 9 зазначеного спільного робочого плану передбачено прийняття змін до Закону України "Про електронні довірчі послуги" до 1 січня 2022 року.

З огляду на зазначене положення проекту акта спрямовані на забезпечення:

- максимального наближення положень національного законодавства до європейських вимог у сферах електронної ідентифікації та електронних довірчих послуг;

[13] *https://bit.ly/2Q8V2VZ*
[14] *https://bit.ly/3sDsdOh*

- використання фізичними та юридичними особами надійних, безпечних, альтернативних для одного рівня довіри, сучасних засобів електронної ідентифікації за принципом технологічної нейтральності;
- утворення системи надавачів послуг електронної ідентифікації, їх обліку та сприяння їх ефективній діяльності;
- підтвердження відповідності засобів електронної ідентифікації, що видаються в рамках схеми електронної ідентифікації, певному рівню довіри до засобів електронної ідентифікації;
- включення схем електронної ідентифікації до переліку схем електронної ідентифікації, які використовуються у сфері електронного урядування;
- можливості використання засобів електронної ідентифікації для автентифікації в інформаційних та інформаційно-телекомунікаційних системах, за допомогою яких надаються електронні послуги;
- забезпечення транскордонного визнання схем та засобів електронної ідентифікації, в тому числі тих, що базуються на кваліфікованих електронних довірчих послугах;
- удосконалення державного регулювання у сфері електронних довірчих послуг.

Державне регулювання у сфері електронної ідентифікації, що пропонується запровадити проектом акта, прискорить початок активного використання та подальший розвиток технологій електронної ідентифікації за паспортом громадянина України у формі картки, в яку імплантовано безконтактний електронний носій (CardID), мобільного електронного підпису (MobileID), банківської електронної ідентифікації (BankID), електронної ідентифікації за допомогою мобільного застосунку у смартфоні або планшеті (SmartID).

Висновки

З огляду на те, що попередні консультації щодо українського проекту закону ще тільки почались, а пропозиції щодо оновлення Регламенту eIDAS ще не опубліковані, а також з огляду на більш детальний аналіз регуляторного впливу і розрахунки, опубліковані на сайті Мінцифри, маємо декілька застережень.

Розрахунки щодо внесення змін до чинного Закону України «Про електронні довірчі послуги» не містять розрахунків для створення органу з оцінки відповідності.

На сьогодні наш Закон розповсюджує сферу на публічний і приватний сектор, і, як видно із аналізу майбутніх змін Регламенту eIDAS, він теж тепер буде діяти для обох секторів.

Найбільше занепокоєння у ЄС викликає питання електронної ідентифікації, Мінцифра при цьому пропонує врегульовувати зараз, не чекаючи змін, що є передчасним з огляду на вже затверджені плани для укладення угоди між ЄС та Україною.

Не була зроблена оцінка нормативних та технологічних вимог, старт якої запланований на квітень. Навіть якщо оновлення Регламенту eIDAS і буде опубліковне у квітні, знадобиться досить часу для вивчення експертами цього проекту. Хоча для оцінки, проект оновленого Регламенту eIDAS застосований бути не може, його можна лише взяти до відома.

Оновлення Регламенту eIDAS буде здійснюватись орієнтовно 1,5 – 2 роки до його ухвалення і набрання ним чинності. Тому, зупинятись на такий великий проміжок часу Україні не варто.

Підсумовуючи, слід запропонувати рухатись далі, не очікуючи оновлення Регламенту eIDAS, але все ж при підготовці проекту Закону до внесення його в Верховну Раду України на розгляд, слід все ж критично оглянути на предмет відповідності пропонованим змінам і провести додаткові консультації із стороною ЄС, оскільки така ситуація буде повторюваною щонайменше тричі – оновлюється NIS Директива, Директива 114, Директива, що стосується надання послуг у сфері інформаційного суспільства тощо. Слід також звернути увагу на невирішене питання імплементації саме Регламентів, які третя країна по відношенню до ЄС, не може прийняти і застосовувати так само, які країни ЄС. Здається, стороні ЄС для країн, що мають угоди про асоціацію, необхідно буде виробити спільну позицію і правила, що допоможуть здійснити мрію про вступ хоча б у цифровий ЄС

Поширення інформації як складова Єдиного цифрового ринку

Ольга Большакова

Як зазначається у Стратегії єдиного цифрового ринку для Європи[1] (далі – Стратегія), вона побудована на трьох стовпах, першим з яких є кращий доступ споживачів та підприємств до онлайн-товарів та послуг по всій Європі. При цьому, цифровий контент виокремлюється в Стратегії як особливий предмет регулювання, втім а ні його зміст, а ні правова природа не розкриваються. Аналіз пункту 2.4. Стратегії дозволяє лише зробити висновок, що цифровий контент може бути об'єктом авторського права, може використовуватися у «цифрових розвагах» та поширюватися засобами масової інформації, а також – що окремими видами послуг із надання цифрового контенту є «контент-послуги», зокрема «відео на замовлення», а також «тексти» і «дані», зокрема, ті, що використовуються у наукових дослідженнях.

При цьому Стратегія передбачила доцільність перегляду та оновлення змісту двох директив:

1. Директиви Ради 93/83/ЄЕС «Про координацію деяких положень авторського права і суміжних прав при застосуванні їх до супутникового мовлення і кабельної ретрансляції» від 27 вересня 1993 року[2], з метою оцінки необхідності розширення сфери її дії на онлайн-трансляції мовників та необхідності застосування подальших заходів для забезпечення розширеного трансграничного доступу до послуг мовників в Європі;
2. Директиви 2010/13/ЄС Європейського Парламенту та Ради від 10.03.2010 р. про координацію певних положень, встановлених законами, підзаконними актами та адміністративними положеннями у державах-членах стосовно надання аудіовізуальних медіа-послуг (Директива про аудіовізуальні медіа-послуги) (далі — Директива 2010/13/ЄС) – щодо розширення її сфери дії на нові послуги та гравців, які до цього моменту «не розглядаються як аудіовізуальні медіа-послуги».

Також окремий розділ Стратегії (пункт 3.3.) присвячений створенню нормативного середовища для широкого кола онлайн-платформ (серед яких є платформи, що поширюють аудіовізуальний контент), які стрімко зросли та «кинули виклик традиційними бізнес-моделям», «...що викликало ряд занепокоєнь щодо зростаючої ринкової сили окремих платформ».

Втім, найважливіше питання щодо регулювання цифрового контенту поставлене у п. 3.3.2. Стратегії. Фактично, саме тоді були закладені підвалини перегляду принципу, який лежав в основі розвитку Інтернету в Європі: принципу, відповідно до якого провайдери Інтернет-посередників не повинні нести відповідальність за контент, який вони передають, зберігають або розміщують, якщо вони діють виключно пасивним чином. Посилаючись на суспільні дебати щодо доцільності підвищення загального рівня захисту від незаконних матеріалів в Інтернеті, Стратегія поставила завдання проаналізувати необхідність запровадження нових заходів з боротьби із незаконним контентом в Інтернеті та підвищення відповідальності посередників при управлінні їхніми мережами та системами.

Таким чином, хоча Стратегія і включила до «цифрового контенту» такі види інформації як «тексти» та «дані», удосконалення правового регулювання нею передбачалось перш за все у сфері поширення аудіовізуальної інформації. Це повністю відповідає історії розвитку європейського законодавства у сфері медіа, яка фактично розпочалась у 1989 році із прийняття

[1] *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52015DC0192*

[2] *https://zakon.rada.gov.ua/laws/show/994_433#Text*

Європейської конвенції про транскордонне телебачення (далі – Конвенція). Ця Конвенція була ратифікована Україною наприкінці 2008 року і на сьогодні залишається чинною для України, так саме як і для інших країн, які є сторонами Конвенції, але не є членами Європейського союзу. Що ж до країн-членів ЄС, то для них майже одночасно з Конвенцією набула чинності Директива 89/552/ЄЕС Європейського Парламенту та Ради від 03.10.1989 р., яка значною мірою дублювала положення Конвенції та фактично була скасована Директивою 2010/13/ЄС.

Таким чином, од самого початку європейське законодавство у сфері медіа поширювалось виключно на телебачення, тоді як регулювання радіо та преси на загальноєвропейському рівні відсутнє, хоча ці медіа також можуть мати транскордонне поширення. Можна очікувати, що такого регулювання і не відбудеться, обмеження поширення інформації цими традиційними медіа, а також – аналогічними онлайн-ресурсами, залишиться в межах цивільного та кримінального законодавства, тобто таких загальних заборон, як заборона поширення дифамації, закликів до насильства, дискримінаційних висловлювань, дитячої порнографії тощо. На користь такого прогнозу свідчать і зміни, внесені до Директиви 2010/13/ЄС згідно з Директивою (єс) 2018/1808 Європейського Парламенту і Ради від 14 листопада 2018 року, якими її дія була поширена на послуги платформ спільного доступу до відео, але не на радіо чи пресу і Інтернет: *«Послуги платформ спільного доступу до відео забезпечують аудіовізуальний контент, доступ до якого дедалі активніше здійснюється широкою громадськістю, особливо молоддю. ...Такі соціальні медіа-послуги потрібно включити до сфери застосування Директиви 2010/13/ЄС, оскільки вони конкурують за ту ж саму аудиторію та надходження, що й аудіовізуальні медіа-послуги. Крім того, вони також здійснюють значний вплив у тому, що полегшують можливість для користувачів формувати та впливати на думки інших користувачів. Таким чином, з метою захисту неповнолітніх від шкідливого контенту, а всіх громадян – від підбурювання до насильства, ненависті та тероризму, ці послуги мають охоплюватися Директивою 2010/13/ЄС тією мірою, наскільки вони відповідають визначенню послуги платформи спільного доступу до відео»*.

Слід відзначити, що ці твердження є певною мірою звуженим тлумаченням ситуації. Якщо подивитися на конкуренцію в сфері медіа, або навіть ще ширше – в сфері поширення інформації та розваг, то очевидно, що аудіовізуальні медіа конкурують за одну і ту ж саме аудиторію, що і радіо та преса, в тому числі – онлайн, тоді як платформи спільного доступу до відео значною мірою конкурують у сфері розваг. Втім, повна картина складається з ще кількох передумов: по-перше, регулювання радіо та преси в країнах усталеної демократії завжди було і залишається на сьогодні значно м'якішим, ніж регулювання телебачення, імовірно, саме тому так і не було уніфіковано вимоги до цих видів медіа на загальноєвропейському рівні; по-друге, контент, що поширюється радіо в цілому є більш безпечним для суспільства, ніж контент, який поширюється телебаченням, крім того – наявність відеоряду створює більший вплив на сприйняття інформації аудиторією; по-третє, будь-якій владі значно легше контролювати кількох потужних гравців на ринку платформ спільного доступу до відео, ніж десятки, чи то – сотні тисяч текстових видань, ефективність контролю – тобто співвідношення витрат на його здійснення із досягнутим результатом буде істотно вищою; і, нарешті, вчетверте – запропоновані механізми контролю за контентом покладають витрати саме на індустрію, про що реалістично досягти домовленості з потужними міжнародними компаніями, але які викличуть величезний спротив з боку маленьких видань.

Проект Закону про медіа: вся галузь та супутні ринки в одному законі

Натомість, в Україні, починаючи з перших кроків розвитку галузевого законодавства у сфері телерадіомовлення, тобто з першої редакції Закону України «Про телебачення і радіомовлення» від 1994 року, обидва види медіа регулювались майже однаково.

З 2006 року до сфери дії закону включена також діяльність провайдерів програмної послуги, які фактично всі були операторами телекомунікацій, що надавали послуги із доступу до кабельного телебачення. Такі зміни стали наслідком тривалого та жорсткого конфлікту, започаткованого розвитком кабельних мереж та руйнуванням систем колективного прийому ефірного телебачення, що привело до контролю операторів кабельних мереж за доступом до аудиторії до телеканалів і, навпаки, доступом телеканалів до своєї аудиторії. Користуючись таким галузевим «монопольним положенням», оператори кабельних мереж вимагали від телеканалів значної оплати за трансляцію їх програм. Це суперечило інтересам телеканалів, які не лише віддавали власний програмний продукт безоплатно, але і були змушені двічі платити за його поширення – спочатку за ефірне, а потім – за кабельне. Тоді як оператори кабельних мереж отримували оплату і від телеканалів, і від абонентів за продаж їм чужого продукту. Крім того, така ситуація шкодила інтересам держави, оскільки рішення про те, які програми зможе дивитися аудиторія, приймав не державний регулятор Національна рада України з питань телебачення і радіомовлення, а приватні особи – оператори кабельних мереж. Доволі часто вони приймали такі рішення, виходячи не лише з комерційних, але і з політичних міркувань своїх власників або місцевої влади, від дозвільних рішень якої залежить розвиток кабельних мереж. У 2005 році ситуація стала настільки загрозливою, що телеіндустрія і регулятор обмірковували можливість відновити системи колективного прийому ефірного телебачення – оскільки в кабельні мережі транслювали переважно російські канали.

Тому в редакції Закону України «Про телебачення і радіомовлення» від 2006 року було введено окремий вид діяльності – надання програмної послуги, який підлягав ліцензуванню Національною радою України з питань телебачення і радіомовлення, а також обов'язок надання доступу до універсальної програмної послуги (УПП), яка складалась із українських ефірних телеканалів. Це дозволило врегулювати ситуацію, оскільки на той момент діяльність без ліцензії була кримінальним злочином, отже, оператори кабельних мереж були змушені дотримуватись закону під загрозою кримінальної відповідальності. На сьогодні це діяння декриміналізоване, втім традиція поширення УПП вже склалась і практично не порушується. Крім того, заборона поширення російських телеканалів та розвиток захисту авторського і суміжних прав призвів до того, що в 2016 році потужні комерційні загальнонаціональні телеканали самі відмовились від того, щоб їх програми входили до складу УПП, і наразі отримують від провайдерів програмної послуги значну оплату за право продавати їх програми абонентам.

Поза тим, відносини між державним регулятором, телеканалами та операторами кабельних мереж залишаються напруженими, тому в проекті Закону України «Про медіа», до сфері дії відносяться не лише телебачення та радіо, але і провайдери аудіовізуальних сервісів, які фактично є тими ж самими операторами телекомунікацій/провайдерами програмних послуг. Оскільки цього року вже з'являються повідомлення про погіршення умов співпраці між операторами кабельних мереж та місцевими кабельними телеканалами, які не входять до складу УПП, можна прогнозувати, що регулювання діяльності операторів кабельних мереж буде залишатися в медійному законодавстві як мінімум ще протягом дії наступної редакції закону.

Крім того, окремим суб'єктом є постачальники електронних комунікаційних послуг для потреб мовлення з використанням радіочастотного ресурсу. Це також «історичний спадок», зумовлений двома факторами:

1. розподіл радіочастотного ресурсу, який використовується для цілей телебачення і радіомовлення, належить до компетенції Національної ради України з питань телебачення і радіомовлення од самого початку її створення;
2. на початку розвитку цифрового телебачення Національна рада видала ліцензії на експериментальне цифрове телебачення чотирьом компаніям, які одночасно були і мовниками, і операторами телекомунікацій, згодом, експериментальні ліцензії були замінені на

ліцензії провайдерів; до всіх цих ліцензій увійшло право на використання відповідного радіочастотного ресурсу. На підставі цього прецеденту, було видано спочатку ліцензію першому загальнонаціональному провайдеру ТОВ «УЦТМ», а потім - ТОВ «Зеонбуд» - фактично монопольному провайдеру і оператору цифрового ефірного телебачення в Україні. Всі ці ліцензії були видані без конкурсу і без жодних умов щодо якості надання послуг. Це започаткувало затяжний конфлікт з одного боку, між телеканалами і ТОВ «Зеонбуд» щодо тарифів надання послуги, а з іншого – між державою і ТОВ «Зеонбуд» щодо якості покриття території країни сигналом цифрового телебачення, а також – щодо впливу держави на канали, що транслюються в мережі. На цей момент вже вичерпані всі можливості щодо остаточного врегулювання цього конфлікту, тому внесення «постачальників електронних комунікаційних послуг для потреб мовлення з використанням радіочастотного ресурсу» до проекту Закону про медіа є чи не останньою спробою держави повернути собі контроль за цифровим телебаченням.

Слід зазначити, що розширення сфери регулювання в проекті Закону про медіа не суперечить сучасним тенденціям розширення сфери дії самої Директиви на послуги платформ спільного доступу до відео. В процесі підготовки проекту Закону України «Про медіа» українська сторона провела низку консультацій з європейськими експертами, які підтвердили, що більш широка сфера дії закону, тобто включення до неї радіо, преси, провайдерів програмної послуги тощо, не суперечить зобов'язанням України перед Європейським союзом щодо імплементації директиви та законодавству Європейського союзу в цілому.

Також, наразі до сфери дії проекту Закону про медіа входить преса, втім дебати щодо цього продовжуються і є імовірність того, що друковані медіа залишаться в межах регулювання окремого закону.

Мультистейкходеризм як підхід до законотворчості: позитивний приклад негативного відбору

З огляду на викладене вище, очевидно, що проект Закону про медіа зачіпає інтереси величезної кількості категорій суб'єктів діяльності у сфері медіа (власне, телекомпаній, радіо, преси, онлайн медіа, операторів телекомунікацій тощо), а також – фактично, кожного громадянина, при чому і як дописувача соціальних мереж чи відео-блогера, і як споживача медіа інформації, і як учасника політичних процесів (політика, громадського активіста тощо), вплив медіа на які залишається надзвичайно високим. Це призводить до того, що кожний громадянин України має власні, інколи – взаємовиключні інтереси, на які впливає проект Закону про медіа – наприклад, як автор відео-блогу, він прагне зменшення регулювання, а як батько малолітньої дитини – навпаки, максимально безпечних онлайн медіа.

Це призвело до того, що робота над імплементацією Директиви триває в Україні з 2011 року, коли її ініціювала європейська сторона. Перша робоча група, яка працювала з 2012 по 2014 роки, складалась із представників всіх стейкхолдерів (крім, представників аудиторії від імені яких виступали представники громадських організацій у сфері медіа та представники Національної ради України з питань телебачення і радіомовлення). Робоча група не змогла знайти компроміс щодо низки ключових питань, зокрема – щодо складу УПП, тому проект так і не був узгоджений. Народний депутат Олена Бондаренко, яка без згоди учасників робочої групи зареєструвала проміжну версію проекту, не змогла винести його на порядок денний, тому він був знятий з розгляду парламенту наступного скликання. Цей приклад мультистейкхолдеризму, реалізованого шляхом широкої участі всіх зацікавлених сторін, але без належної медіації процесу, засвідчив, що він є ефективним лише в сенсі негативного відбору – тобто недопущення прийняття законів, в яких не досягнуто балансу інтересів.

З урахуванням досвіду попередньої роботи, у наступному скликанні парламенту Комітет з свободи слова та інформаційної політики вирішив не створювати робочу групу з широким представництвом, а доручити доопрацювання проекту кільком експертам. На результат їх роботи вплинуло кілька факторів – ці експерти належали до громадських організацій у сфері медіа, які мали дуже активну громадянську позицію, період роботи над проектом співпав із гострою фазою інформаційної війни, остаточне рішення щодо змісту проекту приймали народні депутати, які в першу чергу були зосереджені на забезпеченні інформаційної безпеки України. У сукупності це призвело до того, що обмеження прав суб'єктів у сфері медіа в проекті виявилось настільки надмірним, що викликало активний спротив з боку індустрії. Крім того, автори проекту недооцінили навантаження на експертів, які не змогли забезпечити належну юридичну техніку опрацювання самого тексту. В результаті, автори проекту були змушені розпочати його широке обговорення та пошук компромісів, але не досягли в цьому успіху. Проект був зареєстрований головою Комітету Вікторією Сюмар переважно для активізації дискусії з індустрією, про що вона повідомляла публічно, але він так і не був поданий на заміну після узгодження тексту, і, відповідно, не потрапив до порядку денного парламенту. Фактично, висновок, який можна зробити з цього досвіду – це те, що неможливо уникнути широкого обговорення при прийнятті комплексного галузевого законопроекту в умовах демократичної роботи парламенту. Досягнення згоди по ключових питання є доцільним на першому етапі роботи над концепцією закону, оскільки на більш пізніх етапах воно призводить до необхідності переробляти значну частину тексту.

Парламент наступного скликання також намагався врахувати досвід попередньої роботи і створив робочу групу, до якої увійшли як представники індустрії, так і представники громадськості. Втім, формування цієї робочої групи відбувалось не прозоро, рішення приймали автори на власний розсуд, виходячи із прагнення доопрацювати текст і прийняти закон максимально швидко. Їм дійсно вдалось зменшити обсяг дебатів всередині робочої групи, що прискорило її роботу, але, натомість, автори проекту знову недооцінили складності завдання, отже робота тривала значно довше, ніж вони очікували. Тим більше, що на цьому етапі перед робочою групою було поставлено завдання включити у сферу регулювання пресу, яка традиційно регулюється в Україні окремим законом, а відповідно – і всі текстові онлайн-ресурси. Імовірно, ця тактика обрання найбільш конструктивних та поміркованих представників серед значної кількості стейкхолдерів без дотримання чітких процедур їх делегування, могла б спрацювати, якби проект був підготовлений швидше. Втім, просування проекту розпочалось із тривалих та переважно політичних дискусій всередині Комітету із гуманітарної та інформаційної політики, які широко висвітлювались в медіа і ініціювали надзвичайно емоційну громадську кампанію проти прийняття проекту. Невдовзі Комітет розпочав галузеві обговорення проекту, а потім і обговорення з громадськістю. За результатами цих обговорень робоча група доопрацювала проект, який був внесений до парламенту 2 липня 2020 року[3].

Втім, до вже доопрацьованого проекту знову було подано численні та змістовні зауваження, як від громадськості[4], так і від індустрії[5], отже, можна очікувати, що текст буде поданий на заміну ще як мінімум один раз.

Зауваження громадськості надійшли від низки організацій, проте вони не суперечать одні одним, тому їх можна згрупувати наступним чином:

1. проект передбачає поширення повноважень Національної ради з питань телебачення і радіомовлення на контроль за здійсненням будь-якої інформаційної діяльності, включаючи

[3] *http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69353*

[4] *https://bit.ly/3xaaul9*

[5] *https://bit.ly/2QHv1g1*

розповсюдження інформації друкованими ЗМІ, незареєстрованими онлайн-медіа, блогерами і дописувачами соціальних мереж – на думку громадськості це не відповідає європейським підходам, втім, таке поширення підтримує державний регулятор та традиційні аудіовізуальні медіа, які вважають, що ситуація за якої вони підлягають жорсткому державному регулюванню та контролю, а онлайн медіа абсолютно вільні від нього, є незбалансованою та несправедливою;

2. проект містить декларативні норми щодо дотримання професійних стандартів журналістики – хоча проект Закону України «Про медіа» є суто галузевим і його автори неодноразово наголошували на тому, що вони не мають намірів поширювати його на діяльність журналістів, медіа громадськість наполягає на включенні положень про журналістську етику та саморегулювання;
3. натомість, інститут спільного регулювання, що впроваджується у проекті, не має чіткого визначення повноважень його учасників і розділення повноважень між ними – це зауваження також підтримують представники індустрії;
4. у проекті зберігається застарілий та неефективний механізм запобігання концентрації медіа в руках одного власника.

Зауваження великої індустрії висловили дві великі медіагрупи – «1+1 медіа» та «Медіа Група Україна». Це свідчить про непередбачуваність процесу доопрацювання та прийняття проекту, оскільки представники обох груп брали участь у розробці проекту на всіх етапах (тобто, і під час підготовки першої редакції, і під час доопрацювання), проте їх спільна позиція виявилась досить критичною – індустрія фактично наполягає на заміні тексту перед першим читанням. Ці зауваження також можна згрупувати:

1. у проекті розширено повноваження регулятора, зокрема, допускається суб'єктивна оцінка наявності контентних порушень, запроваджені нові санкції, введено повноваження по отриманню документів та інформації, які прямо не стосуються можливих порушень суб'єктів у сфері медіа, а також зафіксовано можливість регулятора самостійно встановлювати строки надання таких документів, порядок прийняття Національною радою нормативно-правових актів не містить жодних запобіжників;
2. положення проекту щодо створення органу спільного регулювання створюють ризики що він не буде відображати реальну позицію ринку;
3. підстави застосування санкцій, які передбачені проектом, не враховують специфіку та умови діяльності окремих суб'єктів, тяжкість порушень і тому є дискримінаційними;
4. проект створює нерівність українських та іноземних суб'єктів у сфері медіа, до мовлення або послуг яких є доступ на території України.

Таким чином, індустрію непокоїть посилення контролю з боку регулятора, тоді як громадськість вважає його недостатнім. Натомість, громадськість занепокоєна поширенням контролю на онлайн-медіа та пресу, тоді як індустрія вважає, що це збалансує регулювання конкуруючих між собою галузей. І, на жаль, очевидно, що обидві сторони не задоволені запропонованим у проекті механізмом спільного регулювання, який, власне і покликаний запровадити мультистейкхолдерізм в галузі медіа.

Досвід мультистейкхолдеризму на цьому етапі знову продемонстрував, що без медіації, яка дозволить досягти балансу інтересів всіх сторін, та без чітко визначеної процедури прийняття рішень, яка передбачатиме фіксацію домовленостей та межі їх перегляду, процес підготовки проекту може тривати надзвичайно довго.

Спільне регулювання як форма мультистейкхолдерізму

Директива 2010/13/ЄС передбачає два підходи до дерегулювання діяльності медіа:

1. **Саморегулювання** – це різновид добровільної ініціативи, яка дає змогу суб'єктам господарювання, соціальним партнерам, неурядовим організаціям та об'єднанням ухвалювати між собою та для себе спільні практичні рекомендації. Вони несуть відповідальність за розроблення, контроль і забезпечення виконання цих практичних рекомендацій. Державам-учасницям, згідно зі своїми різними правовими традиціями, слід визнавати роль, яку ефективне саморегулювання може відігравати, доповнюючи наявні законодавчі, судові та адміністративні механізми, а також його корисний внесок у виконання завдань, поставлених Директивою 2010/13/ЄС. Хоча саморегулювання може становити доповняльний метод в імплементації певних положень Директиви 2010/13/ЄС, воно, однак, не має замінювати собою обов'язки національного законодавця».
2. **Співрегулювання**, яке у своїй мінімальній формі забезпечує правовий зв'язок між саморегулюванням і національним законодавцем згідно з правовими традиціями Держав-учасниць. У співрегулюванні регуляторну роль розділено між зацікавленими сторонами та урядом або національними регуляторними відомствами чи органами. Функція відповідних державних органів включає до себе визнання системи співрегулювання, проведення перевірок її процесів і фінансування цієї системи. Співрегулювання має уможливлювати державне втручання у разі невиконання поставлених перед ним завдань. Без шкоди офіційним зобов'язанням Держав-учасниць щодо транспонування, Директива 2010/13/ЄС заохочує використання само- та співрегулювання. Це не має зобов'язувати Держав-учасниць як встановлювати режими само- та (або) співрегулювання, так і зривати чи ставити під загрозу наявні ініціативи зі співрегулювання, що вже існують і ефективно функціонують у Державах-учасницях.

Відповідно до Міжвідомчої угоди 2003/С 321/01 Європейського парламенту, Ради Європейського Союзу про вдосконалення законотворчої діяльності 2003 р.[6]: Спільне регулювання означає механізм, за допомогою якого у законодавчому акті досягнення цілей, визначених законодавчим органом, доручається сторонам, які визнані в цій галузі (таким як економічні оператори, соціальні партнери, неурядові організації або асоціації). Цей механізм може бути використаний на основі критеріїв, визначених у законодавчому акті, з тим, щоб забезпечити можливість адаптації законодавства до відповідних проблем та інтересів галузей, зменшити законодавче навантаження, зосередившись на основних аспектах, та спираючись на досвід зацікавлених сторін.

Таким чином, спільне регулювання з одного боку відповідає європейським підходам до регулювання окремих галузей, а з іншого – допускає застосування цілої низки різних форм в процесі його імплементації до національного законодавства.

В Україні перша спроба запровадження системи спільного регулювання була здійснена у 2012 році за підтримки ОБСЄ, коли експерти запропонували робочій групі у складі представників індустрії та працівників Національної ради України з питань телебачення і радіомовлення (далі – Національна рада) низку варіантів організації діяльності органу співрегулювання. На той момент, сторони не домовились, оскільки Національна рада прагнула зберегти за собою право прийняття остаточного рішення, яке може суперечити експертному висновку, а індустрія не бачила сенсу фінансувати експертний орган, рішення якого не будуть мати істотної ваги для регулятора.

[6] *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003Q1231%2801%29*

У 2014 році загострення інформаційної війни з пропагандою держави-агресора, в тому числі – в медіа, які зареєстровані в Україні, призвели до посилення регулювання медіа контенту в цілому, і, зокрема, на телебаченні і радіо. Національна рада, яка до 2014 року практично не застосовувала санкції за незаконний контент, була змушена приймати рішення, які викликали значний суспільний резонанс. З огляду на складну політичну ситуацію та обмежений бюджет, регулятор звертався до низки експертних організацій з метою отримання підтримки для своїх рішень. Такий підхід викликав стурбованість в індустрії, оскільки організації, що надавали експертні висновки, діяли без жодних методик експертизи, без визначення вимог до експертів та не несли жодної відповідальності за зміст своїх експертних висновків.

У 2015 році Національна асоціація медіа (колишня – Незалежна асоціація телерадіомовників) та компанія Старлайтмедіа створили ініціативну групу із запровадження системи спільного регулювання у сфері телерадіомовлення. Концепція, яку ініціативна група представила у 2016 році, передбачала, зокрема, внесення змін до галузевого законодавства, отже відповідні норми були запропоновані до проекту закону «Про аудіовізуальні медіа-сервіси», яка була актуальною на той момент. Водночас, відбулась широка просвітницька компанія та низка громадських та індустріальних обговорень.

Спільне регулювання є окремою формою регулювання, яке поєднує в собі ознаки:

1. саморегулювання в частині прийняття рішень щодо специфічних галузевих питань експертним органом, створеним з висококваліфікованих фахівців у сфері медіа та суміжних сферах;
2. державного регулювання в частині застосування державного примусу для забезпечення виконання рішень експертного органу.

Слід зазначити, що для медіа галузі, яка звикла до системи журналістського саморегулювання, спрямованою на свободи висловлювань, спільне регулювання має як переваги, так і недоліки.

З одного боку, орган спільного регулювання має чітко визначений та погоджений сторонами статус, а не є однією із багатьох схожих організацій, серед яких Національна рада може на власний розсуд обирати ту, яка відповідає її поточним інтересам, оскільки всі вони мають однаково суперечливий склад учасників, процедури та експертів. З іншого боку, створення органу спільного регулювання є набагато складнішим, ніж заснування саморегуляторної громадської чи індустріальної ініціативи, оскільки установчі документи органу спільного регулювання потребують згоди Національної ради по всіх ключових питаннях, навіть, у разі, якщо вимоги до них значною мірою будуть визначені в законі.

З одного боку, рішення органу спільного регулювання приймаються експертами відповідно до регламенту, яким може бути визначено, зокрема, кількість експертів, порядок прийняття колегіального рішення, відповідальність експертів, а також - вимоги до аналізу контенту в повному обсязі, зокрема, у співставленні з іншим контентом у відповідному циклі матеріалів, отримання пояснень від медіа тощо. Регламентні процедури мають унеможливити прийняття суб'єктивних або кон'юнктурних рішень. З іншого боку, це означає, що орган спільного регулювання при прийнятті рішень не буде ставати на бік індустрії, якщо порушення дійсно мало місце, отже – це захист лише від безпідставних санкцій.

З одного боку, наявність органу спільного регулювання із визначеними процедурами та вимогами до експертів, має припинити практику звернення Національної ради до організацій, які надають експертні висновки нижчої якості. З іншого боку, погодження експертів всіма учасниками від індустрії та Національною радою, скоріше за все призведе до обрання відо-

мих спеціалістів, послуги яких коштують дорожче, що істотно збільшить вартість проекту, порівняно із саморегуляторним органом, до якого учасники зазвичай делегуються індустрією та громадськістю і працюють безкоштовно.

Спільне регулювання у сфері медіа – це поєднання функцій та засобів державного регулювання та галузевого саморегулювання з метою забезпечення участі суб'єктів у сфері медіа у розробці та визначенні вимог до змісту інформації, яка поширюється медіа, та недопущення цензури і зловживання свободою слова.

Предметом спільного регулювання є визначення вимог до поширення інформації, для якої законодавством передбачено регулювання змісту, шляхом прийняття кодексів (правил) створення та поширення такої інформації. При цьому суб'єкти у сфері медіа добровільно беруть на себе обов'язок дотримуватись цих вимог, а Національна рада визнає, що ці вимоги є достатніми для забезпечення суспільних інтересів.

Слід зазначити, що до визначення критеріїв віднесення інформації до такої, яку заборонено поширювати на території України (зокрема, заклики до насильства, пропаганда комунізму, інформація, що може завдати значну шкоду фізичному, психічному або моральному розвитку дітей), які відносяться до предмету спільного регулювання в європейській практиці, в процесі роботи над проектом було додано також критерії віднесення осіб до певних категорій, що є новелою українського підходу, зокрема:

1. встановлення критеріїв віднесення осіб, що поширюють онлайн-медіа без здійснення добровільної реєстрації, до суб'єктів у сфері онлайн-медіа;
2. визначення критеріїв віднесення лінійних медіа до тематичних та обсяги національного та європейського продукту для таких медіа;
3. розподіл дітей на вікові категорії та критерії класифікації програм (крім фільмів) за віковими категоріями аудиторії, на яку вони розраховані.

Також до предмету органу спільного регулювання були віднесені затвердження ескізів та вимог до демонстрування графічних попереджень (символів) та вимоги до оголошення звукових попереджень, та визначення порядку віднесення суб'єктом у сфері медіа інформації до відповідних вікових категорій дітей та обрання відповідних попереджень (символів). В цілому, це відповідає європейській практиці затвердження кодексів органів спільного регулювання, до яких наведені вище положення можуть увійти як складова або додаток. Крім того, органу спільного регулювання делеговане затвердження правил мовлення у дні пам'яті.

Проект передбачає низку запобіжників, які мають гарантувати, що процедура створення органу спільного регулювання не буде штучно гальмуватися Національною радою або частиною індустрії.

Також, проект передбачає вимоги до збалансованого представництва всіх видів медіа в органі спільного регулювання, втім не містить чітких кількісних критеріїв такого представництва: «Загальні збори органу спільного регулювання призначають правління, до складу якого мають бути включені представники від всіх видів суб'єктів у сфері медіа, що є членами органу спільного регулювання. При призначенні складу правління має бути врахований принцип рівності представництва інтересів всіх видів суб'єктів у сфері медіа, що є членами органу спільного регулювання». Саме ці положення викликають наразі зауваження як з боку громадськості (яка взагалі не представлена), так і індустрії (яка усвідомлює, що різні види медіа мають різний ступінь зацікавленості в роботі органу спільного регулювання, а відповідно – різну готовність брати участь у фінансуванні його діяльності).

Необхідно зазначити, що наразі в Україні є ще одна законодавча ініціатива проєкт Закону України «Про саморегулювання господарської та професійної діяльності» № 4221 від 15.10.2020 р. (далі – Проєкт №4221), який за оцінкою медіа громадськості, що створює штучні перешкоди для розвитку саморегулювання в Україні та може сприяти розвитку корупції. Зокрема, статтею 20 Проєкту №4221 фактично запроваджується **спільне регулювання** в Україні, оскільки вона передбачає можливість делегування саморегулівним організаціям повноважень державних органів.

Втім, для досягнення суспільно важливих цілей, правові засади системи спільного регулювання мають дуже чітко визначати обсяг делегованих повноважень (тобто, чи має право державний орган відступити від рішення органу спільного регулювання у разі незгоди з ним), підходи до внутрішнього контролю (тобто способи перешкоджання недобросовісній конкуренції в межах відповідної галузі із використанням органів спільного регулювання) та порядок фінансування (оскільки система спільного регулювання передбачає високі витрати з боку галузі). Жодне з цих питань у Проєкті №4221 не вирішене. Більше того, аналіз її положень свідчить, що вона не лише не розширює можливості саморегулювання порівняно із чинним законодавством, а навпаки ускладнює процес запровадження делегування повноважень (тобто, спільного регулювання).

По-перше, частина 1 статті 20 передбачає, що для делегування кожних конкретних повноважень в кожній галузі має бути спеціальній закон, тобто так само, як і зараз. Проте, частина 3 цієї ж статті передбачає, що Кабінетом Міністрів України має бути прийнятий ще і загальний порядок делегування повноважень, який наразі законодавство не вимагає. Крім того, частина 2 цієї ж статті передбачає, що повноваження можуть бути делеговані не будь-якій організації, а лише такій, яка «об'єднує не менше 25 відсотків від загальної кількості суб'єктів господарської або професійної діяльності у певній сфері (галузі), або певного виду (видів)», хоча ніде більше в Проєкті не передбачається окремого статусу **репрезентативної саморегулівної організації**. Також незрозуміло, як буде підраховуватись загальна кількість суб'єктів діяльності, яка не ліцензується і не реєструється, наприклад, у господарській діяльності у сфері маркетингу або професійній діяльності у сфері журналістики.

Також, хоча саморегулівна організація наче має право вимагати делегування їй повноважень шляхом подання заяви, їй може бути відмовлено у разі «виявлення недостовірних відомостей у поданих документах». При цьому перелік документів Проєктом не визначений, очевидно, що він включатиме реєстр членів, який має підтвердити репрезентативність саморегулівної організації. І очевидно, що велика організація, до складу якої входить багато фізичних осіб, не зможе забезпечувати постійну перевірку та оновлення реєстру. Отже, державні органи завжди зможуть відмовити у делегуванні повноважень будь-якій саморегулівній організації.

Натомість, вони так само зможуть будь-яку організацію визнати належною і не лише делегувати їй повноваження, але і **зобов'язати всіх учасників ринку у відповідній галузі стати її членами**, відповідно до частини 3 статті 13 Проєкту: *«Обов'язковість членства всіх суб'єктів господарської або професійної діяльності у певній сфері (галузі) або певного виду (видів) в одній саморегулівній організації чи принаймні одній саморегулівній організації може встановлюватися законом у разі покладання ним на таку саморегулівну організацію повноважень з контролю та/або регулювання відповідної господарської або професійної діяльності та/або* ***в разі, коли законом передбачено можливість делегування таким організаціям відповідних повноважень****»*.

Таким чином, положення статті 20 Проекту створюють умови для корупції, зокрема, для утворення державними органами «кишенькових» саморегулівних організацій та примушення всіх учасників ринку до вступу до цих організацій, до їх фінансування та до виконання їх внутріш-

ніх правил. Реальність цього ризику підтверджується тим, що схема отримання державними посадовцями хабарів від підприємців через внески до їх «кишенькових» організацій була широко поширеною в Україні наприкінці 90-х років.

На жаль, положення Проекту Закону про медіа також містять положення, які потенційно можуть заблокувати запровадження інституту спільного регулювання, а саме необов'язковість його висновків для Національної ради: «Висновки експертних колегій органу спільного регулювання мають рекомендаційний характер. Національна рада враховує ці висновки при прийнятті рішень або відхиляє із обґрунтуванням причин відхилення». Хоча на певному етапі індустрія погодилась із таким підходом, сподіваючись на те, що Національна рада не стане відхиляти висновки, які підготовлені із належною якістю, але після початку роботи органу спільного регулювання кожний відхилений висновок фактично може стати причиною зупинення фінансування з боку індустрії, а отже – зупинення спільного регулювання в цілому.

Поза тим, включення до проекту Закону про медіа положень про спільне регулювання є значним кроком до запровадження європейських підходів до регулювання медіа галузі.

Мультистейкхолдеризм з динамічністю законотворчого процесу та стабільністю прийнятих рішень

Виходячи з викладеного вище, стає зрозумілим, що колегіальність прийняття рішень, яка є мінімальною умовою балансу інтересів всіх зацікавлених осіб, створює низку викликів, а саме:

1. прозорість процедур делегування представників зацікавлених сторін до колегіального органу (постійного або тимчасового, на кшталт робочої групи): надання можливості всім зацікавленим особам делегувати своїх представників або взяти участь в обранні одного представника від низки зацікавлених осіб, інтереси яких переважно співпадають. Хорошим прикладом вирішення схожої проблеми є процедури, передбачені статтею 8 Закону України «Про Суспільне телебачення і радіомовлення України»[7], яка визначає порядок проведення конференцій громадських організацій для обрання їх представників до наглядової ради НСТУ. Слід зазначити, що така процедура є доволі складною, якщо вона проводиться серед значної кількості зацікавлених громадських організацій, проте довід проведення таких конференцій свідчить про її реалістичність та результативність. Крім того, проведення подібного обрання має бути значно легшим за умови, що кількість зацікавлених осіб є меншою. До прикладу, на сьогодні є близько десяти організацій, які тією чи іншою мірою представляють інтереси операторів кабельних мереж в Україні і зазвичай, якщо створюється робоча група з обмеженою кількістю осіб, ці організації самі визначають одного чи двох представників від своєї галузі;
2. забезпечення адекватності представників зацікавлених сторін стосовно їх професіоналізму, досвіду, відсутності конфлікту інтересів тощо – чинне законодавство містить багато прикладів визначення таких вимог, зокрема, це вимоги до громадянства, освіти, досвіду роботи на певних посадах тощо. Доцільно утриматись від визначення вимог до авторитетності представників, оскільки така авторитетність автоматично витікає із того факту, що вони уповноважені певною стороною;
3. процедура делегування представників має передбачати чітке визначення їх повноважень, тобто обсяг делегованих їм прав щодо прийняття рішень в колегіальному органі. В окремих випадках обсяг повноважень може визначатись статутними документами особи, яка делегує представника, а також – рішенням про його делегування;

[7] *https://zakon.rada.gov.ua/laws/show/1227-18#Text*

4. забезпечення динаміки прийняття рішень колегіальним органом, який включає представників сторін, інтереси яких суперечать один одному – дискусії в межах робочих груп можуть завершуватись прийняттям рішень шляхом голосування, яке має бути доповненим правом всіх осіб, які не підтримали рішення, долучити до нього їхні окремі думки. Також, якщо остаточне рішення приймає інший орган, наприклад, парламент, робоча група може фіксувати всі пропозиції з питань, по яких не було значної переваги на користь однієї із пропозицій;
5. забезпечення стабільності прийняття рішень колегіальним органом можливе за умови, якщо результати голосування по кожному питанню фіксуються належним чином та оприлюднюються, а також – за умови, якщо процедури відкликання голосу, передбачають його вмотивованість та обмежують строки на відкликання.

У випадку вирішення питань у сфері медіа, найскладнішим завданням стає забезпечення повноти представлення та балансу інтересів всіх зацікавлених сторін. Залежно від важливості та змісту поставленого перед колегіальним органом питання, представництво від суб'єктів у сфері медіа може бути більш чи менш широким. У разі роботи над великим міжгалузевим актом, імовірно буде достатнім делегування до робочої групи окремих представників від телебачення, радіо та друкованих ЗМІ, які водночас можуть представляти інтереси їх онлайн версій. Втім, брати до уваги, що навіть в межах одного виду медіа є не лише конкуренція, але і істотна різниця інтересів між великим, малим та середнім бізнесом, тому зазвичай до колегіальних органів також окремо включаються представники організацій, які об'єднують локальних мовників та видавців регіональної преси. Щодо представництва онлайн медіа, які не пов'язані з жодним видом традиційних медіа, то на сьогодні питання ускладнюється через відсутність традицій співпраці між ними, відсутність усталених організацій, які об'єднують значну частину таких видань, а також – відсутність загальновизнаних авторитетів. На сучасному етапі цю проблему можна вирішити шляхом представництва їх інтересів делегатами від організацій, які працюють у сфері захисту свободи висловлювань.

ПРЯМУЄМО РАЗОМ
МІЖНАРОДНИЙ ФОНД ВІДРОДЖЕННЯ
Комітет цифрової трансформації
European Media Platform

Кібербезпека, захист персональних даних і інтеграція України до Єдиного цифрового ринку ЄС

Костянтин Корсун

1. Огляд ринку кібербезпеки України

Станом на початок 2021 рік в України сформувався стійкий ринок товарів та послуг індустрії кібербезпеки, ступінь конкуренції на якому оцінюється як висока.

Достовірної статистики стосовно ринку кібербезпеки України на теперішній день не існує через відсутність всеукраїнської професійної асоціації та/або єдиного державного регулятора (координатора), до яких би надходили релевантні дані для подальшого аналізу та оприлюднення.

За експертними оцінками, більшість учасників ринку (близько 60-70%) орієнтовано на внутрішнього споживача, близько 15-20% має пріоритет на зовнішній ринок, виключно на зовнішній ринок працює не більше 5-10% гравців ринку.

Розподіл ринку кібербезпеки в Україні в цілому збігається з розподілом ринку країн з розвинутою кібер-індустрією, і його напрямки можна умовно поділити на три нерівні частини:

- виробники (вендори) кібербезпекового програмного забезпечення (software) та відповідного обладнання (hardware): на українському ринку прямо чи через посередників представлені практично усі провідні світові вендори: Cisco, Fortinet, Mikrotik, McAfee, PaloAlto, FireEye. Безпосередньою реалізацією обладнання, рішень, софта та технологій вендорів на території України займаються компанії-дистриб'ютори (ERC, МУК, Бакотек, Softprom);
- компанії-інтегратори, які вбудовують (адаптують) рішення від різних виробників в існуючи комп'ютерні мережі українських клієнтів: таких компаній найбільше і, як правило, вони обслуговують декілька (до 10) великих замовників; (OptiData, It-solutions, Integrity Vision, Світ-IT, IT IS, RMRF, NetWave);
- консалтингові компанії, які здебільшого надають послуги з кібербезпеки: аудит безпеки IT-інфраструктури, тестування на проникнення, аналіз коду, організація проведення Bug Bounty, відповідність нормативним вимогам (compliance), кібер-розвідка (Threat Intelligence), тощо; такі компанії спеціалізуються здебільшого на високорівневих технічних аспектах кібербезпеки і кількість таких компаній невелика відносно загальної кількості учасників українського кібер-ринку; (Berezha Security, 10Guards, Advantio, UnderDefense, Імпрувмент Сервіс.)

Організації державної форми власності (державні органи та державні компанії) також представлені на кібер-ринку України, але переважно у ролі споживача товарів та послуг. Їхня доля на ринку є малопомітною через низькі фінансові можливості та законодавчі обмеження стосовно процедур закупівлі послуг з кібербезпеки, орієнтованих на найнижчу ціну, що прямо впливає на симетрично найнижчу якість таких послуг.

Українська спільнота фахівців з кібербезпеки (кібер-ком'юніті) є доволі активною та також впливає на розвиток ринку та підвищення загально-національного рівня кібер-захищеності. Активність кібер-ком'юніті полягає у проведенні масштабних (до 600 учасників) кібер-конференцій, впливу на роботу державних інституцій через громадські об'єднання, а також популяризації ідей кібербезпеки у публічних медіа та соціальних мережах.

Основними споживачами товарів та послуг індустрії кібербезпеки України є переважно великий та середній бізнес: банки та кредитно-фінансові організації, транспортна галузь, енергетика, машинобудування, зв'язок, розробники програмного забезпечення, торговельні та виробничі компанії та багато інших компаній, робота яких прямо чи опосередковано залежить від рівня кібер-захищеності їхніх комп'ютерних та інформаційних мереж.

Головними ризиками споживачі товарів та послуг індустрії кібербезпеки України вважають наступні:

- Можливі витоки та компрометація даних;
- Потенційна можливість викрадання грошових коштів та ресурсів компанії;
- Можливе блокування зловмисниками публічних інформаційних ресурсів як методу комунікації з клієнтами;
- Промислове шпигунство як метод конкурентної боротьби;
- Недружнє ставлення органів влади, корупція

Однією з ключових проблем функціювання внутрішнього кібер-ринку та його інтеграції з ринками ЄС є відсутність єдиного центру компетенції та довіри. Особливо це актуально для тих споживачів товарів та послуг, які не мають можливості самостійно оцінити компетентність та надійність окремих «продавців» на даному ринку. Через це на ринку існують некомпетентні та нечесні гравці, які наносять репутаційної шкоди іншим гравцям та знижують рівень довіри до індустрії загалом.

Для вирішення подібних проблем зазвичай створюється професійна асоціація учасників місцевого ринку, але справжньої достатньо авторитетної професійної асоціації наразі в Україні не існує. Натомість існує багато маловідомих об'єднань, які називають себе професійними асоціаціями учасників ринку кібербезпеки, але засновані вони одним або кількома учасниками ринку (часто з сумнівною компетенцією або діловою репутацією) і не викликають довіри в усіх інших учасників. Причин для такого стану справ існує кілька: нерівний рівень кваліфікації різних гравців, висока конкуренція, різні підходи до оцінки якості послуг, репутаційна неоднорідність ринку, його неструктурованість.

Але головною причиною є системна недовіра між учасниками ринку товарів та послуг кібербезпеки, хоча більшість з них готова до створення професійної асоціації та багато учасників неодноразово наголошували на такій потребі для ринку в цілому.

2. Наявні проблеми в сфері кібербезпеки та захисту персональних даних в Україні, які заважають інтеграції до DSM

2.1

Існування та розвиток ринку кібербезпеки України відбувається завдяки самим учасникам ринку, відповідно до законів економічного розвитку та за умови практично повної відсутності державного регулювання.

Завдяки цьому ринок розвивається, і на ньому існує здорова конкуренція.

Разом з тим, відсутність загально-національної координації та єдиних "правил гри" теж має свої негативні сторони.

Серед найпомітніших з них є розсинхронізована державна політика щодо захисту національних інтересів держави Україна у кіберпросторі.

Згідно Закону України "Про основні засади забезпечення кібербезпеки України"[1], основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України. Координація діяльності у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України. Усі зазначені організації є державними органами, більшість з яких відносяться до силового блоку.

Приватний сектор та кібер-ком'юніті, кількість представників яких загалом у кібер-індустрії переважає 80%, серед основних суб'єктів національної системи кібербезпеки не представлені взагалі. Також не представлені підприємства критичної інфраструктури, на захист яких мають спрямовувати свої зусилля зазначені у Законі "основні суб'єкти".

Через такий дисбаланс відсутнє поле для діалогу та взаємопорозуміння, можливості напрацювання спільних ефективних рішень є обмеженими, а ефективність шляхів побудови ефективної моделі національної кібербезпеки залишається низькою.

Крім того, навіть поміж основними суб'єктами національної системи кібербезпеки не існує чітких домовленостей та єдиного бачення шляхів розвитку національної кібербезпеки. Рівень міжвідомчої конкуренції за фінансування та повноваження залишається між ними високим, що, за умов ігнорування значного потенціалу приватного сектору, негативно впливає на стан національної кібербезпеки та державної політики у цій сфері.

У 2019 році було створено Міністерство цифрової трансформації України[2], яке також претендую на лідируючу роль у формуванні державної політики у сфері кібербезпеки, хоча не має для цього законодавчих підстав. Але завдяки фактичним преференціям з боку найвищих посадовців виконавчої влади України, Міністерство активно втручається у питання національної кібер-захищеності України, що додає ентропії у і без того розбалансовану державну кібер-політику.

2.2

Питання свободи доступу до глобальної мережі Інтернет та свободи поширення інформації у ньому досить гостро стоїть у сучасній Україні.

Під приводом посилення боротьби зі злочинністю (дитяче порно, тероризм, сепаратизм, шахрайство) владні структури та правоохоронні органи не полишають спроб налагодити масове стеження за користувачами Інтернет і таким чином обмежити права громадян на вільне поширення інформації та свободу слова.

Українськими судами формально заблоковано доступ до більш ніж 100 інформаційних ресурсів в Інтернет. При цьому легітимність цих судових рішень є досить сумнівною, а рішення могли бути прийняті під значним тиском правоохоронної системи.

[1] *https://zakon.rada.gov.ua/laws/show/2163-19#Text*

[2] *https://thedigital.gov.ua*

Указом Президента України № 133/2017 від 15 травня 2017 року[3] про введення в дію рішення РНБО України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)».

Особливістю нових санкцій стала вимога блокування інтернет-провайдерами доступу до веб-ресурсів інтернет-компаній ВКонтакті, Одноклассники, «Mail.ru», «Яндекс», «Лабораторія Касперського», «Dr.Web», офіційного дистриб'ютора «1С» на території України та інших строком на 3 роки.

Зазначений Указ протирічив деяким нормам українського законодавства та багаторазово критикувався професійною юридичною спільнотою, а його його легітимність досить сумнівна. Також Указ не містив механізмів технічної імплементації блокувань, тому деякі провайдери рішення даного Указу не виконували або виконувли частково.

Враховуючи те, що владні структури не мають ані технічних можливостей заблокувати певні ресурси, ані відповідних повноважень, продовжуються спроби закріпити у законах України право працівників правоохоронної системи мати безконтрольний доступ як до метаданих про українських користувачів Інтернет, так і до змісту інформації, що передається каналами Інтернет-комунікацій.

Подібні ініціативи з боку влади мали місце у 2017 та 2018 роках, коли у Верховну Раду України вносився законопроект № 6688, згідно якого оператори та провайдери Інтернет-комунікацій зобов'язувалися за власні кошти встановити на своїх вузлах спеціальне обладнання для перехоплення інформації їхніх користувачів. При цьому законопроектом передбачалася можливість прямого доступу без рішення суду невизначеної кількості правоохоронців, слідчих, прокурорів до трафіку користувачів без запровадження механізмів контролю за цією діяльністю.

У 2017 та 2018 роках законопроект №6688 викликав бурхливі та масові протести як з боку провайдерів/операторів зв'язку, так і з боку IT-середовища, громадських організацій, професійної спільноти.

Внаслідок зазначених протестів законопроект 6688 обидва рази був переглянутий, а згодом відкликаний. Але спроби владних структур та правоохоронців встановити контроль за комунікаціями в Інтернет не припиняються.

Так, у січні 2021 року набув чинності Закон України «Про електронні комунікації»[4], в ст. 121 якого зазначено два принципових для правоохоронних органів моменти:

"*2. Зняття інформації з електронних комунікаційних мереж постачальників електронних комунікаційних послуг забезпечується єдиною системою технічних засобів, що використовується усіма уповноваженими законом органами, на умовах автономного доступу до інформації у порядку, визначеному законодавством*"

Цим пунктом фактично узаконено можливість доступу поліцейських структур напряму в мережі провайдерів/операторів. Механізм контролю за можливими зловживаннями у Законі не визначено.

У наступному пункті закріплено зобов'язання провайдерів/операторів сприяти наданню такого безконтрольного прямого доступу до своїх мереж та інформації абонентів:

[3] *https://www.president.gov.ua/documents/1332017-21850*

[4] *https://zakon.rada.gov.ua/laws/show/1089-20#Text*

"3. Постачальник електронних комунікаційних послуг та/або мереж повинен забезпечити можливість підключення технічних засобів, зазначених у частині другій цієї статті, в точці для такого доступу в електронній комунікаційній мереж, визначеній постачальником електронних комунікаційних мереж та/або послуг».

Таким чином, фактично у Законі України «Про електронні комунікації» закріплено право правоохоронних структур України запровадити масове стеження за невизначеною кількістю користувачів Інтернет, при цьому не зазначено запобіжники до можливих зловживань та перебільшення повноважень з боку працівників органів правопорядку.

Натомість у жодному із законів України не закріплена заборона втручання у безперешкодне функціювання мережі Інтернет, а також не захищені права громадян на вільний доступ до інформації в Інтернет та свободу поширення не забороненої законом інформації.

Наявність такого Закону позитивно вплинула б на стан захисту прав та свобод громадян України, а також сприяла б оздоровленню стосунків між державою та громадянином та позначила б дійсне прагнення до побудови правової держави.

2.3

Чинне українське національне кібер-законодавство є застарілим та слабо корелюється з ландшафтом сучасних кібер-загроз та викликів. Законодавчих, підзаконних, регуляторних та нормативно-правових актів існує велика кількість, але багато з них не узгоджені між собою (а інколи протирічать одне одному), не регулюють актуальні аспекти національної кібербезпеки та функціювання відповідного сектору економіки, часто не є актуальними для сучасних загроз, незручні у користуванні, деякі вимоги важко виконати без значних ресурсів, багато нормативних актів мають корупційну складову.

Також українське законодавство не адаптовано до термінології, вимог та сутності законодавства ЄС та міжнародних актів. Зокрема, Конвенції з кіберзлочинності[5], яка ратифікована українським парламентом у 2005 році, але досі не імплементована у чинне законодавство у повному обсязі.

Тобто наразі кібер-сфера України законодавчо регулюється лише частково, фактична діяльність у цій сфері централізовано координується лише для держструктур, і теж частково та з недостатньою ефективністю.

Як виконавча, так і законодавча гілки влади усвідомлюють складність завдання реформувати законодавче забезпечення кібер-сфери, але також розуміють нездатність зробити це силами лише державних чиновників та посадовців.

Численні заклики влади до професійної спільноти долучитися до процесу реформування законодавчої сфери галузі кібербезпеки не знаходять розуміння через непрозорість умов такої співпраці, невпевненість у практичній імплементації її результатів, високі корупційні ризики процесу розробки законодавства (лобізм з боку великих компаній), а також через загальну недовіру до компетентності представників державного сектору.

Через ситуацію, що склалася, процес реформування кібер-законодавства України наразі знаходиться у патовій позиції, оскільки драйвером цього процесу мав би бути ринок, але ринок переважно не довіряє владі та не вірить у перспективи подібної співпраці. Влада, зі свого

[5] *https://zakon.rada.gov.ua/laws/show/994_575#Text*

боку, продемонструвала системну неспроможність реформувати кібер-законодавство без тісної співпраці з недержавним сектором. Також для бізнесу та ком'юніті не зрозуміло, з якою з дев'яти державних інституцій слід співпрацювати, яка з них здатна імплементувати нове законодавство, та яка з них нестиме відповідальність за розробку нових чесних правил гри та за результати реформи сектору в цілому. Додатково викликає сумніви рівень підготовки фахівців державного сектору та ступінь їх мотивації для реалізації відповідних реформ.

Таким чином, на даний час жоден з 9 основних суб'єктів національної системи кібербезпеки не має повноважень, відповідальності та бажання системно підійти до реформування кібер-сфери за зразком NIS Directive та ENISA Regulation: Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013[6] concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 (ENISA Regulation)[7]; Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016[8] concerning measures for a high common level of security of network and information systems across the Union (NIS Directive).

Для започаткування проекту суттєвої актуалізації системи кібер-законодавства як невід'ємної частини докорінного реформування всього сектору кібербезпеки, в Україні станом на 2021 рік відсутні як політична воля правлячих еліт, так і належна компетенція виконавців, а також відчувається брак розуміння необхідності такого реформування. Також у державних установах мало вкрай недостатньо представлено прагнення до співпраці з приватним сектором на рівних умовах та здатність нести відповідальність за результати подібних масштабних змін.

2.4

Питання захисту персональних даних є однім з найпроблемніших в Україні 2021 року. Фактично цей аспект усунуто з переліку актуальних завдань, а захист персональних даних громадян не здійснюється, а лише імітується. До 2014 року в Україні існувала Державна служба захисту персональних даних[9], яка системно займалися даною проблематикою. Але у 2014 році зазначена Державна служба була розформована, а функції захисту персональних даних покладено на Уповноваженого Верховної Ради України з прав людини (омбудсмена)[10]. З метою забезпечення виконання Уповноваженим функцій контролю за виконанням законодавства в сфері захисту персональних даних в Секретаріаті Уповноваженого Верхової Ради України з прав людини створено Департамент у сфері захисту персональних даних.

Але зазначений Депртамент не має дієвих повноважень, сил та засобів з ефективного захисту персональних даних громадян України, а працівники Департаменту не мають належної кваліфікації. Внаслідок такої ситуації права громадян на захист персональних даних постійно та масово порушуються, і практично ніхто не несе за це відповідальності.

Тому утворення незалежного уповноваженого органу з питань захисту персональних даних, як того вимагає Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних[11] та GDPR[12] є нагальною потребою та першочерговою задачею для України на шляху до комплексного вирішення проблем інформаційної та кібербезпеки.

[6] *https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:EN:PDF*

[7] *https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML*

[8] *https://eur-lex.europa.eu/eli/dir/2016/1148/oj*

[9] *https://uk.wikipedia.org/wiki/Державна_служба_України_з_питань_захисту_персональних_даних*

[10] *https://ombudsman.gov.ua/ua/page/zpd/*

[11] *https://zakon.rada.gov.ua/laws/show/994_326#Text*

[12] *https://gdpr-info.eu*

3. Прогноз щодо змін в Україні після ухвалення Digital Service Act, Cybersecurity Strategy, інших важливих європейських ініціатив

На жаль, держава Україна системно демонструє низький рівень уваги до питань власної кібербезпеки, незважаючи на тяжкі наслідки активної фази російсько-української кібервійни 2014-2018 років.

У той час, коли ЄС запроваджує поліпшені правила NIS Directive, GDPR, Open Internet Access Regulation[13] та ENISA Regulation, українська влада лише імітує зацікавленість у підвищенні кіберзахисту громадян, критичної інфраструктури, бізнесу та економіки.

Недосконалий та частково непрацюючий Закон України «Про основні засади забезпечення кібербезпеки», який неодноразово піддавався критиці експертним середовищем – системно не оновлювався з 2017 року. Правова база із захисту критичної інфраструктури почала розроблятися лише у 2020 році. Стан захисту персональних даних лише погіршується. Судова практика по блокуванню веб-ресурсів містить прямі порушення законодавства та порушує основні права громадян. Державні органи, уповноважені займатися кібербезпекою та кібер-захистом, недостатньо компетентні у цих питаннях, а державно-приватне партнерство у цій сфері дотепер не налагоджено і перспективи його налагодження доволі сумнівні. Силові структури не полишають спроб налагодження масового стеження за громадянами у Інтернет. Координація національної системи кібербезпеки країни по суті – не здійснюється. Каналами міжнародної технічної допомоги у країну надходять технології, обладнання, проводяться тренінги та консультації, але ключові проблеми залишаються невирішеними, і на загальний рівень кібербезпеки країни міжнародні програми допомоги не впливають.

Аналіз фактичної діяльності та/або бездіяльності органів державної влади України у сфері кібербезпеки та кіберзахисту свідчить про фактичне небажання наслідувати прогресивні світові практики. При цьому офіційні особи формально, на словах, визнають важливість ролі кібербезпеки у сучасному Світі, але практичними ділами подібні заяви майже не підкріплені.

Існує велика вірогідність того, що розробка та прийняття нових важливих європейських ініціатив досить мало або ніяк не вплине на покращення ситуації з національною кібербезпекою та станом кіберзахисту критичної інфраструктури в Україні.

4. Пропозиції щодо бажаних подальших дій

Враховуючи неефективність заходів органів державної влади України з питань покращення національної кібербезпеки, а також низьку ефективність поточних міжнародних програм допомоги у цій сфері, вважається доцільним зосередити зусилля міжнародних донорів та друзів України на напрямку вдосконалення фундаментальних основ побудови системи національної кібербезпеки– довіри між стейкхолдерами - із широким залученням професійної спільноти та українського кібер-бізнесу.

Як відомо, успішні практики побудови ефективних систем колективного кібер-захисту будуються на взаємні довірі та повазі між усіма її учасниками, і цей ключовий елемент повністю відсутній у конструкції будівлі національної кібербезпеки України.

Ключові стейкхолдери – кібер-бізнес, кібер-спільнота, державні інституції та кібер-наука – критично мало довіряють один одному і не мають чітких спільних позицій навіть всередині своїх розрізнених та неструктурованих екосистем.

[13] *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2015.310.01.0001.01.ENG&toc=OJ:L:2015:310:TOC*

Напрацювання довіри між усіма ключовими стейкхолдерами українського кібербезпекового сектору у рамках нового окремого проекту за умов незалежного фінансування групою міжнародних донорів повинен стати першим, але визначальним етапом для створення у подальшому працюючого прототипу моделі національної кібербезпеки України.

Підтримка проекту усіма ключовими стейкхолдерами та отриманий від них кредит довіри буде використаний для налагодження ефективної взаємодії всередині країни, зокрема для побудови працюючого прототипу національної системи обміну інформацією про інциденти.

У свою чергу, працюючий прототип системи обміну інформацією про інциденти міг би стати основою для продовження побудови ефективної системи національної кібербезпеки в усіх секторах економіки (у тому числі у критичній інфраструктурі), що суттєво підвищило б кібер-захищеність України.

Цілями подібного проекту повинні бути:

- Напрацювання довіри між ключовими стейкхолдерами: кібер-бізнесом, кібер-ком'юніті, органами державної влади (виконавча та законодавча гілки), кібер-наукою/академією, IT-громадськістю, операторами/провайдерами, міжнародною кібер-спільнотою.
- Побудова горизонтальних зв'язків між ключовими стейкхолдерами.
- Створення стійкого механізму співпраці та партнерства у сфері кібербезпеки між ключовими стейкхолдерами.

Принципи проекту:

- Домінування професіоналізму та ділової репутації;
- Якісні публічні комунікації, засновані на відкритості та фаховості;
- Максимальна прозорість щодо фінансування проекту;
- Врахування інтересів різних стейкхолдерів на засадах рівноправ'я;
- Заохочення професійного підходу та розвитку ринку кібербезпеки;
- Незалежність від державного фінансування;
- Нульова толерантність до корупції та будь-якої "нечесної гри".

Шляхи можливої реалізації:

1. В рамках вибудовування довіри між усіма суб'єктами кібербезпеки, створити незалежну Об'єднану Раду Кібер-Експертизи (робоча абревіатура ОРКЕ), до якої на громадських засадах увійдуть найавторитетніші експерти усіх основних стейкхолдерів. Кожен з них має бути відомим професіоналом з бездоганною діловою репутацією, що сприятиме підвищенню довіри до новоствореного осередку кібер-експертизи.
2. За сприяння ОРКЕ будувати горизонтальні зв'язки як між суб'єктами забезпечення кібербезпеки як по галузях, так і між суб'єктами різних стейкхолдерів: офіціні та неформальні зустрічі кібер-фахівців та їхніх керівників, семінари з обміну досвідом, міні-конференції, змагання, кібер-навчання, тощо.
3. Під егідою ОРКЕ розробити зрозумілі та прозорі правила та принципи для моделі державно-приватного партнерства у сфері національної кібербезпеки. Розроблені принципи та правила запропонувати на затвердження органами влади.
4. Під егідою ОРКЕ започаткувати проект з розробки нового кібер-законодавства, синхронізованого як всередині країни, так і з міжнародними стандартами, Конвенцією з кі-

берзлочинності, NIS, GDPR та іншими нормативними документами ЄС. Підготовлені напрацювання запропонувати на затвердження органами влади.

5. Під егідою ОРКЕ розробити принципи створення незалежного національного регулятора з питань захисту персональних даних (у відповідності до GDPR), а також законодавства із захисту цифрових свобод громадян.

Підготовлені напрацювання запропонувати на затвердження органами влади.

6. З використанням ОРКЕ та за участі учасників ринку, розробити загальні правила взаємодії його учасників, Code of Conduct для кібер-ринку, набір мінімальних вимог до компаній на кібер-ринку, за потреби – розробити систему оцінювання кібер-фахівців, тощо. Сприяти у заснуванні незалежної асоціації учасників ринку кібербезпеки України (за ініціативою за безумовної підтримки учасників ринку)
7. Максимальна популяризація мінімальних правил кібербезпеки (кібер-гігієна) та тематики «кібербезпека» загалом: блог, подкаст, канал на YouTube, регулярні повідомлення у соціальних мережах, коментарі та інтерв'ю членів ОРКЕ для медіа (телеканали радіостанції, періодичні видання), відкриті онлайн-дискусії. Організація регулярних мітапів, конференцій, круглих столів на теми кібербезпеки під егідою ОРКЕ, виступи експертів перед студентами профільних факультетів, організація кібернавчань, CTF, тощо.
8. Підготовкою рішень ОРКЕ та операційними питаннями імплементації її рішень займатиметься постійно діюча робоча група (виконавчий комітет) з числа професіоналів у відповідних галузях за ринковох вартістю їхніх послуг.

Схожі за ідеями "Пропозиції з реформування національної системи кібербезпеки"[14] були підготовлені ініціативною групою у складі сімох найвідоміших українських експертів з кібербезпеки, але її ключові ідеї та принципи залишаються нереалізованими та незатребуваними. Окремі положення та ініціативи із зазначених "Пропозицій.." деякі органи влади намагаються реалізувати, але відбувається це без врахування системних ідеологічних засад: рівноправного партнерства стейкхолдерів, відмови від "керівної ролі держави" під час реформування, реалізація інтересів держави через інтереси її громадян, прозорий механізм фінасування проекту з реформування сектору національної кібербезпеки, напрацювання кредиту довіри суспільства як головного драйвера подальшого розвитку.

У якості позитивного прикладу створення об'єднання кібер-стейкхолдерів можна навести CyberScotland Partnership (Партнерство КіберШотландії)[15], до якого увійшли 10 організацій, у тому числі бізнес-асоціація Scottish Business Resilience Centre (Шотландський Центр Кібер-Відновлювальноздатності), але також і Уряд Шотландії та Поліція Шотландії.

Коаліція з 10 організацій, які увійшли до складу CyberScotland Partnership проголошує своєю метою "...реагувати на виклики задля ясності навколо кібербезпеки як від приватних осіб, так і від бізнесу" to respond to calls for clarity around cyber security both from private individuals and businesses.)

Також CyberScotland Partnership не є і не може мати якихось владно-примусових повноважень, оскільки це добровільне об'єднання ключових кібер-стейкхолдерів на основі взаємної довіри.

CyberScotland пропонує свої ресурси кожному (не тільки для державних органів), хто шукає інформацію та підтримку з питань кібербезпеки та проблем відновлювальноздатності бізнесу,

[14] *https://www.slideshare.net/KostiantynKorsun/sean-brian-townsend*

[15] *https://www.computerweekly.com/news/252496747/CyberScotland-offers-centralised-security-resource-hub*

а також у питаннях кібер-кар'єри, розвитку навичок, чи то настанов.» (...central online hub to offer resources for anyone seeking information and support across a number of cyber security and business resilience issues – as well as cyber careers and skills support and guidance.)

Задля підтримки бізнесу, CyberScotland Partnership обіцяє "сприяти розквіту шотландських кібербезпекових продуктів та послуг" (...the partnership will help to promote Scotland's flourishing cyber security products and service industry.)

Нове кібер-об'єднання Шотландії також запобігатиме «дублюванню зусиль».

Кілька цифр про CyberScotland Partnership: національний кібербезпековий «кластер» налічує близько 230 компаній, з яких 48% засновані у Шотландії, і при цьому кожен рік з'являється близько 10 новий підприємств.

Приклад Шотландії не слід сприймати як зразок та прямий приклад до наслідування через невідповідність ряду ключових вхідних умов: культурологічних особливостей, характеру стосунків сусіпільства та влади, давнішу історію демократичного урядування у країні, наявність більш справедливої системи судочинства, вищий рівень довіри до владних інституцій, тощо.

Але разом з тим, використати дух та ідеї подібного кібер-об'єднання під час розбудови принципово нової системи національної кібербезпеки було б корисно для усіх українських кібер-стейкхолдерів задля покращення рівня кібербезпеки України.

ПРЯМУЄМО РАЗОМ
МІЖНАРОДНИЙ ФОНД ВІДРОДЖЕННЯ
Комітет цифрової трансформації
European Media Platform

Налагодження співпраці стейкхолдерів в процесі інтеграції України до Єдиного цифрового ринку Європи

Олег Цільвік

Споживач, як стейкхолдер

«Споживачі — це всі ми. Споживачі — це найбільший економічний прошарок, який впливає майже на будь-яке приватне або державне економічне рішення ... Але це єдиний голос, якого часто не чутно».

Зі звернення президента США Джона Кеннеді до Конгресу, 15 березня 1962 року

Існує безліч визначень терміну Стейкхолдер (англ. Stákeholder), але узагальнюючим для всіх цих визначень є те, що «зацікавлена сторона» - це особа, група осіб чи організація, інтереси яких мають бути враховані під час прийняття конкретного рішення, і це рішення має відповідати їх потребам і очікуванням.

Усі стейкхолдери так чи інакше пов'язані один з одним через комплекс взаємовідносин і взаємної залежності, які визначають їх поведінку і ставлення один до одного. Порушення балансу прав та інтересів будь-кого зі стейкхолдерів створює ризик для ефективності функціонування та сталості усієї системи.

У більшості випадків споживачі та їх об'єднання обов'язково мають розглядатися у якості стейкхолдерів. Для прикладу, ще у 1978 році при Міжнародній організації стандартизації (ISO) засновано Комітет зі споживчої політики (COPOLCO)[1], як відповідальний орган за просування інтересів споживачів в стандартизації. Слід зазначити, що одним із базових принципів робіт зі стандартизації є прийняття стандартів на основі консенсусу (відсутності суттєвих протиріч) усіх зацікавлених сторін. Звісно, що участь споживачів у розробці стандартів є важливою складовою, адже кінцевою метою управлінських рішень та виробничих процесів, для яких розробляються стандарти, є задоволення вимог та потреб кінцевого споживача.

На необхідності врахування думки споживачів наголошується і в Керівних принципах Організації Об'єднаних Націй для захисту інтересів споживачів[2], затверджених Резолюцією Генеральної Асамблеї ООН у 1985 році (остання редакція 2015 р.). Зокрема, у керівному принципі 5h в якості законної потреби чітко вказана «свобода створювати споживчі та інші відповідні групи або організації та можливість таких організацій представляти свою думку в процесі прийняття рішень, що зачіпають їх інтереси».

В основу сучасного споживчого законодавства закладена концепція захисту прав слабкої сторони. Досвід більшості країн світу та рекомендації міжнародних правозахисних інституцій свідчить, що правове регулювання, яке спрямоване на захист прав споживачів, ідентифікує споживача як найбільш незахищену (економічно та інформаційно) сторону у договірних правовідносинах із суб'єктами, що виробляють та продають товари, здійснюють виконання робіт або надають послуги.

[1] *https://www.iso.org/ru/copolco.html*

[2] *https://undocs.org/pdf?symbol=ru/a/res/70/186*

Виходячи із зазначеного, основною метою об'єднань споживачів є мінімізація негативних наслідків такої нерівності. Для досягнення своєї мети організації споживачів виконують різні функції, зокрема:

a) Проводять опитування і дослідження з метою вивчення проблем, з якими стикаються споживачі, включаючи вплив політики уряду на споживачів і рівень їх поінформованості;

b) Займаються просвітницькою діяльністю серед споживачів та наданням їм незалежної інформації (у тому числі отриманої в результатів власних перевірок і досліджень) стосовно товарів і послуг, щоб споживачі мали можливість робити усвідомлений вибір і відповідально підходити до споживання;

c) Розглядають скарги споживачів і консультують їх з приводу шляхів та методів врегулювання спору та отримання компенсацій за порушені права (така діяльність може включати як участь в органах по врегулюванню суперечок, так і в процесі захисту громадських інтересів від імені споживачів);

Втім, найбільш важливою функцією об'єднань споживачів є виконання представницьких функцій, щоб споживачі могли колективно донести свої погляди та точку зору до інших учасників ринкових відносин та влади. Ця діяльність полягає у налагодженні діалогу з урядом і діловими колами з метою інформування, переконання і ведення переговорів від імені споживачів. Для досягнення своєї мети споживчі об'єднання можуть вдаватися і до інших форматів просування своєї точки зору: від організації груп лобістів в парламенті і скоординованих кампаній в ЗМІ, до організації кампаній зі збору підписів, написання листів, навіть бойкотів і мітингів.

Спроможність та компетентність споживчих об'єднань

У Керівних принципах ООН для захисту інтересів споживачів неодноразово наголошується на важливій ролі асоціацій споживачів і рекомендується національним урядам надавати сприяння їх розвитку, зокрема у керівному принципі 1е зазначено - «сприяти розвитку незалежних груп споживачів». Цей документ став відправною точкою для країн-учасниць у питанні легалізації правового статусу об'єднань споживачів у національному законодавстві.

Україна не стала виключенням і на виконання цих рекомендацій у ст. 42 Конституції України[3] передбачено, що держава сприяє діяльності громадських організацій споживачів, а розділ III Закону України «Про захист прав споживачів» повністю присвячений питанням правового статусу громадських організацій споживачів (об'єднань споживачів) та їх правам[4].

Потреба у законодавчій легалізації об'єднань споживачів обумовлена необхідністю залучення до переговорного процесу або консультацій по тій чи іншій тематиці у якості третьої сторони, незалежного суб'єкта, який міг би озвучити проблеми, з якими стикаються споживачі. До того ж, цей суб'єкт не повинен бути політичною партією і має функціонувати на некомерційній основі. Тобто, одним із завдань об'єднань споживачів є необхідність донести точку зору широких верств населення, а особливо недостатньо представлених, у тому числі соціально незахищених, які не мають можливості висловитися через обмеженість у знаннях чи ресурсах.

У зв'язку із відсутністю законодавчих обмежень щодо процедури утворення об'єднань споживачів та в залежності від активності громадянського суспільства, кількість таких організацій по кожній конкретній країні може відрізнятися. Наприклад, станом на лютий 2021 року в Україні, за даними реєстру громадських об'єднань, зареєстровано близько 750 організацій, від

[3] *https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text*

[4] *https://zakon.rada.gov.ua/laws/show/1023-12#Text*

всеукраїнських до місцевих, які виходячи зі своєї назви можуть вважатися об'єднанням споживачів. Для порівняння, у країнах пострадянського простору станом на 2018 рік[5] розбіжність у кількості зареєстрованих громадських організацій споживачів була досить суттєвою, зокрема: Киргизстан – 4, Вірменія – 6, Білорусь – 21, Казахстан – 172, Росія – 1774.

На превеликий жаль, досвід України показує, що система захисту прав споживачів, насамперед державна, набула «слави» корумпованої, внаслідок чого державний орган влади, який відповідає за реалізацію політики у сфері захисту прав споживачів зазнав низку трансформацій та реформ протягом останніх років. І як крайній захід у боротьбі з корупцією в цій сфері, навіть запроваджувався мораторій на перевірки органами захисту прав споживачів. Звісно, що і громадський сектор не оминула ця проблема. Окремі організації споживачів утворювалися з метою участі у корупційних схемах, про що свідчать неодноразові публікації у ЗМІ про затримання «активістів» споживчих організацій за вимагання неправомірної вигоди від представників бізнесу. Усі ці фактори значним чином скомпрометували споживчий рух в нашій країні. Втім, за окремими критеріями, можна виділити низку найбільш відомих та активних споживчих об'єднань, які наразі проводять роботу в інтересах споживачів:

	Назва	Рік реєстрації	Сайт/сторінка у соц. мережах	Кількість осередків/ відділень	Напрямки діяльності
1	ГО "СОЮЗ СПОЖИВАЧІВ УКРАЇНИ"	2004	http://consumerunion.org.ua/ https://www.facebook.com/ consumerunion.com.ua	34	Просвітницька діяльність Моніторинг ринків та дослідження Робота зі споживачами Представницькі функції
2	ГО "ВСЕУКРАЇНСЬКА АСОЦІАЦІЯ З ПИТАНЬ ЗАХИСТУ ПРАВ СПОЖИВАЧІВ "СПОЖИВЧА ДОВІРА"	2012	https://vgo-dovira.org/ https://www.facebook.com/ spozhivchadovira/	-	Просвітницька діяльність Дослідження продукції Представницькі функції
3	Спілка об'єднань громадян "Всеукраїнська федерація споживачів "ПУЛЬС"	2010	https://www.facebook.com/ groups/ucf.pulse	-	Просвітницька діяльність серед студентів Представницькі функції

В сучасних умовах надзвичайно складно оцінити спроможність об'єднань споживачів, адже способи та напрямки їх роботи істотно різняться. Переважно це залежать від рівня економічного розвитку країни, де функціонує конкретне об'єднання споживачів, та заможності населення. У розвинених країнах основна роль об'єднань споживачів полягає у проведенні порівняльних тестувань та наданні достовірної інформації щодо продукції та послуг. Джерелами фінансування таких організацій є підписки на їх журнали і онлайн-сервіси, а також членські внески. Це найкращий приклад підтвердження незалежності організації, який дозволяє організації самостійно визначати пріоритетні напрямки діяльності.

Як правило, організації розвинених країн виступають ініціаторами та активними учасниками міжнародної співпраці та глобального споживчого руху. Для прикладу, впливова та найвідоміша - Міжнародна організація споживачів (Consumers International), була заснована у 1960 році п'ятьма об'єднаннями споживачів з наступних країн: США, Великої Британії, Австралії, Бельгії та Нідерландів. На сьогодні ця організація включає близько 200 членів з понад 100 країн світу.

[5] *https://bit.ly/3sw3Bas*

Доля об'єднань споживачів у країнах, що розвиваються, дещо відрізняється. Вони здебільшого працюють виключно на національному рівні і орієнтовані на вирішення базових потреб споживачів або навіть вузько направлених інтересів споживачів. Основна частина їх фінансування надходить із зовнішніх джерел - від організацій-донорів, які у свою чергу можуть значною мірою впливати на процеси прийняття рішень та визначення пріоритетних напрямків діяльності «залежних» (підконтрольних) організації.

В деяких країнах національні уряди надають споживчим об'єднанням фінансування на реалізацію просвітницьких проектів або компенсують видатки на правозахисну діяльність. В умовах, коли в країні існує багато об'єднань споживачів, які конкурують між собою за право стати законними представниками руху споживачів, такий інструмент може вважатися фактично визнанням легітимності організації. Втім, на думку експертів, в залежності від економічної ситуації в країні, це може також негативно позначитися на незалежності об'єднання споживачів адже керівництво організації може вдатися до дій спрямованих на прояв лояльності до дій регулятора, в обмін на фінансування, замість виконання своїх обов'язків забезпечувати просування та відстоювання точки зору та інтересів споживачів.

Беззаперечно, що ключовим фактором забезпечення довіри до об'єднання споживачів є його незалежність та фінансова життєздатність, втім забезпечити обидва фактори у країнах, що розвиваються, досить складно. У такому випадку бажано переконатися у відсутності залежності організації від політичних партій та прямого зв'язку із компаніями.

Існує ще низка факторів, які також доцільно враховувати, вирішуючи питання щодо залучення кожного конкретного об'єднання споживачів у якості стейкхолдера. Одним з них є наявність достатньої членської бази та механізмів проведення консультацій з членами організації. Втім, враховувати цей фактор потрібно з обережністю, адже невеликі організації, якім складно довести відповідність цьому критерію та отримати можливість виконувати представницьку функцію, можуть представляти інтереси невеликої групи споживачів (наприклад, осіб, що постраждали від дій надавача послуг по конкретному будинку чи представляти соціально-незахищених споживачів району, які не є членами організації).

Як правило, жодне об'єднання споживачів не спроможне повною мірою представити позицію усіх споживачів. В залежності від інтересів різних категорій споживачів, що входять до організації, формування пріоритетів її діяльності може обумовлюватися національною і етнічною приналежністю членів організації, місцем їх проживання та родом зайнятості, статтю, віком, рівнем доходу. Інколи інтереси споживачів настільки різняться, що за певних обставин це може призводити до виникнення гострих конфліктів між різними групами споживачів. Наприклад, якщо певні домогосподарства вже підключилися до надавача послуг (електрика, зв'язок, водопостачання) – їм може бути вигідне збереження низьких тарифів за рахунок підвищення вартості підключення, у той же час для домогосподарств, які ще не підключилися до цих послуг, найбільшу актуальність буде представляти питання вартості послуг підключення. Тож, якщо будуть враховуватися інтереси тільки діючих споживачів послуг, інтереси осіб, які наразі не є споживачами (тих, хто не має підключення), залишаться не врахованими.

Не останню роль при визначенні стейколдера відіграє такий фактор, як рівень освіти споживачів, на яких розрахований той чи інший продукт. Більш складні продукти, наприклад, фінансові послуги, які надаються онлайн, в тому числі через мобільні телефони, можуть створювати ризики для споживачів з обмеженою фінансовою грамотністю. Тож засоби і заходи, спрямовані на розширення доступу до інформації для споживачів, з більшою ймовірністю принесуть користь споживачам із середнім і високим рівнем освіти. Втім вони можуть завдати шкоди споживачам з меншим рівнем відповідних знань. Яскравим прикладом цього може бути ринок небанківських фінансових послуг в Україні.

Наразі у міжнародній практиці відсутні єдині критерії оцінки компетентності об'єднань споживачів. Є окремі приклади врегулювання цього питання, зокрема в Республіці Білорусь. Так, відповідно до п. 3 ст. 48 Закону РБ «Про захист прав споживачів» громадське об'єднання має право давати консультацію споживачеві з питань захисту його прав, звертатися за дорученням споживача з претензією до виробника (продавця, виконавця) про усунення порушень і про відшкодування споживачеві завданих цими порушеннями збитків, звертатися до суду з позовом про захист прав споживача, представляти і захищати в суді права і законні інтереси споживача (невизначеного кола споживачів) за умови наявності у працівника громадського об'єднання споживачів, що реалізує зазначені права цього громадського об'єднання, свідоцтва про атестацію. Станом на 01.02.2021 р. Міністерством антимонопольного регулювання і торгівлі РБ було атестовано 84 працівника громадських об'єднань споживачів[6].

Частково питання кваліфікації піднімається Директивою 2013/11/EU про альтернативне вирішення споживацьких спорів[7]. Але у цьому випадку мова не йде про виключно об'єднання споживачів. Згідно вимог Директиви, кожна держава-член зобов'язана надати перелік організацій на своїй території[8], які можуть бути включені до системи альтернативного вирішення спорів і які відповідають обов'язковим кваліфікаційним вимогам, встановленим Директивою. Серед таких організацій можуть бути, у тому числі, і об'єднання споживачів.

З огляду на зазначене вище можна підвести підсумок, що питання визначення репрезентативного стейкхолдера з числа споживчих об'єднань є надзвичайно складним та багатогранним. Громадські споживчі організації - це самостійні суб'єкти, ефективність діяльності яких багато в чому залежить від організаційно-правової основи діяльності організації, наявності експертної складової та досвіду взаємодії з державними органами влади та бізнесом.

Проблематика законодавчого забезпечення захисту прав та інтересів споживачів

Розвиток законодавства про захист прав та інтересів споживачів являє собою складний процес, адже цей вид законодавства носить горизонтальний і багатоаспектний характер. Закони щодо захисту споживачів взаємопов'язані з багатьма іншими галузями права. У свою чергу, треба передбачити, щоб національне законодавство відповідало також і міжнародному праву.

Європейський досвід доводить, що в основу споживчого законодавства покладається концепція захисту прав слабкої сторони. Основна ідея такої концепції полягає у визнанні споживача найбільш незахищеною (економічно та інформаційно) стороною у договірних правовідносинах із суб'єктами, що виробляють товари, здійснюють роботи чи надають послуги.

Між тим, у багатьох країнах зв'язок між рамковими законами про захист прав та інтересів споживачів і галузевими законами викликає протиріччя. Зокрема, банки, страхові компанії, авіаперевізники та постачальники послуг зв'язку наполягають на тому, що вони керуються не загальним законодавством про захист прав та інтересів споживачів, а тільки законам, які можуть застосовуватися до їх сфер діяльності. Таке тлумачення, як правило, відхиляється судами, які наполягають на горизонтальному або всеосяжному масштабі застосування рамкового законодавства про захист інтересів споживачів. Ця проблема не оминула і Україну. Низка законів має власне визначення терміну «споживач» попри те, що це не узгоджується з

[6] *https://bit.ly/3ei913v*

[7] *https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32013L0011*

[8] *https://ec.europa.eu/consumers/odr/main/?event=main.adr.show2*

пунктом 22 статті 1 Закону України «Про захист прав споживачів», за яким «споживач – фізична особа, яка придбає, замовляє, використовує або має намір придбати чи замовити продукцію для особистих потреб, безпосередньо не пов'язаних з підприємницькою діяльністю або виконанням обов'язків найманого працівника». Для прикладу:

- «споживач послуг – будь-яка фізична особа, яка використовує або замовляє електронну комунікаційну послугу для власних потреб та не надає електронних комунікаційних послуг» (ЗУ «Про електронні комунікації»);
- «споживач телекомунікаційних послуг (споживач) - юридична або фізична особа, яка потребує, замовляє та/або отримує телекомунікаційні послуги для власних потреб» (ЗУ «Про телекомунікації»);
- «побутовий споживач - індивідуальний побутовий споживач (фізична особа, яка використовує електричну енергію для забезпечення власних побутових потреб, що не включають професійну та/або господарську діяльність) або колективний побутовий споживач (юридична особа, створена шляхом об'єднання фізичних осіб - побутових споживачів, яка розраховується за електричну енергію за показами загального розрахункового засобу обліку в обсязі електричної енергії, спожитої для забезпечення власних побутових потреб таких фізичних осіб, що не включають професійну та/або господарську діяльність)» (ЗУ «Про ринок електричної енергії»);
- «споживач - фізична особа, у тому числі фізична особа-підприємець, або юридична особа, що купує електричну енергію для власного споживання» (ЗУ «Про ринок електричної енергії»);
- «споживач фінансових послуг - фізична особа, яка отримує або має намір отримати фінансову послугу для задоволення особистих потреб, не пов'язаних із підприємницькою, незалежною професійною діяльністю» (ЗУ «Про фінансові послуги та державне регулювання ринків фінансових послуг»);
- «кінцевий споживач - споживач, який використовує харчовий продукт виключно для власного споживання» (ЗУ «Про основні принципи та вимоги до безпечності та якості харчових продуктів»);
- «споживач житлово-комунальних послуг (далі - споживач) - індивідуальний або колективний споживач» (ЗУ «Про житлово-комунальні послуги»);
- «індивідуальний споживач - фізична або юридична особа, яка є власником (співвласником) нерухомого майна, або за згодою власника інша особа, яка користується об'єктом нерухомого майна і отримує житлово-комунальну послугу для власних потреб та з якою або від імені якої укладено відповідний договір про надання житлово-комунальної послуги» (ЗУ «Про житлово-комунальні послуги»);

Таке розмаїття визначень перевантажує законодавство та вносить плутанину, хоча галузеве законодавство не може перешкоджати застосуванню рамкових законів, а має лише доповнювати його.

Яскравим прикладом спроби учасників галузі дистанціюватися від дії Закону України «Про захист прав споживачів» є прийняття Закону України «Про електронні комунікації». Навіть не зважаючи на той факт, що закон приймався на основі Європейського кодексу електронних комунікацій (Директива (ЄС) 2018/1972), автори вдалися до певної маніпуляції із термінологією. Наприклад, в Директиві використовується термін «споживач» (будь-яка фізична особа, яка використовує або замовляє загальнодоступну електронну комунікаційну послугу для цілей, які не відносяться до її торгівлі, бізнесу, ремесла або професії). Саме це визначення і застосовується у тексті Директиви понад 70 разів. В той же час, в Законі України «Про електронні

комунікації» автори використали термін «споживач послуг» (будь-яка фізична особа, яка використовує або замовляє електронну комунікаційну послугу для власних потреб та не надає електронних комунікаційних послуг), втім таке словосполучення більше жодного разу не згадується у тексті закону. Натомість, в тексті понад 70 разів використовується термін «споживач».

Не в найкращий спосіб здійснена спроба імплементувани положення ст. 25 Директиви (ЄС) 2018/1972 щодо позасудового вирішення спорів. Зокрема, метою зазначеної статті є інтегрування механізмів Директиви 2013/11/ЄС (про альтернативне вирішення спорів), які, відповідно до першоджерела, спрямовані на досягнення високого рівня захисту споживачів. Незважаючи на той факт, що у ст.123 Закону України «Про електронні комунікації» на регулятора покладаються функції органу позасудового врегулювання спорів за зверненням споживачів, у тексті Закону взагалі відсутні кваліфікаційні вимоги щодо осіб, які можуть виконувати цей функціонал. Слід зазначити, що Директива 2013/11/ЄС має цілу низку критеріїв, які висуваються, як до органу альтернативного вирішення спорів, так і до конкретних осіб. Зокрема, такі особи, принаймні, мають володіти необхідними знаннями та навичками у сфері альтернативного чи судового вирішення спорі, а також загального розуміння права.

Також спотворено сутність ст. 24 Директиви (ЄС) 2018/1972 щодо консультацій із зацікавленими сторонами. В той час, коли Директивою передбачається механізм залучення усіх зацікавлених сторін до вирішення питань, виключно «пов'язаних з усіма правами кінцевих користувачів і споживачів, включаючи рівнозначний доступ і вибір для кінцевих користувачів з інвалідністю», то в українському варіанті (ст. 22 Закону) пріоритет надається питанням функціонування ринку – «заходів, які мають суттєвий вплив на відповідний ринок, у тому числі щодо конкурсних засад розподілу радіочастотного спектра, аналізу ринків та прийняття рішень за його результатами, вжиття заходів із забезпечення доступності універсальних послуг» і тільки другим пунктом «з питань, пов'язаних з правами кінцевих користувачів».

До того ж, «споживачі» як окрема категорія взагалі випали з переліку учасників консультацій в Законі України «Про електронні комунікації», що знову ж таки, викликає занепокоєння. Якщо в ст. 24 Директиви (ЄС) 2018/1972 чітко наголошується, що потрібно враховувати «позиції кінцевих користувачів, зокрема споживачів, кінцевих користувачів з інвалідністю, виробників та суб'єктів господарювання», то у ст. 22 Закону передбачено «проведення консультацій з кінцевими користувачами, у тому числі споживачами з інвалідністю, виробниками та постачальниками електронних комунікаційних засобів, постачальниками електронних комунікаційних мереж та/або послуг».

Наведений приклад Закону України «Про електронні комунікації» свідчить про певні недоліки процесу наближення вітчизняного законодавства до європейського, особливо в сегменті захисту прав та інтересів споживачів.

Не слід забувати, що внаслідок глобалізаційних процесів економіки країн стають все більш взаємопов'язаними, тож національні органи із захисту прав та інтересів споживачів повинні враховувати міжнародний характер багатьох споживчих угод. Все більше зростає потреба в тому, щоб різні юрисдикції напрацьовували механізми міжнародного захисту інтересів окремих споживачів або категорій споживачів.

Відповідно до Угоди про асоціацію (ст. 415 Глави 20 «Захист прав споживачів» Розділу V «Економічне та галузеве співробітництво») Україна взяла на себе зобов'язання забезпечити високий рівень захисту прав споживачів та досягнути сумісність української системи захисту прав споживачів з аналогічними системами держав-членів ЄС.

Запровадження ефективної системи захисту прав споживачів матиме позитивний вплив на багатьох учасників ринкових відносин і, у тому числі, принесе користь для держави. Насамперед, споживачі відчують підвищення рівня задоволеності отриманими товарами та послугами, а бізнесові кола будуть змушені вдаватися до чесної конкуренції, яка також відіграє важливу роль в задоволені економічних інтересів споживачі, адже конкуренція між компаніями сприяє підвищенню ефективності виробництва та за рахунок інновацій наповнює ринок новими товарами підвищеної якості.

Але забезпечення високого рівня захисту споживачів має додаткові користі - це призводить до збільшення довіри споживачів до різних форм торгівлі і, у свою чергу, позитивно впливає на підвищення рівня споживання, що позначається на пришвидшенні темпів економічного розвитку країни. Саме цей комплекс взаємозв'язків та позитивних наслідків для усіх зацікавлених сторін, став рушієм послідовної політики Європейської Комісії спрямованої на забезпечення високого рівня захисту споживачів.

На жаль, виконання Україною цих зобов'язань наразі є проблематичним. Про це свідчить і положення «Концепції державної політики у сфері захисту прав споживачів на період до 2020 року», схваленої розпорядженням Кабінету Міністрів України від 29.03.2017 р. № 217-р. (через три роки після підписання Угоди), де чітко зазначено, що «Споживачі в Україні не захищені державою і законом внаслідок декларативного характеру проголошених прав та відсутності механізмів їх реалізації та відновлення.»[9]

Усі доступні звіти про виконання Угоди про асоціацію в частині захисту прав споживачів свідчать про майже нульовий прогрес. В той же час частина регуляторних актів, які згідно Угоди Україна має імплементувати, вже втратила чинність або буде змінена найближчим часом, зокрема Директива про певні аспекти продажу споживчих товарів та пов'язані з цим гарантії (1999/44/ЕС)[10]. Відповідно до Директиви, споживач має мінімальну 2-річну гарантію на несправні товари або товари, які виглядають або працюють не так, як зазначено в рекламі.

Спроба імплементувати зазначену Директиву шляхом прийняття Верховною Радою України проєкту Закону України «Про внесення змін до деяких законодавчих актів України (щодо захисту прав споживачів)» (реєстр. № 5548 від 16.12.2016), норми якого передбачали повну імплементацію Директиви 1999/44/ЄС не увінчалася успіхом. Законопроєкт відкликаний 29.08.2019 р.

За цей час через суттєві зміни, що відбулися на ринку ЄС з моменту прийняття цієї Директиви у 1999 році, Єврокомісія вирішила модернізувати регулювання і з 1 січня 2022 року Директиву про продаж товарів та пов'язані з нею гарантії буде замінено двома іншими:

- Директива (EU) 2019/770 щодо контрактів на поставку цифрового контенту та послуг (Директива щодо цифрового контенту);
- Директива (EU) 2019/771 про договори купівлі-продажу товарів 2019/771/ЄС (Директива щодо продажу товарів).

Держави-члени мають строк до 1 липня 2021 р. ввести Директиви у національне законодавство.

Згідно з новими директивами, споживач матиме ті самі права стосовно проблем чи дефектів цифрового контенту, цифрових послуг чи розумних продуктів (тобто продуктів із цифровим компонентом), як і на будь-який інший продукт.

[9] *https://zakon.rada.gov.ua/laws/show/217-2017-%D1%80#Text*

[10] *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31999L0044*

Майже аналогічна ситуація з Директивою № 97/7/ЄС Європейського Парламенту та Ради від 20.05.1997 про захист споживачів стосовно дистанційних контрактів. Директива втратила чинність у 2014 році та була замінена на Директиву 2011/83/ЄС про права споживачів.

Директива про права споживачів 2011/83/ЄС[11] спрямована на наближення законодавчих положень держав-членів щодо дистанційних договорів, договорів, що укладені поза діловими приміщеннями, та деяких інших аспектів споживчих відносин. Втім, Директива має три виключення і її положення не застосовуються до наступних сфер:

1. соціальні послуги, включаючи соціальне житло, догляд за дітьми та підтримка сімей та осіб, що опинилися у складних життєвих обставинах (нужденні) та потребують тимчасового або постійного догляду;
2. медичне обслуговування та медичні послуги, що надаються медичними працівниками пацієнтам для оцінки, підтримання або відновлення стану їх здоров'я, включаючи призначення, відпуск та надання лікарських засобів та медичних виробів, причому, незалежно від того, надаються ці послуги через заклади охорони здоров'я або ні.
3. азартні ігри, включаючи лотереї, ігри у казино та ставки.

Під поняттям «Контракт на відстані» (дистанційний договір), розуміється «будь-який договір, що укладений між продавцем та споживачем в рамках організованої схеми дистанційних продажів чи надання послуг без одночасної фізичної присутності продавця і споживача, виключно шляхом використання одного чи декількох засобів дистанційного зв'язку до моменту і в момент укладення договору» (п. 7 ст. 2). Відповідно до логіки Директиви, укладаючи такий тип контракту, споживач не можете перевірити товар перед покупкою. Через це у нього має бути додатковий захист згідно Директиви, а саме надаються такі права:

- право на повну інформацію щодо товару до моменту покупки;
- надається 14-денний період «охолодження», протягом якого споживач може передумати купувати товар та відмовитися від угоди. Період «охолодження» застосовується до усіх контрактів на відстані, включаючи покупки через Інтернет, втім має виключення щодо персоналізованих предметів (виготовлення під замовлення), замовлення готелів або прокату автомобілів.
- право на повернення коштів протягом 14 днів після скасування угоди;
- право на доставку продукції протягом 30 днів (якщо інший термін не погоджено з продавцем);
- споживач повинен дати свою явну згоду (наприклад, встановивши прапорець і вибравши таку опцію), перш ніж продавець зможе застосувати додаткові витрати;
- зі споживача не можуть стягуватись доплати за певні типи способів розрахунку, наприклад, за сплату кредитною карткою.

Враховуючи швидкі темпи розвитку електронної комерції та з метою модернізації й посилення регулювання щодо захисту прав споживачів Євросоюзу 18 грудня 2019 року була прийнята нова Директива 2019/2161/EU[12] Європейського Парламенту та Ради якою внесено зміни до Директиви 93/13/EEC (несправедливі умови контракту), Директиви 98/6/EU (зазначення ціни), Директиви 2005/29/EU (недобросовісна комерційна практика) та Директиви 2011/83/EU (права споживачів).

[11] *https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:304:0064:0088:en:PDF*

[12] *https://eur-lex.europa.eu/eli/dir/2019/2161/oj*

Основні зміни, внесені новою Директивою:

- Збільшення штрафних санкцій за різноманітні порушення.
- Вимога до більшої прозорості в Інтернеті, зокрема до рейтингу результатів пошуку та персоналізованих цін.
- Розширення прав споживачів на «безкоштовний» цифровий вміст та послуги.

Директива привертає до себе увагу завдяки збільшенню штрафних санкцій до 4% річного обороту торговця в державі-члені (або державах-членах), де сталося порушення, або до 2 мільйонів євро у випадках, коли інформація про обсяг товарообігу відсутня, з можливістю для кожної держави-члена ЄС запровадити ще більші штрафи. Директива також надає споживачам нові індивідуальні засоби правового захисту, на кшталт права на компенсацію за несправедливу комерційну практику.

Ще один документ із Додатку XXXIX до Угоди про асоціацію, який втратив чинність - Регламент (ЄС) № 2006/2004 Європейського Парламенту та Ради від 27.10.2004 про співробітництво між національними органами, відповідальними за виконання законів щодо захисту споживачів (Регламент про співробітництво щодо захисту споживачів). На заміну скасованому був прийнятий Регламент (Regulation (EU) 2017/2394) про співпрацю між національними органами влади, відповідальними за реалізацію законів про захист прав споживачів, і встановлює рамки співпраці, що дозволяють національним органам влади з усіх країн європейського економічного простору спільно розглядати порушення споживацьких прав, коли торговець та споживач знаходяться в різних країнах.

У сукупності національні органи виконавчої влади із захисту прав споживачів утворюють європейську правозастосовну мережу (ЄПМ). Більш детальна інформація щодо Мережі з питань співпраці у справах захисту прав споживачів можна знайти на веб-сторінці Європейської Комісії.

Національні органи виконавчої влади із захисту прав споживачів відтепер мають значні повноваження щодо боротьби з незаконною практикою та виявлення торговців-шахраїв. Вони можуть запитувати інформацію у реєстраторів доменів та банків, щоб виявити особу відповідального торговця, здійснювати таємні покупки, наприклад, перевірити на предмет дискримінації споживачів за географічним принципом чи перевірити умови післяпродажного обслуговування та видати розпорядження про негайне видалення веб-сайтів, які пов'язані із проявами шахрайства.

Європейська Комісія (ЄК) координує співпрацю між цими органами влади, з метою контролю, щоб законодавство про права споживачів послідовно застосовувалось і виконувалось на єдиному ринку. Тепер ЄК може тісно співпрацювати з ЄПМ та координувати загальноєвропейські заходи по боротьбі з практиками, які шкодять значній більшості споживачів ЄС.

З набранням чинності Положенням про співпрацю у сфері захисту прав споживачів відбулась модернізація споживчого законодавства та його правозастосування у транскордонній торгівлі і відтепер санкції за порушення споживчого законодавства можуть досягати 4% обороту підприємств у відповідних державах-членах. Це є наслідком послідовної політики Європейської Комісії щодо забезпечення високого рівня захисту споживачів, особливо в транскордонних договорах. Збільшення довіри споживачів до різних форм торгівлі позитивно впливає на підвищення рівня споживання і, у свою чергу, на пришвидшення темпів економічного розвитку країн ЄЕП.

Новий документ надає національним органам розширені повноваження щодо виявлення недобросовісних практик та спільних швидких дій для їх припинення, зокрема дозволяється видавати приписи на видалення веб-сайтів, використовувати методи оцінки шляхом «таємних покупок», видавати розпорядження про повернення коштів споживачам або відшкодування завданих їм збитків, а також вимагати інформацію у реєстраторів доменів, постачальників послуг Інтернету та банків для виявлення торговця, що порушує права.

Окрім цього, Положенням передбачено право вживати заходів щодо попередніх порушень, втім за умови позовної давності не більше п'яти років.

Слід зазначити, що Положення про співпрацю між національними органами влади, відповідальними за реалізацію законів про захист прав споживачів має два формати застосування, в залежності від ступеня поширення порушення:

1. Поширені порушення. Держави-члени можуть розпочинати скоординовані дії у разі порушень споживчого законодавства ЄС, що зачіпають принаймні дві держави-члени;
2. Поширені порушення за загальноєвропейським виміром. Єврокомісія сама координуватиме всі необхідні дії та підтримуватиме зв'язок із відповідними національними органами влади, якщо порушення стосуються щонайменше двох третин держав-членів та двох третин населення ЄС.

В той же час, якщо порушення споживчого законодавства не відповідає жодній з цих двох категорій, держави-члени все одно можуть звертатися за допомогою до інших держав-членів на основі механізму взаємодопомоги.

Положення має на меті сприяти гармонізації законів про захист прав споживачів але не передбачає загальноєвропейського режиму покарання винних, а отже до порушників застосовуватимуться внутрішні режими покарання, які діють у кожній конкретній країні.

Окрім цього, експерти Європейської комісії напрацювали низку доповнень до Директиви про електронну комерцію (Directive 2000/31/EC), адже з моменту прийняття Директиви у 2000 році, з'явились нові та інноваційні послуги інформаційного суспільства (цифрові), які змінюють повсякденне життя громадян ЄС, формують та змінюють спосіб їх комунікації, споживання та ведення бізнесу. Ці послуги глибоко сприяли соціальним та економічним перетворенням у ЕС та в усьому світі, а криза коронавірусу показала важливість цифрових технологій у всіх аспектах сучасного життя. Водночас використання цих послуг також стало джерелом нових ризиків та викликів як для суспільства в цілому, так і для осіб, які користуються такими послугами.

Щоб належним чином відреагувати на нові виклики, експерти розробили проєкт Регламенту про єдиний ринок цифрових послуг (Закон про цифрові послуги) та внесення змін до Директиви 2000/31/ ЕС[13].

Зважаючи на зазначене вище, Додаток XXXIX до Угоди про асоціацію потребує оновлення аби передбачити для імплементації належні документи. До того ж, слід визначити перелік заходів, які дозволять суттєво пришвидшити темпи гармонізації вітчизняного законодавства в частині захисту прав споживачів.

[13] *https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN*

ПЛАН-ГРАФІК ЕКСПЕРТИЗИ ТА ОЦІНКА ВПЛИВУ ВПРОВАДЖЕННЯ

Ares(2020)2877686 - 04/06/2020

Цей документ містить план-графік експертизи та оцінку впливу впровадження нормативного акту й має на меті поінформувати громадян і всіх причетних про проведену Єврокомісією роботу. Це вможливить надання відгуків стосовно планованої ініціативи, а в подальшому — активну участь у консультаційних заходах. Зокрема, громадянам і всім причетним пропонується висловити погляди щодо розуміння Комісією поточної ситуації, задач і можливих розв'язків, а також надати інформацію, яку вони, можливо, мають, щодо ймовірного впливу різних варіантів.

НАЗВА ІНІЦІАТИВИ	Пакет закону про цифрові служби: розбудова Внутрішнього ринку й уточнення обов'язків у сфері цифрових служб
КЕРІВНИЙ ГД — ВІДПОВІДАЛЬНИЙ ПІДРОЗДІЛ — № АР	CONNECT F.2
ІМОВІРНИЙ ТИП ІНІЦІАТИВИ	Законодавчий акт
ОРІЄНТОВНИЙ ПЛАН	4 квартал 2020 р.
ДОДАТКОВА ІНФОРМАЦІЯ	—

Цей документ «План-графік експертизи та оцінка впливу впровадження» надається винятково з метою інформування. Він не впливає на остаточне рішення Комісії щодо того, чи буде реалізована ініціатива, зарівно як і на її зміст в остаточному вигляді. Усі описані в цьому документі складники ініціативи, включно з графіком, можуть бути змінені.

A. Обставини, експертиза, постановка задачі, перевірка субсидіарності

Обставини

Європейська Комісія оголосила[1], що має намір запропонувати нові й переглянуті правила розбудови Внутрішнього ринку цифрових служб шляхом розширення й узгодження обов'язків і сфер відповідальності щодо цифрових служб, зокрема, онлайн-платформ, а також посилити нагляд і контроль за цифровими службами в ЄС.

«Горизонтальна» нормативна база щодо цифрових служб[2] залишається незмінною з часу затвердження Директиви з електронної комерції в 2000 р. Директива узгодила базові засади, що вможливили транскордонну дію служб, і стала наріжним каменем регулювання цифрових служб у ЄС. На додачу, кілька заходів, ужитих на рівні ЄС у вигляді законодавчих актів[3],

[1] *Цифрова стратегія. Як сформувати цифрове майбутнє Європи. 19 лютого 2020 р. https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf*

[2] *У цьому документі термін «цифрова служба» використовується як взаємозамінний із терміном «служба інформаційного суспільства» й означає: «будь-яка служба, переважно платна, що діє дистанційно, електронними засобами та на окремий запит абонента» (Директива ЄС 2015/1535).*

[3] *Деякі нормативні акти щодо незаконних товарів і матеріалів: Регламент нагляду за ринком, переглянута Директива з аудіовізуальних медіаслужб, Директива із застосування прав інтелектуальної власності, Директива з авторського право на єдиному цифровому ринку, Регламент нагляду за ринком і відповідності товарів нормативам, Проект регламенту запобігання поширенню в Інтернеті терористичних матеріалів, Директива з боротьби проти сексуальної наруги над дітьми, їхньої сексуальної експлуатації та дитячої порнографії, Регламент ринкового обігу й використання матеріалів для виготовлення вибухівки тощо. У Директиву з повнішого застосування*

необов'язкових до виконання норм[4] і добровільної співпраці[5], мали на меті усунення недоліків, пов'язаних із конкретними незаконними чи шкідливими діяннями в Інтернеті користувачів цифрових служб, зокрема, онлайн-платформ.

Техніка, бізнес-моделі й задачі, що стоять перед суспільством, невпинно розвиваються. Широкий асортимент цифрових служб — це фундамент дедалі більш цифровізованого світу. До нього належить і широкий спектр таких служб, як хмарна інфраструктура та мережі розподілу контенту. Такі онлайн-платформи, як пошукові системи, торговельні майданчики, соціальні мережі й платформи спільного доступу до мультимедіа виступають як посередники у великому колі видів діяльності й відіграють особливо важливу роль у тому, як громадяни спілкуються, обмінюються інформацією і споживають її, як підприємства ведуть в Інтернеті господарчу діяльність та які товарі й послуги пропонуються споживачам. Найголовніші функції більшості онлайн-платформ — реклама й рекомендаційна система.

Це наслідок цифрової трансформації, що дав істотний корисний ефект, але й призвів до нових ускладнень. Наприклад, продаж в Інтернеті фальсифікованих, небезпечних та інших незаконних товарів створює ризик для громадян і шкодить легальним підприємствам. Деякі користувачі визискують цифрові служби для поширення в Інтернеті такого незаконного контенту, як дитяча порнографія або ненависницька риторика. Крім того, мають місце порушення прав власності. Ризики пов'язані також із тим, що цифровими службами та покладеними в їхню основу алгоритмічними процесами систематично зловживають, щоб інтенсивніше розповсюджувати в Інтернеті дезінформацію. Під загрозою також безпека вразливих користувачів, особливо дітей. Пандемія COVID-19 наочно показала і те, наскільки важливі цифрові служби, і те, наскільки вони вразливі. Далі, викликають занепокоєння вплив користування онлайн-платформами на суспільство, а також пов'язані з ними перспективи й ускладнення для найманих працівників і фізичних осіб, які пропонують послуги через платформи.

Щоб дієво усувати недоліки й запобігати подальшому роздрібненню законодавчої бази внутрішнього ринку, Комісія взяла на себе зобов'язання актуалізувати «горизонтальні» правила, що визначають певні обов'язки й сфери відповідальності різних цифрових служб. За цих обставин мета планованої Єврокомісією пропозиції нового Закону про цифрові служби полягає, без надмірної деталізації, в тому, щоб розбудовувати внутрішній ринок цифрових служб, створити чіткіші, суворіші й більш узгоджені засади визначення сфер їх відповідальності, щоб поліпшити безпеку громадян в Інтернеті й захистити їхні засадничі права, водночас посилюючи дієве функціювання внутрішнього ринку, спрямоване на поширення інновацій, розвиток і конкурентоспроможність, особливо в стосунку до європейських цифрових інноваторів, підприємств, які нарощують масштаби діяльності, малих і середніх підприємств і нових учасників

й модернізації правил захисту споживачів у ЄС додані вимоги щодо прозорості, яку торговельні майданчики в Інтернеті мають забезпечувати для користувачів. Набувають чинності в травні 2022 р.

[4] Комісія впровадила також загальні настанови для онлайн-платформ і Держав-учасниць щодо дій із незаконними матеріалами в Інтернеті в Комюніке (2017) та Рекомендації (2018).

[5] Наприклад, Інтернет-форум ЄС проти онлайн-пропаганди тероризму, Кодекс поведінки в сфері протидії незаконній ненависницькій риториці в Інтернеті, Спілка за поліпшення захисту малолітніх згідно з Європейською стратегією «Кращий Інтернет для дітей» та всесвітньою спілкою за подолання сексуальної експлуатації дітей в Інтернеті WePROTECT, Спільна дія органів, що входять до мережі співпраці з захисту споживачів, Угода про Протокол про наміри щодо фальсифікованих товарів, Протокол про наміри щодо реклами в Інтернеті та прав інтелектуальної власності, Петиція про безпеку з метою поліпшення безпечності товарів, що продаються через Інтернет. Згідно з засадами Регламенту співпраці в сфері захисту споживачів (CPC), органи захисту споживачів вжили декілька узгоджених заходів, спрямованих на забезпечення дотримання законодавства про захист споживачів у ЄС різними платформами (наприклад, операторами бронювання подорожей, соціальними мережами, ігровими онлайн-платформами, веб-крамницями). Прийнято також низку нормативів для забезпечення вільних і справедливих виборів — https://ec.europa.eu/commission/presscorner/detail/en/IP_18_5681.

ринку. У цій Оцінці впливу впровадження висвітлено логіку впровадження нового нормативного акту.

Питання, розглянуті в цій Оцінці впливу впровадження, тісно пов'язані з заходами, які Комісія вивчає додатково:

- В окремій Оцінці впливу впровадження розглядаються можливі варіанти передбачуваного законодавчого акту для онлайн-платформ, що мають дуже великий масштаб та істотно впливають на мережу, бо діють як куратори внутрішнього ринку ЄС. Цей акт має ввійти в пакет Закону про цифрові служби, запланованого на кінець 2020 р.[6]
- Зважаючи на оголошену експертизу й, можливо, перегляд правил конкуренції в ЄС у цифрову добу, до окремої Оцінки впливу впровадження включено перелік можливих варіантів нового засобу сприяння конкуренції, який мав би доповнити наявну нормативну базу ЄС щодо конкуренції й застосовуватися до всіх галузей економіки (зокрема, підтримувальні інфраструктури окремих платформ і цифрові торговельні майданчики).
- Комісія також реалізує програму відповідності й дотримання нормативних показників (REFIT) стосовно Директиви ЄС із загальної безпеки продукції (GPSD). Ознайомчі й консультаційні заходи стосовно двох зазначених актів будуть ретельно ув'язані з метою забезпечення несуперечливості нормативної бази.
- Комісія також «розгляне шляхи поліпшення умов праці найманих працівників платформ»[7], для чого розгорне широке обговорення умов праці з урахуванням економічних чинників платформ і проведе консультації з низки питань, що вже відкрито обговорюються в стосунку до Закону про цифрові служби.

Комісія переглядає Зведення правил щодо дезінформації з прицілом на запобігання поширенню дезінформації та опрацювання Плану дій європейської демократії, щоб відшукати способи зменшення можливості маніпулювання в суспільному просторі.

Експертиза

Перед оцінюванням впливу Закону про цифрові служби Комісія проведе експертизу Директиви з електронної комерції, згідно з засадою «найперше — експертиза» Настанови з поліпшення регулювання.

Зазначена Директива стосується всіх служб інформаційного суспільства — від базової структури Інтернету (наприклад, провайдерів) до онлайн-посередників, як-от веб-хостингу, хмарних служб і онлайн-платформ.

Її основні цілі:

1. Розбудовувати єдиний ринок, формувати базові умови для впровадження цифрових інновацій та швидкого й дієвого застосування, що ґрунтується на засадах керування з країни реєстрації — механізму співпраці держав-учасниць із транскордонних питань, а також гарантувати свободу заснування й свободу транскордонної реалізації цифрових служб у Євросоюзі.

[6] Комюніке Єврокомісії від 19 лютого 2020 р. Як сформувати цифрове майбутнє Європи https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en

[7] Робота платформи може бути описана як діяльність, у якій онлайн-платформу використовують, щоб уможливити організаціям або фізичним особам доступ до інших організацій або фізичних осіб з метою розв'язання задач або надання послуг в обмін на платню.

2. Особливі положення стосовно підкатегорії служб посередництва щодо контенту інших осіб (наприклад, провайдерів Інтернету, хмарних служб, веб-хостингу чи онлайн-платформ) спрямовані на те, щоб уможливити їхнє дієве функціювання на внутрішньому ринку завдяки узгодженню звільнення від відповідальності за незаконний контент по всьому єдиному ринку. Відповідна мета полягає в тому, щоб сприяти цифровим інноваціям і, водночас, захистити свободу висловлювання користувачів.
3. Посилити довіру до цифрових служб, зокрема, завдяки забезпеченню високого рівня захисту користувачів і прозорості цифрових служб.

Цілком очевидно, що зазначені цілі й досі актуальні. Основні засади Директиви стали наріжним каменем внутрішнього ринку цифрових служб. Їхній базис так само актуальний нині, як 20 років тому, потрібні хіба що деякі уточнення. Вихідні дані для експертизи збиратимуть у процесі нагромадження фактів, значною мірою пов'язаних із юридичними й економічними перепонами, що виникають на внутрішньому ринку цифрових служб. Предметами експертизи будуть дієвість, ефективність, актуальність, несуперечливість та ціннісний внесок ЄС у систему нормативів. При цьому братимуться до уваги останні документи, наприклад, Рекомендація 2018 р. щодо заходів дієвої боротьби з незаконним контентом в Інтернеті, а також зміни в характері й різноманітності цифрових служб і ризики, що з них випливають, особливо через стале збільшення користування службами, оператори яких — не резиденти Євросоюзу й тому на них не поширюється дія Директиви з електронної комерції. Оцінювання покриватиме весь період від набуття чинності Директивою до поточного часу. Використовуватиметься порівняльна методика та матеріали, попередньо опубліковані в звітах про впровадження (2003 і 2012), а також матеріали новіших, у тому числі, незакінчених досліджень. Нагромадження фактів буде зосереджено на останніх 10 роках, бо саме цей період знаменувався бурхливим розвитком служб інформаційного суспільства, нових форм поведінки в Інтернеті й практики правозастосування.

Негативні явища, що їх покликана нейтралізувати ініціатива

Швидкий і повсюдний розвиток цифрових служб був і залишається осереддям цифрової трансформації, в тому числі, підйому електронної комерції й безпрецедентних перспектив вільного поширення інформації в Інтернеті. Корисний ефект цієї трансформації не викликає сумнівів, проте масштаб негативних явищ, зумовлених цифровими службами, істотно змінився за останні 20 років. Так, помітний вплив справляє онлайн-торгівля фальсифікованими, небезпечними й недозволеними товарами, а також іншими товарами, обіг яких незаконний (зокрема, товарами, що ввозяться торговцями з-поза ЄС), а також розповсюдження через Інтернет протизаконного контенту, наприклад, ненависницької риторики й дитячої порнографії.

Через значний розвиток посередництва в поширенні інформації в Інтернеті виникла низка цілком нових явищ: системи та онлайн-реклама відіграють важливу роль в оптимізації доступу споживачів до інформації. Водночас, службами зловживають, щоб поширювати шкідливий контент, як-от дезінформацію (хоч саме по собі це й не порушує законів), експлуатуючи при цьому певні риси застосованих алгоритмів, щоб пришвидшити поширення згаданого контенту.

Ці негативні явища істотно впливають на засадничі права в Інтернеті та належний розподіл відповідальності між причетними, як у приватному, так і в державному секторах...

Відносні масштаби і вплив цих явищ найважливіші там, де найзначніші онлайн-платформи структурують величезну кількість інформаційних потоків в Інтернеті, бо ці області цифрового світу, фактично, перетворилися на «загальнодоступні простори».

На рівні ЄС уже здійснено низку цілеспрямованих заходів у певних галузях, тим не менше, істотні прогалини ще не закриті, реакції на юридичні тягарі немає.

В ході оцінювання впливу будуть детально проаналізовані подані далі негативні явища.

1. Роздрібнення Єдиного ринку й потреба посилення транскордонної співпраці

У відповідь на дедалі більшу роль цифрових служб у торгівлі й розповсюдженні незаконних товарів і контенту в Інтернеті Держави-учасниці приймають закони, якими встановлюють істотно різні рівні відповідальності цифрових служб, зокрема, онлайн-платформ, і різні механізми правозастосування. Цим створюється роздрібнення єдиного ринку, що може негативно позначитися на громадянах і підприємствах ЄС, бо правила та обов'язки не узгоджені. Це також призводить до браку правової визначеності й чіткості в стосунку до цифрових служб на внутрішньому ринку та, ймовірно, меншої дієвості в плані досягнення цілей державної політики, заради яких і приймалися згадані закони.

Схоже, що наявних механізмів транскордонної співпраці не вистачає для усунення негативних явищ на місцях, спричинених користуванням онлайн-платформами. Більш міцна, систематична й маневрена співпраця між державними установами на основі спільних правил запобігання обігу незаконних товарів і контенту посилила б взаємну довіру та дієвість правозастосування. Слід розглянути також порядок дій у стосунку шкідливого, але не конче протизаконного контенту, який забезпечував би чітке розрізнення цих двох категорій. Це забезпечило б поліпшення захисту користувачів і вдосконалення функціювання єдиного ринку, особливо в сполученні з можливістю збирати всю відповідну інформацію з платформ. Буде взято до уваги досвід наявних структур співпраці (наприклад, BEREC, CPC Network, RAPEX), а також такі нововведення, як AVMSD, що надає органам регулювання обігу аудіовізуального контенту нові механізми дії та співпраці, зокрема, в Групі європейських органів регулювання аудіовізуальних медіаслужб (ERGA).

Розвиток системи державного регулювання й ринку породжує ризики для конкурентоспроможності на внутрішньому ринку через обмеження свободи заснування цифрових підприємств і свободи надання транскордонних послуг для цих останніх. Оператори інноваційних цифрових служб, поставлені перед можливістю виникнення 27 різних правових режимів у ЄС, прагнутимуть зростання й розбудови Єдиного ринку, щоб скористатися з його корисного ефекту, бо в іншому разі витрати, спричинені неузгодженістю правил і процедур, витримають і залишаться на ринку лише найбільші платформи. Це негативно позначиться й на дієвості, повноті й узгодженості захисту європейців на всьому єдиному ринку.

2. Ризики для безпеки громадян в Інтернеті й захист їхніх засадничих прав

Онлайн-платформи й далі відіграють істотну роль у поширенні незаконних товарів, послуг і контенту через Інтернет. За відсутності чіткого розподілу обов'язків на рівні ЄС щодо цифрових служб узагалі й платформ зокрема, різні служби забезпечують різні рівні захисту безпеки громадян в Інтернеті. Коли платформи все ж таки вживають заходів проти незаконної поведінки, вони наражаються на невизначеність наявної нормативної бази (особливо в тому, що стосується добровільних заходів із виявлення незаконного контенту).

Водночас, засоби захисту прав користувачів, в тому числі, свободи одержання й поширення інформації, не скрізь однаково надійні.

У численних випадках платформи приймають рішення приватно, без підзвітності, а чинна нормативна база не дозволяє глибоко вивчати те, як вони формують потоки інформації в Ін-

тернеті, зокрема, яку роль відіграють агрегатори онлайн-реклами. Подальше поглиблення співпраці операторів служб із державними органами потрібно також, щоб забезпечити досягнення цілей державної політики у сферах убезпечення й безпеки.

На додачу, дія Директиви з електронної комерції не поширюється нині на служби, резидентні поза межами ЄС, водночас служби операторів-нерезидентів, набувають у ЄС дедалі більшої ваги. Це стосується як електронної комерції, так і соціальних мереж. Зараз вони практично не регулюються.

3. Значна асиметрія інформованості та недієвість нагляду на єдиному ринку

У нинішній нормативній базі бракує нагляду за цифровими службами. Натомість існує значна асиметрія інформованості зазначених служб та їхніх користувачів (громадян і підприємств), а також державних органів. Звіти про прозорість, що їх публікують онлайн-платформи, описуючи вжиті заходи запобігання поширенню незаконних товарів і контенту, переважно добровільні, необ'єктивні й погано надаються до порівняння даних різних служб. Крім цього, коли служби вживають заходів проти «шкідливого» контенту, що не є незаконним як такий, такі заходи та їхні наслідки —зменшення шкоди окремим особам і суспільству, але шкода свободі висловлювання — важко проаналізувати детально. Немає жодної структурованої та юридично зобов'язальної системи співпраці чи діалогу з питань, що постають, наприклад, із непередбачених ускладнень, пов'язаних із «шкідливим» контентом або непередбаченими прийомами маніпулювання службами платформ. Цей розрив у підзвітності стосується й алгоритмічних процесів, уживаних онлайн-платформами, наприклад, рекомендаційних систем, засобів модерації контенту або розміщення реклами.

Засади дій ЄС (нормативні засади й перевірка субсидіарності)

Дії спрямовані на свободу заснування та реалізації служб та належне функціювання Єдиного ринку цифрових служб. Нормативна основа як така — це, ймовірно, стаття 114, а також, можливо, статті 49 і 56 Договору про функціювання Європейського Союзу.

Зважаючи на засадничо транскордонний характер численних цифрових служб та ризики й перспективи, що вони несуть, найкраще реагувати на рівні ЄС у цілому. Жодна з Держав-учасниць, діючи окремо, практично не буде в змозі досягти поставлених цілей.

Б. Цілі й варіанті політики

Загальна мета полягає в тому, щоб створити сучасну нормативну базу для цифрових служб, чим посилити Єдиний цифровий ринок і забезпечити наявним у ЄС операторам цифрових служб можливість діяти відповідально, завдяки чому нейтралізувати ризики, що випливають з користування службами, поважаючи при цьому права й цінності ЄС і захищаючи засадничі права. Ця ініціатива має на меті організувати врівноважене й дієве порядкування в цьому секторі Інтернету, а також чітко визначити ролі, процедури й сфери відповідальності.

У базовому варіанті Комісія не вноситиме змін у чинну нормативну базу, зокрема, в Директиву з електронної комерції. Комісія здійснюватиме поточний контроль упровадження виданих Комісією Рекомендацій щодо заходів дієвої протидії незаконному контенту в Інтернеті, а також дії Директиви з авторських прав на Єдиному цифровому ринку, нещодавно зміненої Директиви з аудіовізуальних медіаслужб і Регламент щодо терористичного контенту , щойно він буде прийнятий. Подальші заходи будуть спрямовані, зокрема, на дії з саморегулювання, які поки що здійснюють добровільно лише ті служби, характер яких це дозволяє, при цьому

будуть враховані обмеження правозастосування й поточного контролю результатів. Суди й далі тлумачитимуть обов'язки нових цифрових служб згідно з наявною нормативною базою ЄС, зокрема, положеннями про служби хостингу статті 14 Директиви з електронної комерції.

Через відсутність подальших нормативних активів ЄС, імовірно, зростатиме роздрібненість. Зважаючи на транскордонний і міжнародний характер питань, сукупність розрізнених заходів в окремих країнах не забезпечить дієвого захисту громадян. Поширення незаконних товарів, що продаються через Інтернет, та розповсюдження протизаконного контенту, імовірно, триватимуть, водночас не буде узгоджених засобів протидії надмірному вилученню законного контенту. Перспективні європейські компанії наражатимуться на завади в нарощуванні діяльності на внутрішньому ринку, натомість великі онлайн-платформи захоплюватимуть дедалі більші його ділянки, тим самим перешкоджаючи конкуренції.

Далі подано загальні міркування щодо політики, на основі яких оцінюватиметься вплив інших варіантів. Підхід, наведений у варіанті 3, доповнює решту варіантів.

1. Нормативний акт обмеженої дії, що регулюватиме процедурні зобов'язання онлайн-платформ. Це матиме на меті переважно надання зобов'язального характеру «горизонтальним» положенням Рекомендації 2018 р.

- Згаданий акт розвиватиме Директиву з електронної комерції й буде спрямований на служби, резидентні в ЄС.
- Будуть упроваджені певні сфери відповідальності онлайн-платформ щодо продажу незаконних товарів і послуг, поширення незаконного контенту та інших незаконних дій їхніх користувачів. Будуть також установлені відповідні обов'язки, наприклад, дієві механізми «сповіщення-дія» в стосунку повідомлення про незаконний контент чи товари, а також дієві зобов'язання усунення недоліків, наприклад, порядок зустрічного повідомлення та обов'язковість прозорості.
- У цьому варіанті не передбачені ані тлумачення, ані актуалізація правил відповідальності платформ та інших онлайн-посередників у порівнянні з Директивою з електронної комерції.

2. Ширші зміни нормативної бази, а саме, актуалізація й модернізація правил, установлених Директивою з електронної комерції, при незмінності її основних засад.

- Будуть витлумачені й розширені правила щодо відповідальності й безпеки цифрових служб, а також усунуті положення, що нині знеохочують добровільні дії щодо незаконних контенту, товарів і послуг, посередниками яких виступають платформи, особливо в тих випадках, коли це стосується служб самих онлайн-платформ. Означення незаконності в Інтернеті ґрунтуватимуться на чинних законах і нормах ЄС і окремих країн.
- Буде узгоджений набір конкретних, зобов'язальних і домірних положень, які конкретизують різні обов'язки, зокрема, в стосунку до служб онлайн-платформ[8]. На додачу до базового набору загально застосовних зобов'язань, імовірно, знадобляться подальші асиметричні зобов'язання, що залежатимуть від типу, масштабів і (або) ризику відповідних цифрових служб, а також структура співпраці й вимоги до належного процесу в кризовій ситуації.

[8] Це узгоджується с правилами, установленими AVMSD, де впроваджено деякі зобов'язання платформ обміну відеоматеріалами (зокрема, спрямовані проти ненависницької риторики), та Рекомендацією 2018 р.

Зобов'язання можуть бути, зокрема, такі:

- узгоджені обов'язки використовувати системи «сповіщення-дія» в стосунку до незаконних товарів, контенту й послуг всіх типів, а також схему «знай клієнта» в стосунку до комерційних користувачів торговельних майданчиків;
- правила, що забезпечують дієву співпрацю операторів цифрових служб із компетентними органами й «надійними сигналізаторами» (наприклад, «гарячими лініями» INHOPE для найшвидшого усунення дитячої порнографії), а також, у разі необхідності, повідомлення;
- можливо, обов'язкове оцінювання онлайн-платформами ризиків, пов'язаних із питаннями визискування їхніх служб для поширення певних категорій шкідливого, хоча й не протизаконного контенту, наприклад, дезінформації;
- більш дієве усунення недоліків і захист від необґрунтованого видалення законного контенту й товарів в Інтернеті;
- комплекс зобов'язань прозорості й звітності в зазначених процесах.
- Крім цього, слід врегулювати зобов'язання щодо прозорості, повідомлень та незалежного аудиту, спрямовані на забезпечення підзвітності алгоритмічних систем (автоматизованої) модерації контенту й рекомендаційних систем, реклами й комерційних повідомлень в Інтернеті, в тому числі, політичної реклами, а також певних аспектів мікротаргетингу, що виходять за межі прав і обов'язків захисту особистих даних. Зазначені заходи уможливлять дієвий нагляд за онлайн-платформами і сприятимуть боротьбі проти дезінформації в Інтернеті. Слід також врегулювати питання юридичної зрозумілості, пов'язані зі смарт-контрактами.
- Буде розглянуто поширення застосування згаданих заходів до всіх служб, спрямованих на єдиний європейський ринок, зокрема, резидентних поза ЄС, з метою виявлення найбільш дієвих способів правозастосування.
- Нормативний акт упровадить також знеохочувальні й домірні санкції за систематичний брак дотримання узгоджених обов'язків або порушення засадничих прав.

3. Варіанти створення дієвої системи регуляторного нагляду, правозастосування та співпраці між Державами-учасницями за підтримки на рівні ЄС. Ці варіанти доповнюють попередні й мають за мету посилення актуалізованого набору правил (який відповідатиме наведеним вище варіантам 1 і 2). Вони мають забезпечити дієве порядкування цифровими службами в усьому ЄС завдяки достатньому рівню узгодження правил і процедур. Ці варіанти ґрунтуються на принципі країни походження й мають дозволити державним органам Країн-учасниць боротися проти незаконних контенту, товарів і послуг в Інтернеті. Зокрема, в регуляторних і наглядових нормах мають бути налагоджені процедури швидкої та дієвої співпраці з транскордонних питань. Державні органи отримають більше можливостей нагляду за цифровими службами завдяки належним повноваженням впроваджувати дієві й знеохочувальні санкції за систематичні порушення службами в їхній юрисдикції відповідних обов'язків, імовірно, встановлених на рівні ЄС. Мають бути вивчені також варіанти дієвого усунення недоліків за судовими приписами.

В усіх варіантах буде забезпечена відповідність галузевим регуляторним нормам, наприклад, Директиві з авторського права на Єдиному цифровому ринку, переглянутій Директиві з аудіовізуальних медіаслужб, проектові Регламенту щодо терористичного контенту в Інтернеті, а також міжнародним зобов'язанням ЄС. Упровадження нового нормативного акту не вимагатиме змін у правилах, установлених актами, які нещодавно набули чинності чи існують у проектах, а доповнюватиме ці правила шляхом актуалізації «горизонтальних» правил у стосунку до цифрових служб.

B. Початкове оцінювання очікуваного впливу

Вплив кожного з варіантів оцінюватиметься за поданими далі категоріями.

Імовірний економічний вплив

Очікуваний економічний вплив пов'язаний переважно з корисним ефектом усунення юридичних перепон для цифрових служб на внутрішньому ринку та підвищення правової визначеності. В ході оцінювання його зіставлятимуть із витратами на узгодження правил для згаданих служб в усьому ЄС. Особлива увага приділятиметься впливові на інноваційні європейські малі й середні підприємства та їхню спроможність нарощувати діяльність на внутрішньому ринку ЄС у транскордонному режимі. Вирішальним чинником уможливлення швидкого економічного відновлення після кризи COVID-19 буде конкурентоспроможність цифрових служб. Міцна галузь цифрових служб стане, значною мірою, локомотивом зростання й уможливить поступ низки похідних послуг, у тому числі, торгівлі товарами. Буде також наявний непрямий позитивний ефект для підприємств, що спеціалізуються в законних товарах і послугах, наприклад, якісні медіаслужби.

Ще одним предметом оцінювання буде вплив на операторів служб, резидентних поза межами ЄС, за умови, що це передбачатиме варіант 2.

В ході оцінювання економічного впливу враховуватиметься масштаб відповідних операторів служб, їхні можливості, а також витрати на чинні зараз механізми.

Імовірний соціальний вплив

Важливо, що цифрові служби, від інфраструктурних до посередницьких стосовно інформаційних потоків — це засадничий засіб обміну інформацією. Переконання в тому, що безпека громадян запевнена, сприятиме ширшому розповсюдженню цифрових служб. У ході аналізу оцінюватиметься вплив на захист споживачів від незаконних товарів, що продаються через Інтернет, зменшення кількості ненависницької риторики, краща захищеність малолітніх. Братимуться до уваги нові системні шкідливі чинники, що впливають на суспільство й демократичні системи. Розглядатимуться також можливості державних органів дієво забезпечувати застосування законів до подій в Інтернеті.

Імовірний вплив на довкілля

Передбачається, що в усіх варіантах вплив на довкілля майже не відрізнятиметься від наявного. Початкова оцінка не дає підстав передбачати, що ініціатива призведе до збільшення впливу цифрових служб на довкілля, бо абсолютні обсяги електронної комерції не поменшають у порівнянні з нинішнім станом, незважаючи навіть на прогнозоване істотне зменшення перевезень незаконних товарів. Проте, зважаючи на різноманіття галузей, де діють онлайн-платформи (туризм, продаж товарів, транспорт тощо), наслідки для довкілля можуть також бути різні. Тому в ході оцінювання впливу слід проаналізувати їх досить детально.

Імовірний вплив на засадничі права

Як свідчать прецеденти Суду Європейського Союзу (СЄС) і Європейського суду з прав людини (ЄСПЛ), регулювання посередницької діяльності впливає на низку засадничих прав. Це

стосується, зокрема, свободи отримання та поширення інформації та думок без втручання державних органів і незалежно від кордонів, а також право на ефективні засоби правового захисту.

В ході оцінювання варіантів братиметься до уваги можливість створення на рівні ЄС у цілому системи належних і дієвих стримувань і противаг, яка забезпечить згадані засадничі права в Інтернеті.

Особлива увага приділятиметься прямим ефектам і заохоченням, які могли б призвести до обмеження того чи іншого засадничого права. У тих випадках, коли є ризик реалізації такого небажаного впливу, будуть розроблені заходи реагування, що забезпечать усунення негативних явищ і справедливу рівновагу для захисту прав в Інтернеті, як того вимагає Хартія засадничих прав Європейського Союзу та міжнародні норми.

Інші засадничі права, які мають бути розглянуті, стосуються, зокрема, захисту персональних даних і приватності, недопущення дискримінації, забезпечення гендерної рівності, свободи зборів, прав дитини, права на ефективний правовий захист, свободу підприємництва й захист інтелектуальної власності.

Імовірний вплив на спрощення та (або) адміністративний тягар

Хоча всі варіанти прогнозовано тягнуть за собою певні витрати державних органів на безперешкодне впровадження й співпрацю, ці витрати, ймовірно, компенсує істотне підвищення ефективності правозастосування в усьому ЄС. Цей аспект також буде розглянуто в ході оцінювання впливу.

Г. Доказова база, збирання даних і засоби поліпшення регулювання

Оцінювання впливу

Після експертизи Директиви з електронної комерції буде проведено Оцінювання впливу з метою уточнення аналізу задач і варіантів політики та порівняння їхнього впливу. Передбачається, що Оцінювання впливу буде закінчено, а його результати подано до Ради регуляторної експертизи Європейської Комісії в другому півріччі 2020 р.

Доказова база та збирання даних

Експертиза й оцінювання впливу ґрунтуватимуться на детальних доказах, нагромаджених за останні роки[9], зокрема, в ході правового оцінювання стану впровадження Директиви з електронної комерції, а також доказів дедалі більшої правової роздрібненості. Додатково в ході структурованих діалогів і добровільної співпраці, узгоджуваних Єврокомісією в кількох сферах політики, регулярно збираються деталізовані дані про конкретні типи незаконного контенту й товарів, наприклад, небезпечні вироби, протизаконна ненависницька риторика, дитяча порнографія (тут також нагромаджуються відомості, отримані завдяки співпраці правоохоронних органів, гарячих ліній і підприємств галузі), фальсифікована продукція, поши-

[9] *Деякі з джерел представлені докладно в додатках до Оцінювання впливу, проведеного в 2018 р. https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-preventing-terrorist-content-online-swd-408_en.pdf*

рення терористичного контенту. Дані збиратимуться також у межах паралельної ініціативи з експертизи й перегляду Директиви з загальної безпеки продукції.

Нарешті, Єврокомісія започаткує цільові дослідження, пов'язані, зокрема, з економічним аналізом, результати якого будуть покладені в основу оцінювання, найновішими досягненнями в техніці модерації контенту в Інтернеті та розвитком певних цифрових служб.

Стратегія консультацій

Експертиза й оцінювання впливу ґрунтуватимуться на консультаціях з широким колом причетних, які матимуть три основні цілі:

- ознайомитися з думками причетних щодо наявних і майбутніх задач у середовищі цифрових служб;
- зібрати докази й конкретні дані щодо згаданих задач;
- вивчити інформовані думки щодо можливих підходів до політики, її варіантів і передбачуваного впливу.

Стратегія консультацій матиме на меті ознайомлення з думками найбільш зацікавлених причетних, зокрема: користувачів онлайн-платформ (і організацій, що представляють їхні інтереси), цифрових служб і посередників — провайдерів Інтернету, служб хмарної інфраструктури, мереж розподілу контенту, служб програмних засобів хмарного базування, операторів служб доменних імен тощо; сторонніх осіб, що працюють із системою цифрових служб (операторів засобів модерації контенту, користувачів онлайн-платформ, операторів платіжних систем, посередників обробляння даних, рекламістів, розробників контенту для Інтернету, правовласників, власників брендів тощо) і організацій, що їх представляють; організацій громадського суспільства, які представляють різні напрямки, наприклад, захист прав у цифровому просторі, захист споживачів, оборона вразливих груп і жертв, соціальних партнерів та інших підприємств і асоціацій працівників, фізичних осіб-підприємців і представників вільних професій; державних органів, закладів науки й вищої освіти; нарешті, окремих громадян.

Стратегія консультацій передбачає відкриті публічні консультації в Інтернеті, на яких спектр обговорюваних питань і задач буде ширший від обсягу цього Оцінювання впливу впровадження, а також низку цільових консультацій, зокрема, семінарів для фахівців і заходів із обміну досвідом Держав-учасниць.

Чи буде прийнятий План упровадження?

План упровадження може бути розроблений, але для цього необхідний подальший аналіз варіантів та їхньої складності в ході оцінювання впливу.