РЕГУЛЯТОРИ ЦИФРОВИХ ЗМІН: АНАЛІЗ ДОСВІДУ ЄС ДЛЯ УКРАЇНИ

Аналітичний звіт

2026

Лабораторія цифрової безпеки

МІЖНАРОДНИЙ ФОНД ВІДРОДЖЕННЯ

Співфінансується Європейським Союзом

Регулятори цифрових змін: аналіз досвіду ЄС для України. Аналітичний звіт. — Авдєєва А., Дворовий М., Людва А. — Ред. Володовська В. — Лабораторія цифрової безпеки — Київ, 2026.

У звіті проаналізовано інституційні моделі регулювання у сферах захисту персональних даних, медіа, цифрових послуг та штучного інтелекту в державах-членах Європейського Союзу та країнах Європейської економічної зони з метою оцінки їхньої ефективності, незалежності та релевантності досвіду для України в контексті євроінтеграції. Дослідження охоплює правовий статус, повноваження, організаційну структуру, фінансування та механізми взаємодії регуляторів, а також аналізує ризики надмірної концентрації повноважень у межах єдиного органу. Результати свідчать про відсутність універсальної європейської моделі та підтверджують доцільність диференційованого підходу до реформування системи цифрового врядування в Україні. На основі європейських практик сформульовано рекомендації щодо посилення/нарощування інституційної незалежності, фінансової стійкості, кадрової спроможності та міжвідомчої координації регуляторів з метою забезпечення відповідності стандартам ЄС і ефективного захисту прав людини у цифровому середовищі.

Матеріал підготовлено за підтримки Європейського Союзу та Міжнародного фонду «Відродження» в рамках спільної ініціативи «Вступаємо в ЄС разом». Матеріал представляє позицію авторів і не обов'язково відображає позицію Європейського Союзу чи Міжнародного фонду «Відродження».

ЗМІСТ

ВСТУП

Цей аналітичний звіт підготовлений на основі дослідження інституційних моделей регулювання у сферах захисту персональних даних, медіа, цифрових послуг та штучного інтелекту в державах-членах Європейського Союзу (далі — ЄС) та країнах Європейської економічної зони (далі — ЄЕЗ). У межах дослідження експерти Лабораторії цифрової безпеки проаналізували правовий статус, організаційну структуру, повноваження, моделі фінансування та механізми взаємодії регуляторів у сферах персональних даних, медіа, цифрових послуг і штучного інтелекту (далі — ШІ).

Детальніше з оглядом інституційного ландшафту держав-членів ЄС можна ознайомитись в Онлайн-довіднику «Регуляторні інституції держав-членів ЄС». Ресурс містить порівняльний огляд підходів, а також детальнішу інформацію щодо кожної окремої країни, та буде оновлюватись з урахуванням майбутніх змін, зокрема з огляду на прогрес в імплементації вимог Акту ЄС про штучний інтелект.

Метою цього аналітичного звіту є виявлення ключових підходів до формування регуляторних і наглядових органів, оцінка їх ефективності та незалежності, а також напрацювання практичних рекомендацій для вдосконалення інституційної архітектури цифрового врядування в Україні в контексті євроінтеграційних процесів.

Результати дослідження свідчать про відсутність уніфікованої моделі регулювання в державах-членах ЄС. Натомість простежується поєднання спеціалізованих та гібридних підходів, що формувалися поступово під впливом європейського законодавства, національного контексту та інституційних традицій. У більшості країн регулятори у сфері захисту персональних даних та медіа функціонують як окремі незалежні органи, тоді як у сфері цифрових послуг і ШІ поширеними є моделі делегування повноважень існуючим інституціям. Водночас поєднання кількох чутливих сфер в одному органі часто супроводжується ризиками конфлікту інтересів, перевантаження повноваженнями та зниження ефективності.

Окремий блок аналізу присвячено оцінці концепції створення Єдиного цифрового регулятора в Україні. Дослідження показує, що така модель за відсутності належних інституційних запобіжників, ресурсного забезпечення та чіткого розмежування компетенцій може створювати загрози для незалежності, операційної спроможності та прозорості регулювання. Європейський досвід свідчить, що універсальні регулятори, які охоплюють одночасно багато цифрових та суміжних сфер, є радше винятком, ніж усталеною практикою.

Для України більш оптимальним варіантом може стати поетапний і диференційований підхід до побудови системи цифрового врядування, який поєднує створення або призначення нових органів та використання уже наявних інституцій із поступовим розвитком їхніх повноважень відповідно до стандартів ЄС. Ключовими умовами ефективного регулювання залишаються інституційна незалежність, прозорі процедури призначення, фінансова автономія, достатній кадровий потенціал та чіткі механізми міжвідомчої координації.

З огляду на викладене, у звіті сформульовано рекомендації, спрямовані на забезпечення відповідності української регуляторної системи європейським стандартам, запобігання надмірній концентрації повноважень, посилення фінансової та операційної спроможності органів влади, а також розвиток експертного потенціалу та міжнародної співпраці. Реалізація цих рекомендацій має сприяти формуванню сталої, ефективної та незалежної системи регулювання цифрової сфери в Україні.

РОЗДІЛ 1. РЕГУЛЯТОРНІ ТА НАГЛЯДОВІ ІНСТИТУЦІЇ В ДЕРЖАВАХ-ЧЛЕНАХ ЄС

Держави-члени ЄС користуються широкою дискрецією щодо формування, повноважень та внутрішньої організації незалежних регуляторів. Ці органи формуються з урахуванням специфіки відповідної сфери, політичного устрою, економічного стану та національних потреб. Водночас усі держави дотримуються спільного підходу: при створенні або наділенні повноваженнями регуляторів на законодавчому рівні обов'язково враховуються вимоги EU acquis. Лише після забезпечення відповідності європейським стандартам держава-член отримує свободу у подальшому формуванні та практичній діяльності відповідного органу.

Цифролаба проаналізувала практику держав-членів ЄС, а також країн ЄЕЗ (Ісландія, Ліхтенштейн, Норвегія) щодо діяльності незалежних органів, призначених для регулювання та моніторингу виконання законодавчих вимог у сферах захисту персональних даних, медіа, цифрових послуг та ШІ.

Нижче наведемо загальний огляд вимог та практик формування і забезпечення діяльності регуляторів у цифровій сфері, які варто враховувати при визначенні моделі регуляторних та наглядових органів в Україні.

Призначення регулятора у відповідній сфері: єдиний та комбінований підходи

Підходи до призначення регуляторного або наглядового органу в окремій сфері суттєво варіюються серед держав-членів ЄС. Деякі країни, зокрема ті, що характеризуються більш стабільною економічною ситуацією, призначають окремий орган для кожної сфери, тоді як інші делегують або поєднують кілька сфер у межах одного регулятора. Водночас незмінним залишається один фактор: формування регуляторних органів у державах-членах ЄС відбувалося поступово та насамперед залежало від актів, ухвалених на рівні ЄС. Так, Загальний регламент про захист даних (GDPR), який набув чинності у 2018 році, зобов'язав усі держави-члени призначити незалежний орган для нагляду за виконанням його вимог. Це призвело до створення окремого регулятора **у сфері захисту персональних даних** у кожній державі-члені ЄС, а також в Ісландії, Ліхтенштейні та Норвегії як країнах ЄЕЗ.

Аналогічна ситуація спостерігається й **у сфері медіа**. Фактично кожна держава-член ЄС (включно з країнами ЄЕЗ) має окремого медіарегулятора, за винятком держав зі специфічним політичним устроєм. Так, у Німеччині діють чотирнадцять незалежних органів на рівні федеральних земель, які об'єднані під спільною парасолькою «Die Medienanstalten». У Бельгії, з огляду на існування трьох мовних спільнот, функціонують три незалежні регулятори: Фламандська медіарада, Французька (Валлонська) Вища рада з питань телерадіомовлення та Рада з питань медіа.

Існування окремих органів у сферах персональних даних і медіа зумовлено не лише різноманіттям питань регулювання, а й чутливістю відповідної інформації. Крім того, органи із захисту персональних даних здебільшого виконують контрольні функції, тоді як медіарегулятори поєднують їх із регуляторною діяльністю.

У сфері **цифрових послуг** єдиний підхід серед держав-членів ЄС не сформувався. Акт ЄС про цифрові послуги (DSA), що набув чинності у 2022 році, зобов'язав держави-члени призначити Координатора з питань цифрових послуг. Замість створення нового органу більшість держав делегували ці повноваження вже існуючим установам. Так,

Бельгія, Болгарія, Хорватія, Чехія, Німеччина, Греція, Литва, Мальта, Польща, Португалія, Румунія та Швеція передали функції Координатора органам у сфері електронних комунікацій. Кіпр, Франція, Ірландія та Словаччина надали ці функції медіарегуляторам. У Австрії, Фінляндії, Угорщині, Італії та Словенії Координаторами були обрані органи, що поєднують регуляторні функції у сферах медіа та електронних комунікацій. В окремих випадках Координаторами стали органи із захисту прав споживачів (Латвія, Естонія), антимонопольні органи (Люксембург) або такі, що поєднують ці сфери (Іспанія, Нідерланди, Данія).

Підходи держав-членів ЄС до регулювання **ШІ** наразі складно систематизувати у зв'язку з нещодавнім ухваленням Акта ЄС про штучний інтелект у 2024 році. Його імплементація перебуває на початкових етапах. Акт передбачає призначення двох незалежних органів: органу ринкового нагляду та нотифікуючого органу. Мальта, Данія та Італія вже розпочали впровадження відповідних положень, передавши ці функції спеціалізованим незалежним органам, діяльність яких безпосередньо пов'язана зі сферою ШІ: Управлінню цифрових інновацій (Мальта), Агентству з питань цифрового урядування (Данія) та Національному агентству з кібербезпеки (Італія). Примітно, що процес призначення відповідних органів все ще формально не закріплений, проте деякі проєкти законів вже прийняті та перебувають на стадії набрання чинності. Проєкти законів, стратегії та загальні обговорення деяких держав-членів ЄС демонструють, що функції ринкового нагляду потенційно може перебрати на себе орган регулювання у сфері електронних або телекомунікацій (Німеччина), медіа (Фінляндія), персональних даних (Люксембург) або новостворений орган (Іспанія). Поширеним також є підхід щодо делегації функцій обох регуляторів у сфері ШІ декільком існуючим органам. Втім, наразі ця практика ще формується.

Функції, обсяг повноважень та їх вплив на внутрішню структуру регуляторів

Поєднання кількох сфер регулювання в межах одного органу може призводити до дублювання або фрагментарності функцій. Для уникнення цього, держави-члени ЄС часто формують внутрішню структуру регуляторів за департаментним принципом.

Так, орган із захисту прав споживачів і технічного регулювання в Естонії має сім відділів, включно з департаментами електронних комунікацій і цифрових послуг. У Фінляндії функціонують чотири основні підрозділи, які включають Національний центр кібербезпеки та Сектор щодо інформації та майбутніх з'єднань, у Франції та Німеччині — десять і дев'ять відповідно. В Ірландії Комісія, яка регулює сфери медіа та цифрових послуг, поділена на чотири основні відділи, очолювані комісарами: Комісар з онлайн-безпеки, Комісар з медіарозвитку, Комісар з цифрових послуг, а також Комісар з питань мовлення та відео на замовлення. Окрім Комісарів, призначених для керування основними відділами, орган поділений на спеціальні підрозділи, до діяльності яких входять бюджетні, адміністративні та правові питання.

Аналіз також свідчить, що більшість органів у сфері захисту персональних даних мають виключно наглядові та контрольні повноваження, що відповідає вимогам GDPR (21 держава-член ЄС)[1]. Натомість у сферах медіа та цифрових послуг регулятори часто поєднують регуляторні, наглядові та контрольні функції. До таких держав-членів належать Австрія, Данія, Естонія, Фінляндія, Франція, Німеччина, Ірландія, Італія, Нідерланди, Португалія, Іспанія та Угорщина. Таке поєднання створює ризики конфлікту інтересів. У деяких державах (зокрема у Франції та Угорщині) це проявляється у формі політичного

[1] Хорватія, Кіпр, Чехія, Данія, Естонія, Фінляндія, Німеччина, Франція, Греція, Угорщина, Італія, Латвія, Литва, Люксембург, Мальта, Нідерланди, Польща, Португалія, Румунія, Словаччина, Швеція

впливу. В інших країнах застосовуються запобіжні механізми на законодавчому та інституційному рівнях.

Як і випадку із внутрішньою структурою органів, описаних вище, регуляторні органи, які поєднують під своєю парасолькою декілька сфер, містять відокремлені департаменти/відділи. Наприклад, в Ірландії вже відомі Комісари, які очолюють відповідні сфери, здійснюють додатковий нагляд відокремлених відділів, зокрема, відділів «Нагляду за платформами та розслідування», «Медіаландшафту» та «Політики, дослідження та стратегії». В Австрії, будь-які ризики упередженості медіарегулятора (KommAustria), який одночасно регулює діяльність у сферах медіа, цифрових послуг та деяких питаннях ШІ, пом'якшуються завдяки існуванню Управління з регулювання мовлення та телекомунікацій (RTR-GmbH). Цей орган, який здійснює здебільшого операційну діяльність щодо медіа, уповноважений оскаржувати рішення медіарегулятора в судах.[2] У Португалії, поруч із Радою директорів регулятора у сферах комунікацій та цифрових послуг, додатково призначається єдиний інспектор, який контролює, зокрема, законність рішень та дій регулятора.[3] Втім, будь-які інші інституційні складнощі, які можуть виникати у регуляторів, очевидно, публічно не адресуються на рівні держав-членів ЄС.

Наглядові органи у сфері захисту персональних даних у більшості держав-членів ЄС (Хорватія, Кіпр, Чехія, Естонія, Фінляндія, Німеччина, Угорщина, Латвія, Литва, Мальта, Польща, Румунія, Словаччина, Словенія, Іспанія, Швеція), а також в Норвегії та Ліхтенштейні із ЄЕЗ є одноосібними. Це зумовлено вузькою спеціалізацією регулювання виключно однієї сфери. Водночас у деяких державах-членах ЄС одноосібність притаманна і органам, які одночасно регулюють сфери телекомунікацій (Польща, Румунія), захисту споживачів (Латвія) або медіа (Фінляндія) зі сферою цифрових послуг.

Колегіальність органів притаманна для держав-членів ЄС (Австрія, Бельгія, Болгарія, Хорватія, Кіпр, Чехія, Данія, Франція, Німеччина, Греція, Угорщина, Ірландія, Італія, Литва, Словаччина, Іспанія), які делегували функції щодо цифрових послуг або ШІ існуючим регуляторам у сфері електронних комунікацій. Серед наглядових органів у сфері захисту персональних даних колегіальність характерна для Ірландії, Італії, Люксембургу, Нідерландів та Ісландії (ЄЕЗ).

Три моделі фінансування регуляторів

Єдиного підходу до фінансування регуляторів у державах-членах ЄС не існує. Водночас можна виокремити кілька типових моделей. В одинадцятьох державах-членах ЄС регулятори фінансуються виключно безпосередньо з державного бюджету (Чехія, Данія, Естонія, Фінляндія, Франція, Італія, Латвія, Люксембург, Польща, Словаччина, Іспанія). Поширеною є також практика бюджетного фінансування органів у сфері захисту персональних даних (Австрія, Бельгія, Болгарія, Хорватія, Кіпр, Німеччина, Греція, Литва, Мальта, Нідерланди, Румунія, Словенія, Швеція).

У сферах медіа та цифрових послуг часто застосовується самофінансування через ліцензійні збори (сфера медіа у Німеччині), власні внески (сфера медіа у Словенії, сфера цифрових послуг у Бельгії, Хорватії, Греції, Португалії, Румунії, Швеції) або обов'язкові платежі суб'єктів регулювання у сферах, що регулюються органом (сфера цифрових послуг у Нідерландах). Така модель зменшує ризики політичної залежності. Винятками є Словенія, регулятор цифрових послуг якої фінансується коштом державного бюджету, та медіарегулятори деяких держав-членів ЄС (Бельгія, Болгарія, Греція, Литва, Нідерланди, Румунія).

[2] KommAustria Act, Sections 16-17
[3] Decree-Law No.º 39/2015, Article 32

Поширеною є також змішана модель, що поєднує бюджетні кошти (основний спосіб фінансування) та внески (додатково). Вона застосовується у більшості держав-членів ЄС (Австрія, Хорватія, Кіпр, Мальта, Португалія, Швеція (сфера медіа), Болгарія, Німеччина, Литва (сфера цифрових послуг), Мальта (сфера ШІ), Португалія (сфера захисту персональних даних). Винятками можна вважати Ірландію (всі сфери регулювання), Мальту (сфера цифрових послуг) та Угорщину (сфери медіа та цифрових послуг), які, хоч і слідують змішаній моделі, більшу пропорцію фінансування все ж відносять на внески та інше фінансування.

РОЗДІЛ 2. КОНЦЕПЦІЯ ЄДИНОГО ЦИФРОВОГО РЕГУЛЯТОРА

У 2025 році Міністерство цифрової трансформації України (далі — Мінцифри) працювало над ідеєю створення Єдиного регулятора в цифровій сфері (далі — Єдиний регулятор), який забезпечуватиме імплементацію відповідних актів ЄС у напрямках:

- ШІ;
- цифрових послуг та ринків;
- захисту персональних даних;
- доступу до даних та публічної інформації;
- захисту прав дітей в цифровому просторі.

Створення нового органу, на думку представників Міністерства, може вирішити проблеми щодо фрагментарності повноважень чинних регуляторів, дотичних до цифрової сфери (як-от, Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку (НКЕК), Національна рада України з питань телебачення і радіомовлення (Національна рада) тощо), відсутності відповідних наглядових органів у неврегульованих наразі сферах (зокрема, ШІ та цифрові послуги), з додатковою оптимізацією бюджетних коштів та фінансового навантаження у контексті ефективної роботи органу.

Концепція Єдиного регулятора не була публічно представленою, проте загальний підхід щодо поєднання повноважень у перелічених сферах в єдиному органі варто проаналізувати з точки зору можливості забезпечення ефективності та незалежності в діяльності.

Відповідність вимогам ефективності

Підхід до створення Єдиного регулятора як способу вирішення проблеми фрагментарності повноважень, водночас, викликає стурбованість щодо занадто широкого обсягу завдань цього органу та здатності їх ефективно виконувати.

Ефективність роботи регулятора передбачає передовсім наявність чітко визначеної сфери компетенції та завдань, які виконуються із врахуванням вимог неупередженості, прозорості та своєчасності.[4] Орган із наглядовими функціями повинен мати у своєму арсеналі повноваження щодо забезпечення виконання зобов'язань, зокрема, здійснення розслідувань, накладення санкцій, здійснення авторизації заходів та надання консультацій у випадку розгляду скарг від фізичних осіб.[5] Водночас регуляторний орган повинен мати

[4] Digital Services Act, Article 50(1)
[5] General Data Protection Regulation, Preamble 129

необхідні технічні, фінансові та експертні ресурси для виконання поставлених завдань.[6] Це включає і автономність регулятора при організації власного бюджету та його лімітів.

З огляду на поступовість впровадження європейських регламентів із захисту даних, цифрових послуг та ринків, ШІ, в державах-членах ЄС відсутні приклади конвергентних регуляторів, які б охоплювали всі перелічені сфери. Національні регулятори у сфері захисту персональних даних існують окремо від цифрових сфер, медіа та ШІ, де застосовується гібридна модель з можливим поєднанням функцій спеціалізованих органів. Наприклад, координаторами цифрових послуг у державах-членах ЄС є здебільшого регулятори у сферах захисту прав споживачів, медіа або електронних комунікацій. Ці ж органи є кандидатами на призначення нотифікуючих органів та органів нагляду за ринками при подальшій імплементації Акту про ШІ.

Слід також звернути увагу на відокремлення цифрових та нецифрових сфер пояснюється не лише ризиком поєднання декількох чутливих сфер (зокрема, кіберзагрози для інтегрованих баз даних та масивів даних), але й обсягом повноважень, якими повинні бути наділені відповідні регулятори. Так, досвід держав-членів ЄС явно демонструє, що регулятори у сфері персональних даних уповноважені здебільшого на наглядові та контрольні функції. Натомість цифрові регулятори мають в арсеналі як регуляторні так і наглядові функції.

Поєднання усіх перелічених сфер в одній інституції створить ситуацію, коли потрібно буде реалізовувати і регуляторні, і наглядові, і контрольні функції в різних комбінаціях, іноді щодо одних і тих же суб'єктів. Це створює додаткові складнощі із формуванням чіткого переліку повноважень, їх розмежування, залежно від напрямку, та визначення додаткових гарантій від зловживання.

Власне, визначення переліку повноважень Єдиного регулятора для усіх перелічених сфер саме по собі буде нелегким завданням та надзвичайно об'ємною частиною регулювання статусу такої інституції. Розглянемо лише кілька прикладів повноважень, які мають виконувати регулятори відповідно до вимог права ЄС.

Цифрові послуги. Відповідно до Акту ЄС про цифрові послуги, орган, що буде визначений Координатором цифрових послуг відповідатиме не лише за розгляд скарг та застосування санкцій до посередників, а також має бути уповноважений на сертифікацію незалежного органу, створеного для врегулювання позасудових спорів, для об'єктивного та неупередженого розгляду скарг користувачів.[7] Аналогічна сертифікація повинна надаватися регулятором і довіреним суб'єктам, які ідентифікують та повідомляють про незаконний контент для належного захисту користувачів у мережі.[8] Крім того, необхідно передбачити механізм обміну даними між Координатором цифрових послуг та постачальниками послуг найбільших пошукових онлайн-систем — з отриманням відповідних даних регулятором та перевіреними дослідниками для моніторингу, аналізу ризиків та оцінки дотримання законодавства.[9]

Штучний інтелект. Імплементуючи вимоги Акту ЄС про ШІ, Цифровий регулятор повинен бути уповноважений не лише на оцінку ризиків високоризикових систем ШІ, але й розробку методологій для розробників щодо оцінки впливу таких систем на фундаментальні права людини.[10] Обов'язковим є також механізм розгляду скарг осіб, які зазнали впливу від рішень розробника системи ШІ.[11] Такою функцією має бути

[6] Digital Services Act, Article 50(1)
[7] Digital Services Act, Article 21
[8] Digital Services Act, Article 22
[9] Digital Services Act, Article 40
[10] Artificial Intelligence Act, Article 27
[11] Artificial Intelligence Act, Article 86(1)

наділений орган ринкового нагляду, призначення якого є обов'язковим відповідно до Акту ЄС про ШІ.[12] Водночас, іншою обов'язковою складовою імплементації європейського регламенту є призначення окремого нотифікуючого органу у сфері ШІ.[13]

Персональні дані, доступ до публічної інформації та управління даними. Окрім вимог до наглядового органу у сфері захисту персональних даних, передбачених Загальним регламентом про захист даних, варто звернути увагу, що повноваження потенційного регулятора мають враховувати обов'язки та вимоги, що містяться в низці актів, що регулюють дотичні сфери. Наприклад, механізм обробки персональних даних в цілях запобігання, виявлення та розслідування правопорушень, що регулюється Директивою ЄС 2016/680, повноваження, пов'язані із впровадженням Акту ЄС про дані, Акту про управління даними, Регламент про обіг неперсональних даних, Директиву ЄС про відкриті дані та ін.

Європейський досвід свідчить, що поєднання регулювання персональних даних, цифрових послуг, ШІ та управління даними в межах одного органу не є поширеною практикою та супроводжується значними інституційними ризиками. Відмінність у характері повноважень, рівні чутливості сфер та обсязі регуляторних завдань зумовлює необхідність їх функціонального розмежування або застосування гібридних моделей. Створення єдиного регулятора без чіткої спеціалізації, внутрішніх запобіжників і достатніх ресурсів може призвести до перевантаження інституції, ускладнення правозастосування та зниження ефективності нагляду та регулювання.

Відповідність вимогам незалежності

Будь-які компетентні органи, які номінуються для регулювання цифрової сфери та сфери захисту персональних даних, повинні бути незалежними від зовнішнього впливу.[14] Водночас гарантії інституційної незалежності включають, зокрема, прозору процедуру призначення членів, визначений строк повноважень, завчасно визначені вимоги до членів органу та їх компетенції, а також правила щодо конфлікту інтересів.[15]

Форма діяльності та процедура призначення

Особливості реалізації гарантій незалежності значною мірою залежатимуть від обраної форми діяльності Єдиного регулятора — як колегіального чи одноосібного органу.

Колегіальний підхід інституційної організації органу є типовим для держав-членів ЄС, особливо у країнах, які одночасно поєднують сфери медіа та цифрових послуг під єдиною парасолькою регулювання. Крім того, колегіальність сприяє залученню різноманітної експертизи та підвищенню відповідальності кожного члена за окремі напрями діяльності відповідно до їхньої спеціалізації, що, своєю чергою, забезпечує ефективний розподіл функцій.

Колегіальність краще сприяє прозорості та збалансованості у процесі ухвалення рішень, яке здійснюється шляхом голосування. Зрештою, практика національного рівня у впровадженні колегіальності органів відкриває можливості для аналізу та запозичення досвіду, напрацьованого в національному контексті, зокрема на прикладі діяльності НКЕК, Національної ради та Центральної виборчої комісії.

Втім, у випадку такого різноманітного поєднання сфер в одному органі, ключовою проблемою щодо реалізації колегіальності буде питання забезпечення критично

[12] Artificial Intelligence Act, Articles 70(1), 78.
[13] Artificial Intelligence Act, Articles 28(1), 70(1)
[14] Digital Services Act, Articles 49-50; Audiovisual Media Service Directive, Article 30.
[15] General Data Protection Regulation, Articles 51-54.

важливої експертизи під час ухвалення рішень. Наявність у складі лише одного представника, що володіє експертизою у відповідній сфері, віднесеній до відома органу, буде недостатньо для ухвалення справді незалежних та ефективних рішень.

З іншого боку, практика ЄС демонструє, що **одноосібна структура** органу, як правило, характерна для регулювання однієї окремої сфери — вона переважає здебільшого у випадку регуляторних органів, які здійснюють нагляд у сфері захисту персональних даних. З огляду на це, запровадження одноосібної моделі для органу, що поєднує кілька сфер регулювання, супроводжуватиметься радше недоліками, ніж перевагами. Одними з ключових проблем у цьому випадку є кадрова складність на рівні керівника — призначена особа фактично повинна мати експертизу у всіх питаннях, що розглядатимуться регуляторним органом (персональні дані, цифрові послуги, ШІ тощо), а також загроза інституційної прогалини у випадку припинення його повноважень або звільнення, що супроводжуватиметься пошуком нової людини знову ж таки з глибокою експертизою та аналогічними знаннями.

У випадку перебування всіх сфер регулювання в рамках юрисдикції одного органу з'являється також підвищений ризик зовнішнього тиску та лобіювання для прийняття найбільш сприятливого рішення, що становитиме серйозну загрозу незалежності регулятора. Потенційні шляхи вирішення такої проблеми можуть бути запозичені із практики окремих держав-членів ЄС, які встановили внутрішні законодавчі механізми для збереження неупередженості регуляторів. Наприклад, у Німеччині, де одноособовий орган одночасно регулює сфери електронних комунікацій та цифрових послуг, передбачено окрему законодавчу процедуру щодо призначення голови Відділу координації цифрових послуг для забезпечення незалежності. Крім того, в країнах, які поєднують декілька сфер регулювання, передбачено призначення інституційно відокремлених суб'єктів, які моніторитимуть роботу регулятора та матимуть можливість оскаржити його рішення у судовому порядку. Так, в Австрії таким суб'єктом є окремий виконавчий департамент RTR-GmbH при австрійському медіарегуляторі (уповноважений на оскарження рішень регулятора), у Португалії — інспектор (відповідальний за контроль законності, правильності та належного фінансового та майнового управління медіарегулятора), а у Норвегії, що входить до ЄЕЗ, — Рада з питань приватних апеляцій (розглядає апеляції на рішення, прийняті регулятором у сфері захисту персональних даних).

Незалежно від обраної форми діяльності, процедура призначення членів колегіального органу чи одноосібного уповноваженого, чи комісара, стандарти ЄС вимагають прозорої процедури. Серед іншого, це стосується збалансованості представників Конкурсної комісії для гарантування її незалежності та інклюзивності. Наприклад, Служба державних призначень в Ірландії, яка призначає Комісарів, що відповідають за окрему сферу регулювання, складається з семи членів, чотири з яких становлять представники державного сектору, а три — приватного. Аналогічний досвід спостерігається і в Литві, де Регулятора, який загалом складається з одинадцяти членів, призначають окремі суб'єкти: п'ять членів призначаються представниками уряду, а шість членів — представниками журналістських та релігійних спільнот.

Для України розширення кола суб'єктів, які формуватимуть Конкурсну комісію, представниками академічної спільноти, громадськими або професійними об'єднаннями може посилити об'єктивність та фаховість у контексті вибору найкращого кандидата на посаду члена регулятора/одноосібного органу. Наприклад, механізм формування Конкурсної комісії може бути запозичений із досвіду роботи НКЕК, де окремі члени комісії пропонуються різними суб'єктами. Водночас залучення представників міжнародних

інституцій до Конкурсної комісії за прикладом того, як це відбувається у сфері правосуддя, потребує додаткового обговорення, адже належна оцінка досвіду та відповідності кандидатів посадовим вимогам може потребувати врахування національного контексту.

Операційна незалежність

У разі створення Єдиного регулятора, він буде наділений повноваженнями у сферах цифрових послуг, цифрових ринків, ШІ, персональних даних, доступу до публічної інформації та обігу даних, а також інформаційної безпеки в мережі щодо захисту дітей.

Очевидно, що визначення статусу цього органу потребуватиме розмежування компетенцій та функцій з іншими державними органами, які виконують завдання у суміжних сферах регулювання. Так, до прикладу НКЕК уже регулює діяльність суб'єктів, що надають посередницькі цифрові послуги з доступу до інтернету, які також підпадатимуть під нагляд Координатора цифрових послуг, повноваження якого виконуватиме Єдиний регулятор. Відсутність розмежування та чітких інструкцій для учасників ринку може створити додаткову невизначеність та тиск. Схожі питання можуть виникнути й щодо розмежування повноважень з медіа регулятором, до сфери якого належить нагляд за діяльністю провайдерів послуг спільного доступу до відео.

Аналогічно, у контексті захисту прав дітей у цифровому просторі, повноваження Єдиного регулятора щодо встановлення механізмів виявлення та блокування незаконних матеріалів, створюватимуть колізії із реалізацією функцій, якими вже наділені НКЕК (щодо блокування вебсайтів) та Національна рада (обмеження діяльності онлайн-медіа).

У сфері регулювання персональних даних необхідно встановити чіткий механізм взаємодії між Єдиним регулятором та Уповноваженим ВРУ з прав людини (далі — Омбудсмен) — наразі єдиним суб'єктом, наближеним до регулятора у сфері захисту даних.

Фінансова незалежність

Регуляторний орган повинен бути наділений достатніми фінансовими ресурсами для належного та ефективного виконання своїх завдань.[16] Управління власними фінансами становить одну із вимог незалежності регулятора. У такому випадку, орган має суттєву автономію у прийнятті рішень щодо власного бюджету та його обсягів.[17] Хоча кожен наглядовий орган підлягає фінансовому контролю, це не впливає на його фінансову незалежність щодо управління своїм публічним бюджетом, який є складовою загального державного бюджету.[18]

Практика держав-членів ЄС демонструє, що регулятори фінансуються трьома методами: коштами державного бюджету, власними «доходами» органу-регулятора та змішаним форматом, який поєднує перші два способи. Державний бюджет є найбільш поширеним джерелом фінансування у ЄС (всі регулятори у сфері персональних даних, а також деякі регулятори у сфері медіа та цифрових послуг).

В Україні повна залежність від бюджетного фінансування підіймає очевидні питання щодо потенційної загрози об'єктивності та незалежності регулятора, особливо якщо під його парасолькою концентруватиметься декілька чутливих сфер (як-от, персональні дані та онлайн-безпека). Крім того, з'являється загроза урізання державного бюджету з огляду на економічні складнощі. Така проблема вже мала місце при фінансуванні

[16] Digital Services Act, Article 50(1), Artificial Intelligence Act, Article 70(3), General Data Protection Regulation, Article 52(4)
[17] Digital Services Act, Article 50(1)
[18] General Data Protection Regulation, Article 52(6)

українського медіарегулятора та регулятора у сфері електронних комунікацій. Так, бюджет, виділений Національній раді на 2025 рік, становив приблизно на 40% менше необхідного фінансування, передбаченого у Законі «Про медіа».

У разі ж створення нового єдиного регуляторного органу, з огляду на обсяг сфер, що пропонується віднести до його відання, питання фінансування буде одним із ключових, як для забезпечення його незалежності, так і гарантування ефективності. При цьому, щонайменше на початку запуску діяльності такого органу, державний бюджет може буде основним, чи навіть, єдиним способом фінансування.

Фінансування регуляторів коштом внесків учасників ринку або ліцензійних та інших зборів характерне переважно для економічно розвинених країн зі стабільною фінансовою системою. Такий підхід можливий завдяки достатньому обсягу ринку, високому рівню довіри до інституцій та спроможності забезпечувати сталі джерела фінансування.

Водночас, доцільно також розглянути можливості внесення змін до бюджетного законодавства та запровадження поширеної для ЄС «змішаної» моделі, яка поєднуватиме фінансування з державного бюджету та безпосередні збори та внески. Такий підхід, поширений, зокрема, у Швеції, Хорватії та Австрії, дозволить забезпечити незалежність та автономію регулятора з одночасною фінансовою стабільністю.

РОЗДІЛ 3. АЛЬТЕРНАТИВНІ ПІДХОДИ

Оскільки підхід щодо створення Єдиного регулятора має чимало проблемних у реалізації аспектів, слід розглянути альтернативні моделі розподілу повноважень у цифровій сфері. З огляду на обмежені фінансові ресурси, а також потенційні конфлікти та накладення повноважень, варто обережно підходити до питання створення нових органів і, де можливо, використовувати наявні інституції, розширюючи й адаптуючи їхні повноваження до європейських стандартів. Пропонуємо розглянути, яким чином можна організувати регуляторні, наглядові та контрольні функції у п'ятьох ключових сферах, які планувалося віднести до компетенції Єдиного регулятора.

Сфера персональних даних та доступу до публічної інформації

Однією з ключових проблем включення цих двох сфер до компетенцій Єдиного регулятора було те, що вони мають великий нецифровий сегмент. Як наслідок, це потребує компетенцій щодо ряду важливих європейських стандартів.

У сфері захисту даних це включає вже згадані Загальний регламент про захист даних (GDPR) і Директиву 2016/680 (Law Enforcement Directive), що містить правила обробки персональних даних в правоохоронних цілях, а також Конвенцію 108+. У сфері доступу до публічної інформації важливо імплементувати не лише Конвенцію Тромсо (про доступ до публічної інформації) і Директиву щодо відкритих даних, а й Акт про дані, Акт про управління даними, Регламент про обіг неперсональних даних, Директиву 2019/790 (щодо доступу до даних, захищених авторським правом), Регламент P2B та деякі положення Акту про штучний інтелект, які напряму стосуються обігу та обробки різних категорій даних.

Цей перелік актів передбачає створення цілої інфраструктури, що забезпечуватиме належний обіг даних як на рівні державних органів, так і на рівні нагляду за дотриманням положень законодавства приватними суб'єктами. При цьому, більшість актів передбачають, що державний нагляд і контроль мають здійснюватися органом, що відповідає критеріям ефективності та незалежності.

Варіантом реалізації таких критеріїв на практиці стала ідея створення окремого органу, що у сфері своїх компетенцій охоплюватиме питання захисту персональних даних та доступу до публічної інформації (а з огляду на чисельність актів у цій сфері — не лише публічної інформації, а управління даними в цілому). Така концепція свого часу була втілена у Законопроєкті 6177, зареєстрованому у парламенті у 2021 році. Чи містить цей документ усі необхідні гарантії відповідно до GDPR (який висуває вимоги до наглядового органу у сфері захисту даних)?

- **Незалежність**. Перш за все, Законопроєкт 6177 встановлює низку заборон щодо сумісності посад, а також вимог до компетенцій та етичної поведінки кандидатів у члени Національної комісії з питань захисту персональних даних та доступу до публічної інформації (далі — Національна комісія). Крім того, склад цього органу планується призначати незалежною комісією, яка затверджується урядом. Іншою гарантією незалежності є порядок формування самої Конкурсної комісії: дві особи призначає парламент, одну — Уповноважений ВРУ з прав людини, ще двох — КМУ та чотирьох — громадські об'єднання, які працюють у сфері компетенцій Національної комісії. Загалом такий орган складається з дев'яти членів. В цілому, такий порядок формування відповідає вимогам GDPR в контексті наявності незалежної процедури призначення та припинення повноважень членів державного органу;

- **Ефективність**. Хоча Законопроєкт містить деякі технічні проблемні аспекти (наприклад, Національна комісія стає повноважною з моменту призначення 4 членів, а для прийняття рішення потрібно щонайменше 5 голосів), такі недоліки можна усунути при підготовці документа до другого читання. Водночас ключовим питанням щодо ефективності роботи органу стане фінансування. Так, Законопроєкт не пропонує запобіжників від ситуацій призупинення фінансування регуляторів в рамках затвердження Закону про бюджет, що стало досить типовою практикою в Україні останніми роками. За відсутності запобіжників у самому законі, ризики недофінансування залишаються актуальними й для цього органу.

Водночас при створенні нового державного органу важливо виключити потенційний конфлікт повноважень з іншими державними інституціями, включно з Омбудсменом, який наразі є ключовим органом у сфері захисту персональних даних. Так, Омбудсмену можна залишити просвітницькі функції, включно з питаннями підготовки осіб, відповідальних за захист даних, в той час як регуляторні і наглядово-контрольні функції можуть перейти до новоствореної Національної комісії.

Права дітей в Інтернеті

На європейському рівні ця сфера охоплює велике розмаїття ініціатив (включно з численними проєктами актів), частина з яких стосується регулювання контенту та поведінки в мережі, а інша частина — порядку авторизації на різних ресурсах. Зокрема, це охоплює проєкт Регламенту проти сексуальних домагань проти дітей (CSAM) та майбутні ініціативи, що будуть впроваджені державами в рамках стратегії Better Internet for Kids (BIK+). Остання включає ряд заходів, щодо реалізації яких першість на себе мали б взяти саме національні регулятори (як-от впровадження цифрових ID, забезпечення уніфікованих механізмів верифікації віку, створення надійних ресурсів для підвищення цифрової грамотності, підвищення кваліфікації державних службовців тощо), зокрема в рамках впровадження Акту про цифрові послуги та GDPR.

В рамках імплементації цих актів (навіть за умови незначних змін у текстах проєктів), повноваження щодо захисту прав дітей в Інтернеті можна розподілити між такими регуляторами:

- **Національна рада**. Цей орган вже має повноваження в контексті забезпечення прав дітей в медійній роботі та матеріалах медіа (відповідно до статті 42 Закону України «Про медіа»), а також щодо реклами, яка поширюється в медіа та може впливати на права дітей (згідно зі статтею 20 Закону України «Про рекламу»). Крім того, питання захисту дітей в цифровому просторі можуть вирішуватися в межах механізмів спільного регулювання, до яких долучена Національна рада (зокрема, вже розробляється Кодекс щодо захисту дітей в медіа в аудіовізуальній сфері, але аналогічні положення можуть мігрувати й в сферу онлайн-медіа);

- **НКЕК**. Серед його повноважень присутні процедури блокування ресурсів, що здійснюють неправомірну діяльність, зокрема поширення дитячої порнографії. Підстави блокувань також можуть бути розширені, щоб охоплювати типи контенту, передбачені вищезгаданими актами ЄС. Сама ж процедура і порядок блокувань потребують доопрацювання та чіткого законодавчого визначення, зокрема в контексті діяльності платформ спільного доступу до інформації;

- **Омбудсмен**. В рамках діяльності цього органу існує посада Уповноваженого з прав дитини, який, зокрема, має повноваження у наглядовій сфері, а також активно займається просвітницькою діяльністю. Такі функції можна було б розширити повноваженнями комунікувати з платформами та іншими онлайн-ресурсами в контексті захисту прав дітей, а у разі виявлення порушень, на які платформи не реагують — звертатися до інших державних органів (як-от НКЕК) для ініціювання процедури блокування ресурсів чи вжиття інших заходів для усунення порушень.

Крім того, окремими аспектами питань щодо забезпечення цифрової грамотності можуть опікуватися профільні міністерства: Мінцифри (в рамках проєктів Дія.Освіта) та міністерство, чия діяльність охоплюватиме сферу інформаційної політики (включно з проєктом «Фільтр»). Мінцифри також може стати лідером в розробці і впровадженні концепції цифрових ID, враховуючи аспект забезпечення прав дітей (оскільки така діяльність стосується більше виконавчих, ніж наглядових функцій, і не потребує залучення незалежного регуляторного органу).

Зрештою, питання протидії контенту, створення і поширення якого є криміналізованим, також вимагатиме залучення органів правопорядку, включно з Національною поліцією, прокуратурою, тощо.

Штучний інтелект

Акт ЄС про штучний інтелект, який Україні належить імплементувати в рамках євроінтеграції, встановлює обов'язок призначити щонайменше два органи у сфері ШІ: нотифікуючий орган та орган з нагляду за діяльністю ринку. Ймовірніше за все, ці повноваження покладатимуть на вже існуючих, а не новостворених регуляторів.

Хто може опікуватися такими питаннями?

Нотифікуючий орган, відповідно до статті 28 Акту про штучний інтелект, має здійснювати процедуру оцінювання, призначення та повідомлення інституцій з оцінки відповідності та моніторингу їх діяльності. За своєю суттю діяльність нотифікуючого органу передбачає сертифікацію таких інституцій. Як наслідок, найлогічніше покласти такі повноваження на Національне агентство з акредитації України, ключовим завданням якого і є посвідчення спроможності організацій та установ діяти відповідно до законодавства та здійснювати перевірки.

Втім, важливо забезпечити інституційну незалежність і ефективність Національного агентства. Наразі його діяльність регулюється Положенням Міністерства економіки України, що передбачає прямий вплив уряду на обсяг і порядок реалізації повноважень такого органу. Тож потенційні зміни мають стосуватися не лише розширення обсягу повноважень і охоплення сфери ШІ, а і порядку формування Національного агентства. Важливо, що такі повноваження не можуть покладатися на орган, що займатиметься ринковим наглядом.

Орган ринкового нагляду. Як вже згадувалося, поміж іншого, такий регулятор буде уповноважений на оцінку високоризикових систем, розробку методологій для оцінки впливу ШІ на права людини, а також розгляд скарг від осіб, які зазнали впливу через рішення розробників чи впроваджувачів систем ШІ. В цілому, перелік компетенцій є досить широким, але водночас охоплює значну кількість суміжних сфер, які вже мають потужну регуляторну базу (захист даних, протидія дискримінації, прозорість і публічні закупівлі тощо). Відповідно, раціональніше покладати компетенції органу ринкового нагляду на вже існуючі (заплановані до створення) органи. Серед них дотичними до сфери ШІ можна вважати:

- **Координатора цифрових послуг.** Орган, що відповідатиме за цю сферу (моделі дизайну органу наведені нижче), муситиме відповідати критеріям незалежності та ефективності, а також вже матиме компетенції в цифровій сфері та достатні інституційні правозастосовчі механізми для впровадження норм Акту про ШІ. Крім того, це дозволить уникнути внутрішній конфлікт повноважень у ситуації, коли орган поєднує і регуляторні, і контрольні функції, на додачу до функцій роботи з представниками індустрії та створення сприятливого середовища для розвитку бізнесу. Схожої логіки при призначенні органу ринкового нагляду дотримувалися у Мальті, Данії та Італії;

- **Національну комісію із захисту персональних даних та доступу до публічної інформації.** Оскільки орган вже займатиметься більшістю питань, пов'язаних з управлінням даними, а також відповідатиме конкретним вимогами щодо незалежної та ефективної діяльності, він є одним з найкращих варіантів для призначення регулятором у сфері ШІ. Водночас постає питання спроможностей органу охоплювати таку велику кількість питань, на додачу до управління даними. Ефективність цієї моделі значною мірою залежатиме від здатності забезпечити регулятора фінансовими, експертними та адміністративними ресурсами. Втім, успішність такої моделі вже продемонстрував досвід Люксембургу, який вирішив делегувати сферу ШІ саме органу у сфері захисту персональних даних.

Зрештою, частина повноважень може бути покладена на спеціалізовані органи: наприклад, Антимонопольний комітет України (АМКУ) може здійснювати нагляд за ринковою конкуренцією у сфері ШІ. Це допоможе уникнути створення численних нових органів і, водночас не покладатиме на орган ринкового нагляду нетипові для нього компетенції в антимонопольній сфері.

Регулювання онлайн-платформ

У цій сфері законодавець ЄС одразу передбачив можливість спільного нагляду та контролю за суб'єктами — Інтернет-посередниками — на національному рівні. Відповідно до статті 49 Акту про цифрові послуги, Координатор цифрових послуг має відповідати за впровадження усіх вимог Акту, окрім випадків, коли специфічні завдання або сектори передані до відання інших компетентних органів. При цьому, на всі такі органи мають поширюватися вимоги до незалежності, а саме:

- безсторонність, прозорість та вчасність реалізації повноважень (стаття 50 (1) Акту);
- наявність належних технічних, фінансових та людських ресурсів для реалізації таких повноважень (стаття 50 (1) Акту);
- належна автономія в управлінні власним бюджетом (стаття 50 (1) Акту);
- свобода від зовнішніх впливів та заборона отримувати інструкції від публічних органів та приватних осіб ззовні (стаття 50 (2) Акту).

Концептуально, об'єднання всіх повноважень під одним дахом в рамках компетенцій Координатора цифрових послуг є рідкісним у законодавчій практиці держав-членів Європейського Союзу. З-поміж них, лише Австрія, Латвія, Люксембург, Румунія та Словаччина пішли таким шляхом.

Превалює підхід передачі частини функцій з нагляду за впровадженням окремих положень статей 26 (щодо реклами на онлайн-платформах) та 28 (захисту неповнолітніх в онлайні) на інші органи, переважно у сфері захисту прав споживачів (якщо такий орган не номінований Координатором цифрових послуг) та захисту персональних даних відповідно. У окремих країнах — таких як Фінляндія та Ірландія — окремо виділяються і повноваження щодо онлайн-платформ, за допомогою яких укладаються дистанційні контракти.

При цьому, конкретні положення законодавства, передані під компетенцію інших компетентних органів, зазвичай чітко визначаються в національному законодавстві, що покликане імплементувати Акт про цифрові послуги, хоча в деяких країнах співпраця Координатора з іншими органами визначена нечітко — через передбачення загального обов'язку такої співпраці (наприклад, в Італії та Португалії). Лише одна з країн, яка не має конвергентного регулятора у сферах електронних комунікацій та медіа або не поклала виконання функцій Координатора цифрових послуг на медійного регулятора, — Болгарія — розмежувала потенційні конфлікти повноважень за Актом про цифрові послуги та Директивою про аудіовізуальні послуги щодо платформ спільного доступу до відео.

З дослідження, проведеного у першому кварталі 2025 року, зрозумілими стають і потреби Координаторів цифрових послуг та інших компетентних органів у нових людських та фінансових ресурсах. У країнах, що є значно меншими за розмірами — а тому і за потенційною кількістю суб'єктів, що підпадатимуть під юрисдикцію, на впровадження Акту про цифрові послуги планується винайняти 22 (Бельгія), 49 (Словаччина) або ж до 70 (Нідерланди) нових працівників. При цьому, слід пам'ятати, що в ЄС найбільші онлайн-платформи регулюватимуться винятково на рівні Європейської комісії, що має власний бюджет та кадрову структуру.

В Україні існує декілька органів, які можуть бути визначені як компетентні органи влади в контексті Акту про цифрові послуги. Найімовірнішими кандидатами на визначення Координатором цифрових послуг є Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку та Національна рада.

Обидва з них є колегіальними органами з визначеними у профільних законах гарантіями операційної незалежності та невтручання зі сторони інших органів влади. Членів обох органів обирають за конкурсними процедурами, з урахуванням специфіки закріплення статусу Національної ради в Конституції України та участі в обранні її членів Президента та Верховної Ради України. Законодавство, що регулює діяльність регуляторів у сфері електронних комунікацій та медіа, також фіксує розміри матеріального забезпечення членів органів та працівників апарату. Крім того, Національна рада має законодавчо закріплені гарантії щодо виділення певної суми з Державного бюджету.

Втім, дія фінансових положень як Закону України «Про Національну комісію, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку», так і Закону України «Про медіа», послідовно припиняється Законами України про державний бюджет на кожен наступний рік у період 2023-2025 років. На це послідовно звертає увагу Європейська комісія у щорічному звіті про розширення, зазначаючи, що Україна має «*забезпечити аби незалежні регулятори у сферах медіа та електронних комунікацій ... мали достатнє фінансування та людські ресурси для виконання своїх функцій*».

Як і Національна рада, так і НКЕК не мають у своєму нинішньому арсеналі належних людських та технічних ресурсів для регулювання онлайн-платформ. Також в обох органів відсутній досвід регулювання онлайн-платформ. Діяльність НКЕК концентрується переважно на врегулюванні діяльності лише однієї категорії таких посередників — постачальників електронних комунікаційних послуг (де-факто — Інтернет-провайдерів). Що ж до медійного регулятора, то попри появу внаслідок запровадження Директиви про аудіовізуальні медіапослуги у нього повноважень щодо контролю за дотриманням статті 28 Закону України «Про медіа», що містить обов'язки у сфері належної обачності (due diligence) щодо такої категорії онлайн-платформ як платформи спільного доступу до відео, на практиці Національна рада не втілювала їх у життя щодо двох платформ, які зареєструвалися та підпадають під юрисдикцію України.

Водночас, з публічної інформації, яку ці регулятори надають на своїх сайтах, можна ознайомитися з напрямками, в яких вони нарощують спроможності власного персоналу. Саме представники Національної ради концентруються на Акті про цифрові послуги в рамках програми Twinning, в той час, як пріоритетом для НКЕК в рамках механізму TAIEX є питання роумінгу та загальної авторизації, а також позасудового вирішення спорів.

З огляду на це, в рамках нинішньої конфігурації, доцільнішим виглядатиме надання статусу Координатора цифрових послуг саме Національній раді, яка є більш компетентною в питаннях протидії шкідливому контенту в Інтернеті. Оскільки повноваження щодо регулювання найбільших онлайн-платформ та пошукових онлайн-систем теж пропонується покласти на Координатора цифрових послуг, саме медійний регулятор буде здатен якісніше усвідомити системні ризики, яким мають протидіяти такі платформи, та надбудовувати власні здатності на базі понад декади досвіду у сфері захисту інформаційного простору та його прозорості. При цьому, критичним питанням буде забезпечення стабільного фінансування для Національної ради, від якого прямо залежатиме і якість людських ресурсів, що їх буде здатен найняти регулятор. В інших аспектах він відповідатиме критеріям незалежності, що їх висуває Акт про цифрові послуги до органів, які отримують статус Координатора цифрових послуг.

Водночас, через комплексність питань, що врегульовуються Актом про цифрові послуги, доцільним буде долучення інших компетентних органів. З конфігурації, яка переважно застосовується на рівні держав-членів ЄС, оптимальним буде залучення регулятора у сфері захисту персональних даних (на сьогодні — Омбудсмен) до нагляду за дотриманням вимог щонайменше статей 26 (3) та 28 (2) Акту, в яких йдеться про обмеження показу реклами, що спирається на профілювання, користувачам, з можливим розширенням компетенцій на всі положення, що стосуються захисту дітей. Іншим таким органом може бути Державна служба України з питань безпечності харчових продуктів та захисту споживачів (Держпродспоживслужба), що відповідала б за взаємодію з онлайн-платформами, які дозволяють укладати дистанційні контракти. Положення Акту про цифрові послуги щодо відстежуваності продавців (traceability of traders) та комплаєнсу-за-дизайном у статтях 30-32 перегукуються з вимогами до маркетплейсів

щодо розміщення інформації про суб'єктів електронної комерції у новій редакції Закону України «Про захист прав споживачів», що має набути чинності з моменту скасування в Україні правового режиму воєнного стану.

Такий підхід дозволив би краще спрямувати наявні ресурси цих органів та надати кожному з них повноважень у суміжних до вже покладених на них сфер діяльності. Це, своєю чергою, може сприяти оптимізації бюджетних витрат на діяльність компетентних органів в умовах обмежених спроможностей Державного бюджету України. Координація таких органів могла б відбуватися або шляхом укладання відповідних протоколів між Координатором цифрових послуг та Омбудсменом і Держпродспоживслужбою, за прикладом Нідерландів або ж адміністративних договорів, як у Німеччині.

В такій моделі спільного регулювання нагальним питанням буде забезпечення незалежності інших компетентних органів. Омбудсменові бракує ефективних повноважень щодо притягнення до відповідальності за порушення вимог законодавства про захист персональних даних, а також кадрового ресурсу для нагляду над усіма суб'єктами, що перебувають в юрисдикції України. Хоча ситуація може змінитися зі створенням Національної комісії із захисту персональних даних та доступу до публічної інформації, наразі регулятора не можна вважати таким, що відповідає вимогам статті 50 Акту про цифрові послуги. Держпродспоживслужба є центральним органом виконавчої влади в системі Кабінету Міністрів України, голова якої призначається та звільняється урядом, а структура і фінансування якої погоджується з іншими міністерствами. Її інституційна незалежність є обмеженою, а тому може потребувати законодавчих змін задля відповідності вимогам Акту про цифрові послуги.

ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

Держави-члени ЄС не мають уніфікованого підходу щодо створення чи призначення регуляторних та наглядових органів, тож вивчення їх досвіду може бути важливим для розуміння переваг та недоліків різних варіантів, але не може відтворюватись без врахування національного контексту. Для України наразі важливо обрати збалансовану модель інституційної структури, що забезпечить ефективність та незалежність регулювання та нагляду без надмірної фрагментації повноважень між багатьма інституціями чи перевантаження одного органу функціями у кількох масштабних сферах.

Запропоновані нижче рекомендації спрямовані на формування в Україні сучасної, прозорої та стабільної системи цифрового врядування, здатної забезпечити належний рівень захисту прав людини, ефективний нагляд за ринками та відповідність європейським стандартам:

1. **Забезпечити повну відповідність регуляторної моделі вимогам права ЄС.** Це стосується, зокрема, повного узгодження статусу, переліку функцій та повноважень, які мають виконувати інституції, відповідальні за впровадження відповідного регулювання, а також визначених вимог та гарантій щодо ефективності та незалежності таких інституцій.

2. **Відмовитися від надмірної концентрації повноважень у межах одного органу**, а також мінімізувати ризики конфлікту інтересів між регуляторними, наглядовими та контрольними функціями у сферах цифрового регулювання.

3. **Провести комплексну інституційну оцінку існуючих органів регулювання та нагляду**, які реалізують окремі повноваження у сферах медіа, регулювання платформ спільного

доступу до інформації, електронних комунікацій, захисту персональних даних, штучного інтелекту. Зокрема, варто здійснити системний аудит спроможностей Національної ради, Національної комісії з електронних комунікацій та інших державних органів, оцінити їх кадровий потенціал, технічну інфраструктуру, досвід правозастосування, фінансові та організаційні потреби. Такий аналіз є необхідним для обґрунтованого прийняття рішень щодо розширення або перерозподілу повноважень.

4. **Забезпечити повноцінну незалежність регуляторних та наглядових органів.** Законодавство, що регулюватиме створення або призначення відповідних органів має встановлювати прозорі конкурсні процедури, чіткі критерії відбору, фіксовані строки повноважень, правила запобігання конфлікту інтересів. Необхідно також розширити участь у конкурсних комісіях представників академічної спільноти, громадських організацій, професійних асоціацій, та обмежити можливості політичного впливу на призначення та звільнення членів регуляторів, зокрема через встановлення чітких та вичерпних вимог та підстав.

5. **Запровадити стійку та передбачувану модель фінансування.** Відмовитися від повної залежності регуляторів від щорічних бюджетних рішень та передбачити інші джерела фінансування. Закріпити в законодавстві мінімальні фінансові гарантії для регуляторів та забезпечувати їх виконання на практиці. Забезпечити автономію регуляторних та наглядових органів в управлінні власними бюджетами. Фінансова автономія є ключовою умовою інституційної стійкості та здатності інституцій ефективно виконувати свої повноваження.

6. **Розвивати механізми міжвідомчої координації.** Ефективність впровадження нового регулювання у цифровій сфері залежатиме від належної взаємодії між компетентними органами. З огляду на це, щонайменше потрібно визначити чіткі механізми обміну інформацією та розглянути можливість впровадження спільних процедур для реагування на порушення, які зачіпають одночасно декілька сфер.

7. **Інвестувати у розвиток кадрового та експертного потенціалу для регуляторних та наглядових органів.** Це може включати інвестиції в їх підготовку, постійне спеціалізоване навчання, перекваліфікацію, стажування в інституціях ЄС тощо. Регуляторні інституції мають також бути відкритими до залучення зовнішніх експертів з академічної сфери, громадянського суспільства чи представників суб'єктів регулювання, зокрема в рамках ініціатив спільного регулювання.

8. **Підтримувати міжнародну співпрацю та європейську інтеграцію регуляторів.** Важливо продовжувати налагоджувати канали для обміну інформацією та комунікації з європейськими наглядовими та регуляторними органами, активно долучатися до мереж європейських регуляторів, спільних навчальних програм, використовувати інструменти Twinning, TAIEX та інші формати співпраці, особливо для новостворених чи призначених регуляторів.

Лабораторія цифрової безпеки

МІЖНАРОДНИЙ ФОНД ВІДРОДЖЕННЯ

Співфінансується Європейським Союзом

2026