International IDEA

STIFTUNG MERCATOR

НАВІГАТОР ПО ПРАВОВІЙ СИСТЕМІ ЄВРОПЕЙСЬКОГО СОЮЗУ У СФЕРІ ЦИФРОВІЗАЦІЇ: ЧАСТИНА 1

Короткий огляд регуляторного впливу на виборчі процеси

НАВІГАТОР ПО ПРАВОВІЙ СИСТЕМІ ЄВРОПЕЙСЬКОГО СОЮЗУ У СФЕРІ ЦИФРОВІЗАЦІЇ: ЧАСТИНА 1

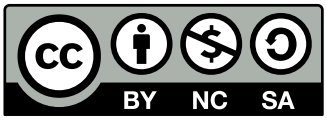
Короткий огляд регуляторного впливу на виборчі процеси

Себастіан Бекер Кастелларо, Гладіола Ллеші та Юліане Мюллер

International IDEA
INTERNATIONAL INSTITUTE FOR DEMOCRACY AND ELECTORAL ASSISTANCE

International IDEA
Strömsborg
SE–103 34 Stockholm
SWEDEN
+46 8 698 37 00
info@idea.int
www.idea.int

Проєкт «Подолання цифрового розриву на виборах у рамках вступу до ЄС» фінансується Stiftung Mercator.



International IDEA
Strömsborg
SE–103 34 Stockholm
SWEDEN
Tel: +46 8 698 37 00
Email: info@idea.int
Website: <https://www.idea.int>

Design and layout: International IDEA
DOI: <https://doi.org/10.31752/64709>
ISBN: 978-91-8137-130-7 (PDF - файл)

Сучасний контекст

Цифровізація змінює виборчі процеси у країнах-членах Європейського Союзу та сусідніх державах-кандидатах. Разом з потужними інструментами для посилення демократичної участі, вона також створює і нові уразливості — від непрозорого фінансування політичних кампаній в Інтернеті та дезінформаційних кампаній до ворожого іноземного втручання і додаткових загроз кібербезпеці. Такі виклики вимагають надійного управління та пильного нагляду за цифровою сферою, аби забезпечити проведення вільних, чесних та прозорих виборів як у самому ЄС, так і за його межами.

Відтак acquis ЄС у сфері цифровізації можна визнати наріжним каменем для забезпечення стійкості демократії. Європейська правова система має значний вплив на організацію та проведення виборів, зокрема у країнах-кандидатах. Часто синхронізація національних законодавств з acquis ЄС там відбувається обмеженим ресурсом і на фоні вирішення нагальних проблем, аж до військового іноземного втручання. Саме тому аналіз процесів та вивчення досвіду цих держав може надати цінні уроки для самого ЄС.

Пропоноване дослідження «Навігатор по правовій системі Європейського Союзу у сфері цифровізації» проводилося у рамках проєкту «Скорочення цифрового розриву в проведенні виборів у період підготовки до вступу до ЄС», за фінансової підтримки Stiftung Mercator. Воно складається з двох взаємодоповнюючих частин, які разом мають на меті усунути критичний розрив у взаємодії між ЄС та чинними і потенційними країнами-кандидатами у цій царині.

У частині 1 *«Короткий огляд регуляторного впливу на виборчі процеси»* досліджується так званий цифровий регламент ЄС, що включає низку знакових нормативних актів, зокрема Акт про штучний інтелект, Акт про цифрові послуги, Європейський закон про свободу ЗМІ, Загальний регламент про захист даних та Регламент про прозорість і тарґетування політичної реклами. Тут представлений стислий аналіз однієї з найбільш комплексних сучасних ініціатив, спрямованих на узгодження технологічних інновацій з демократичними цінностями. Наведені далі практичні приклади дозволяють пояснити, як зазначені нормативні акти допомагають захиститися від кіберзагроз, порушення конфіденційності даних та неетичного використання штучного інтелекту (ШІ) у виборчих процесах, а також упередити непрозору політичну рекламу.

У частині 2 *«Перспективи виборчих процесів у країнах-кандида тах* до ЄС» розглядається прогрес країн-кандидатів у гармонізації національного

законодавства з acquis ЄС. Там надана оцінка чинного національного законодавства, інституційних рамок та можливостей ефективного правозастосування, а також набутий досвід у боротьбі з цифровими загрозами для виборів. У своїй другій частині дослідження зосереджується на чотирьох країнах-кандидатах: Албанії, Молдові, Північній Македонії та Україні. Зроблені на основі аналітичних та польових досліджень висновки ми розглядаємо як корисний внесок у дискусії, що ведуться як всередині цих країн, так і на рівні ЄС.

Представлені у документі висновки та рекомендації містять стислі, але ґрунтовні поради для органів адміністрування виборів, політиків та організацій громадянського суспільства у країнах-кандидатах, а також для відповідних інституцій ЄС. Відтак вони створюють основу для наступного етапу проєкту, що має на меті сприяти зближенню та обміну знаннями між цими суб'єктами.

Ця робота є особливо актуальною саме тепер, коли чотири країни-кандидати поставили амбітні цілі щодо завершення реформ для набуття членства в ЄС до 2030 року, а ЄС посилює свої зусилля щодо впровадження всеохопної правової бази у сфері цифровізації для захисту демократичних інститутів та виборів, зокрема через європейську ініціативу «Щит демократії». Проведене дослідження підтримує такі зміни та сприяє зміцненню відносин між ЄС і країнами, які прагнуть до набуття членства.

Слова подяки

Цей звіт підготовлений Міжнародним інститутом демократії та сприяння виборам (International IDEA) у рамках проєкту «Скорочення цифрового розриву в проведенні виборів у період підготовки до вступу до ЄС», за фінансової підтримки Stiftung Mercator. Автори: Себастіан Бекер Кастелларо, Гладіола Ллеші та Джуліана Мюллер. Дослідження проводилося за участі та експертного внеску Альберто Фернандеса Гібаха, Тейса Хейнмаа, Блерти Хокси, Філіпа Роте, Софі Рау, Сема ван дер Стаака та Петера Вольфа.

Скорочення

ШІ	Штучний інтелект
CJEU	Суд Європейського Союзу
DSA	Акт про цифрові послуги
ЄКПЛ	Європейська конвенція з прав людини (Конвенція про захист прав людини і основоположних свобод)
ЄСПЛ	Європейський суд з прав людини
ЄРЗД	Європейська рада із захисту даних
ЄІЗД	Європейський інспектор із захисту даних
EDS	Європейський щит демократії
ОАВ	Орган адміністрування виборів
EMFA	Європейський закон про свободу медіа
ENISA	Агентство Європейського Союзу з кібербезпеки
FIMI	Зовнішнє маніпулювання інформацією та іноземне втручання
FRIA	Оцінка впливу на фундаментальні права
GDPR	Загальний регламент про захист даних
HRW	Міжнародна організація Human Rights Watch
ІКТ	Інформаційно-комунікаційні технології
ДЄС (TEU)	Договір про Європейський Союз
ДФЄС (TFEU)	Договір про функціонування Європейського Союзу
TTPA	Регламент про прозорість і тарґетування політичної реклами
VLOP	Дуже велика онлайн-платформа
VLOSE	Дуже велика пошукова онлайн-система

Contents

РЕЗЮМЕ ДОСЛІДЖЕННЯ

Представлене «навігаційне» дослідження пропонує вичерпний огляд нормативно-правової бази Європейського Союзу у сфері цифровізації та відзначає зростаючий регуляторний вплив на демократичні процеси і цілісність виборів. Дослідження аналізує принципи та підходи до вироблення ключових правових інструментів, які були б здатні відповідати на складні виклики, пов'язані з цифровими технологіями та їхніми впливами на виборчі процеси, і водночас захищати фундаментальні цінності ЄС — демократію, верховенство права та основоположні права людини. Ми намагалися пояснити, як відповідні нормативні акти — зокрема Акт про штучний інтелект (2024), Акт про цифрові послуги (2022), Європейський закон про свободу медіа (2024), Загальний регламент про захист даних (2016) та Регламент про прозорість і тарґетування політичної реклами (2024) — усі разом створюють правове середовище, що дозволяє забезпечувати прозорість, підзвітність та добросовісність у дедалі більш цифровізованому виборчому процесі.

Окремо дослідження підкреслює важливість захисту основоположних прав у контексті використання персональних даних, поширення онлайн-контенту та використання штучного інтелекту. Тут ви знайдете приклади того, як зловживання персональними та конфіденційними даними, непрозорі алгоритмічні системи та маніпулятивні онлайн-практики загрожують цілісності виборів. Спираючись на правовий аналіз та практику судів ЄС, дослідження підкреслює критичну вагу стандартів мінімізації обсягу, пропорційності, згоди та прозорості у використанні персональних даних для захищення демократичних принципів. Цей механізм має вирішальне значення для управління ризиками, пов'язаними з мікротарґетингом на основі штучного інтелекту для створення

і поширення політичної реклами та маніпулятивного контенту, особливо на дуже великих онлайн-платформах.

Приклади недобросовісних практик з угорських парламентських виборів 2022 року та румунської президентської кампанії 2024 року демонструють наслідки прогалин в унормуванні та правозастосуванні. Подібні реальні кейси наочно показали, як маніпуляції й дезінформація в мережі разом з нездатністю захистити конфіденційні дані можуть спотворити результати виборів та підірвати довіру громадськості. Дослідження звертає увагу на нагальну потребу в більш проактивній міжвідомчій взаємодії, чітко окреслених регуляторних повноваженнях та послідовному правозастосуванні — як на рівні ЄС, так і у кожній окремій європейській країні.

Щодо органів адміністрування виборів (ОАВ) у державах-членах ЄС, для них така швидко змінювана регуляторна ситуація, з одного боку, відкриває можливості, а з іншого — створює значні операційні виклики. ОАВ доводиться брати на себе дедалі більше додаткових обов'язків і відповідальності, попри суттєві розбіжності у їхніх правових мандатах та інституційних можливостях у кожній окремій країні. Варто зазначити, що інноваційність та неусталеність впроваджуваної регуляторної бази ЄС у сфері цифровізації є викликом навіть для найрозвинутіших держав-членів, яким доводиться швидко адаптувати свої складні юридичні, технічні та інституційні екосистеми у постійно змінюваному контексті розвитку ІКТ.

Та попри згадані складнощі, оновлену правову базу ЄС у сфері цифровізації варто вважати одним із найамбітніших зусиль світового рівня щодо узгодження практик управління новітніми технологіями з традиційними демократичними цінностями. Ефективність її подальшого впровадження залежатиме від здатності інституцій ЄС та органів влади держав-членів, включно з ОАВ, тісніше координувати свої дії, обмінюватися провідним досвідом та посилювати цифрову грамотність і стійкість до дезінформації та інших неправомірних впливів протягом усього виборчого циклу.

У висновках автори дослідження позиціонують acquis ЄС у сфері цифровізації не лише як основу для регулювання ринку, але і як важливий інструмент для забезпечення демократичної стійкості. Лише скоординоване управління та пильний нагляд можуть поставити технологічні інновації на службу цінностям відкритих, справедливих і прозорих демократичних систем,

а не підривати їх зсередини та ззовні. Ініціативи, подібні до Європейського щита демократії, варто вважати прикладом перспективного підходу, спрямованого на зміцнення суспільних та інституційних захисних механізмів від нових цифрових загроз для демократії.

Розділ 1

ОСНОВОПОЛОЖНІ ПРИНЦИПИ РЕГУЛЮВАННЯ СФЕРИ ЦИФРОВІЗАЦІЇ ЄС ТА ЇХНІЙ ВПЛИВ НА ВИБОРЧІ ПРОЦЕСИ

1.1. ДЕМОКРАТІЯ, ОСНОВОПОЛОЖНІ ПРАВА ЛЮДИНИ ТА ВЕРХОВЕНСТВО ПРАВА ЯК БАЗОВІ ЄВРОПЕЙСЬКІ ЦІННОСТІ, НА ЯКІ СПИРАЮТЬСЯ ACQUIS ЄС У СФЕРІ ЦИФРОВІЗАЦІЇ

Демократія, верховенство права та повага до основоположних прав людини визнаються основними принципами, закріпленими у засновницьких договорах Європейського Союзу. Це чітко викладено у Статті 2 Договору про Європейський Союз (ДЄС), що визначає підвалини політики та правової системи ЄС, включно із сферою цифровізації:

> «Союз засновано на цінностях поваги до людської гідності, свободи, демократії, рівності, верховенства права та дотримання прав людини, зокрема осіб, які належать до меншин. Ці цінності є спільними для усіх держав-членів у суспільствах, де панують плюралізм, недискримінація, толерантність, справедливість, солідарність та рівність жінок і чоловіків».

Водночас Стаття 6(1) Договору про ЄС містить пряме посилання на Хартію основоположних прав Європейського Союзу (Хартія) і визнає її однакову з Договорами юридичну силу. Суд Європейського Союзу підтвердив обов'язковий характер Хартії нарівні з реалізацією законодавства ЄС і відіграв вирішальну роль у тлумаченні її положень (СЄС 2021).

Крім положень Хартії, Стаття 6(3) Договору про ЄС навіть посилює захист основоположних прав, визнаючи права, що гарантуються Європейською конвенцією з прав людини (ЄКПЛ),

загальними принципами права Союзу. Європейський суд з прав людини (ЄСПЛ) відіграв значну роль у тлумаченні та роз'ясненні цих прав, впливаючи у такий спосіб на формування як окремих національних, так і загальних правових рамок ЄС.

Європейський суд також враховує і легітимізує судову практику ЄСПЛ при тлумаченні основних прав у загальній правовій системі ЄС і забезпечує узгодженість між правом ЄС та ширшою європейською екосистемою з дотримання прав людини (Tinière 2023: 328).

Прихильність ЄС до інклюзивної, справедливої, безпечної та стійкої цифрової трансформації закріплена у Європейській декларації цифрових прав та принципів. Ця перша у своєму роді декларація ґрунтується на положеннях Хартії й посилається на Статтю 2 Договору про ЄС, яка визначає, що цінності ЄС та закріплені у правовій базі Союзу права і свободи мають поважатися в Інтернет-середовищі тією ж мірою, що і у реальному світі.

Цінності ЄС, а також закріплені у правовій базі ЄС права і свободи мають поважатися в інтернет-середовищі тією ж мірою, що і у реальному світі.

Цей короткий огляд доводить, що фундаментальні права, демократія та верховенство права визнаються не лише основоположними принципами ЄС, але й створюють юридично обов'язкові зобов'язання як для інституцій ЄС, так і для держав-членів. Інтеграція цих принципів до правової бази Союзу, включно з цифровою сферою, забезпечує відповідність основним правилам будь-яких цифрових політик ЄС, зокрема окремих регуляторних вимог до захисту даних (Загальний регламент про захист даних, GDPR), функціонування платформ (Акт про цифрові послуги, DSA), управління штучним інтелектом (Акт про штучний інтелект), підтримки свободи ЗМІ (Європейський закон про свободу медіа, EMFA) та забезпечення прозорості політичної реклами (Регламент про прозорість і тарґетування політичної реклами, TTPA).

Крім того, Стаття 51(1) Хартії закріплює зобов'язання держав-членів поважати права в імплементації законодавства ЄС, забезпечуючи послідовність у дотриманні демократичних принципів, цінностей та верховенства права всередині Союзу.

Відтак чинна правова база створює підвалини і для забезпечення цілісності виборів, захисту приватного життя та дотримання прозорості у цифровому просторі.

1.2. **ЗАХИСТ ЦІЛІСНОСТІ ВИБОРІВ У ЄВРОПЕЙСЬКІЙ СУДОВІЙ ПРАКТИЦІ: РОЛЬ ЄСПЛ ТА СЄС У ЗАБЕЗПЕЧЕННІ НАЛЕЖНИХ ВИБОРЧИХ СТАНДАРТІВ**

Політика ЄС у сфері цифровізації первинно формується на основі фундаментальних принципів, викладених у Договорі про ЄС та більш широкій правовій базі Союзу, невід'ємною частиною якої є судова практика Європейського суду та ЄСПЛ. Закріплені принципи наголошують на прихильності ЄС до дотримання демократичних цінностей, включно з цілісністю виборів як базової підвалини будь-якої функціонуючої демократії.

Право на вільні вибори закріплено у Статті 3 Протоколу № 1 до ЄКПЛ. За тлумаченням ЄСПЛ, цей принцип вимагає прозорості, доступності та захисту прав виборців від неправомірних зовнішніх впливів.

ЄСПЛ послідовно повертається до тлумачення цієї статті для вирішення проблем, пов'язаних із сучасними технологічними інноваціями, зокрема у сфері функціонування цифрових платформ. Така еволюція судової практики підкреслює важливість прозорості, доступності та захисту прав виборців від неправомірних зовнішніх впливів у цифрову епоху.

У справі *«Давидов та інші проти* Росії»[1] ЄСПЛ підкреслив позитивне зобов'язання держави забезпечити цілісність виборів, включно з ретельним унормуванням процесу зарахування, верифікації та обробки голосів виборців.

ЄСПЛ пропонує ґрунтовні настанови, які підкреслюють еволюційний характер виборчих прав і наголошують на необхідності адаптації правових рамок держав-членів до нових викликів, зокрема тих, які виникають у зв'язку з розвитком цифрових технологій.

Крім того, ЄСПЛ пропонує ґрунтовні настанови, які підкреслюють еволюційний характер виборчих прав і наголошують на необхідності адаптації правових рамок держав-членів до нових викликів, зокрема тих, які виникають у зв'язку з розвитком цифрових технологій. У настановах підкреслюється, що право на вільні вибори охоплює не лише голосування як таке, але й ширший контекст, у якому відбуваються вибори, зокрема інформаційне середовище на цифрових платформах (Європейський суд з прав людини, 2024).

Європейський суд (CJEU) відіграв фундаментальну роль у формуванні політик ЄС щодо забезпечення цілісності виборів, особливо у питаннях захисту даних та конфіденційності. У

1 Справа № 75947/11 (ЄСПЛ, 30 травня 2017 р.).

справі Шварц проти міста Бохум[2], Суд наголосив на необхідності вжити суворих заходів для захисту даних у виборчому контексті та забезпечити відповідальне поводження з персональними даними виборців. У подальшій судовій практиці — наприклад, у справі *Digital Rights Ireland Ltd проти Ірландії*[3] — розглядалося делікатне питання балансу між питаннями безпеки (зберігання даних) та забезпеченням основоположних прав, що значною мірою вплинуло на вироблення відповідних політик, як от Загального регламенту про захист даних (GDPR).

Справи *Planet49 GmbH проти CNIL*[4] та *Google проти CNIL*[5] підкреслюють важливість явної згоди на обробку даних відповідно до GDPR. У справі Planet49 наголошується на необхідності активної, інформованої згоди користувачів (наприклад, необов'язковість заповнення попередньо відмічених полів реєстраційної форми), а у справі Google підкреслюється необхідність згоди користувача на трансфер даних між серверами Google та іншими сторонами і забезпечення права на видалення даних. Ці рішення, хоча вони і не пов'язані безпосередньо з політичним мікротарґетингом, доводять необхідність більшої прозорості у практиках збору даних та захисту приватності виборців у цифровому середовищі, що є надзвичайно важливим у контексті ведення політичних кампаній з використанням тактики мікротарґетингу.

Ці рішення доводять необхідність більшої прозорості у практиках збору даних та захисту приватності виборців у цифровому середовищі.

Нарешті, в acquis ЄС у сфері цифровізації міцно вкорінені основні цінності Союзу — демократія, верховенство права та фундаментальні права людини — аби гарантувати, що цифрова трансформація підтримує, а не підриває цілісність виборів. Нормативні документи ЄС у сфері цифровізації, як от Акт про штучний інтелект, Акт про цифрові послуги, Загальний регламент про захист даних, Акт про свободу медіа та комплекс регуляторних заходів щодо транснаціональної політичної діяльності — усі вони спираються на положення Договору про Європейський Союз (ДЄС), Договору про функціонування Європейського Союзу (ДФЄС) і Хартії, а також на судову практику Європейського суду та Європейського суду з прав людини і комплексно захищають прозорість, персональні дані, свободу ЗМІ та справедливу політичну участь. Така інтегрована

2 Справа C-291/12 (2013).
3 Справа C-293/12 (2014).
4 *Федеральна асоціація центрів споживачів проти Planet49 GmbH* (справа C-673/17 2019).
5 Справа C-507/17 (2019).

правова база гарантує, що в інтернет-просторі застосовуються ті самі права та механізми їхнього захисту, що й у реальному світі, для убезпечення демократичних процесів у цифрову епоху від неправомірних впливів.

Розділ 2

ЗМІЦНЕННЯ ДЕМОКРАТІЇ В ІНТЕРНЕТ-ПРОСТОРІ: ЄВРОПЕЙСЬКІ ПРАВИЛА У СФЕРІ ЦИФРОВІЗАЦІЇ ТА ВИБОРИ

2.1. ПРАВО НА ПРИВАТНІСТЬ ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У ВИБОРЧИХ ПРОЦЕСАХ

Виборчі органи дедалі частіше збирають, опрацьовують та використовують персональні дані для підвищення ефективності виборчого циклу. Учасники виборів можуть використовувати такі дані, зокрема, для ідентифікації та реєстрації виборців і планування та ведення виборчих кампаній. Однак така залежність від збору персональних даних створила тривалу колізію між принципами захисту даних та вимогами до проведення виборів. До прикладу, списки виборців мають бути прозорими та доступними для перевірки усіма зацікавленими сторонами, але вимога такої відкритості може суперечити обов'язку захищати персональні дані фізичних осіб.

Зростаюча залежність ОАВ від збору персональних даних створила тривалу колізію між принципами захисту даних та вимогами до проведення виборів.

Виборчі органи повинні визнавати цей конфлікт і розробляти механізми, які б відповідали як принципам захисту особистих даних, так і вимогам демократичного виборчого процесу. За таких обставин Міжнародний інститут демократії та сприяння виборам (International IDEA) розробив керівні принципи щодо використання біометричних технологій під час виборів (Wolf et al. 2017), а також базу даних з довідковою інформацією про використання інформаційно-комунікаційних технологій (ІКТ) у виборах (International IDEA n.d.). Але слідувати будь-яким рекомендаціям варто з максимальною обережністю та розумінням серйозних викликів, які створює використання цифрових технологій для підвищення ефективності виборчих процесів, зокрема в частині забезпечення права на приватність та захист персональних даних.

Відтак, для дотримання права на приватність та захист особистих даних ЄС ухвалив загальний регламент (GDPR) [Європейський Союз 2016]. Цей правовий акт має на меті захист визнаних Хартією основоположних прав, як от повага до приватного та сімейного життя (Стаття 7) і захист особистих даних (Стаття 8). Такі ж заходи захисту передбачені Статтею 16(1) ДФЄС. Головною метою Регламенту є встановлення принципів та правил захисту даних, яких повинні дотримуватися як державні органи, так і приватні суб'єкти. Тож усі держави-члени ЄС мають оновити свої чинні національні закони про захист даних у відповідності до вимог GDPR, аби гармонізувати правові рамки та забезпечити вільний обмін персональними даними між країнами (FRA and CoE 2018: 29).

Для проведення демократичних виборів ОАВ мають забезпечувати право на приватність та захист даних у виборчому контексті (Gross 2010: 5–6). Водночас, будучи інтегрованими до ширшої системи європейських цінностей, такі права можуть бути обмеженими, якщо це необхідно для досягнення важливих цілей загального суспільного інтересу. Обмеження у частині захисту даних та права на приватність мають оцінюватися для кожного конкретного випадку і за конкретних обставин. Наприклад, на підставі Статті 52(1) Хартії та Статті 23(1) GDPR, для проведення вільних і справедливих виборів допускається обмеження обсягу права на захист персональних даних у якості пропорційного заходу, який обов'язково:

- застосовується відповідно до закону;
- зберігає сутність фундаментального права на захист персональних даних;
- відповідає принципам пропорційності, необхідності та законної мети; та
- визнається ЄС необхідним для досягнення важливих цілей загального суспільного інтересу (FRA and CoE 2018: 36).

Для проведення вільних і справедливих виборів допускається обмеження обсягу права на захист персональних даних у якості пропорційного заходу.

2.1.1. **Застосування принципів GDPR у виборах**

У контексті демократичних виборів технології широко використовуються для збору, зберігання та обробки персональних даних. Прикладами тут можуть бути процеси реєстрації, біометричної ідентифікації та електронного голосування. Тож Стаття 5 GDPR визначає, що використання таких технологій виборчими суб'єктами має відповідати таким принципам: (a) законність, доброчесність та прозорість; (b) обмеження цілей використання; (c) мінімізація обсягу

Вставка 2.1. **Огляд ключових елементів GDPR у контексті виборів**

Регламент підтримує демократію та верховенство права через запобігання зловживанню персональними даними, сприяння прозорості та забезпечення підзвітності у виборчих процесах (Європейська комісія, без дати). Ці елементи є особливо актуальними у контексті проведення політичних онлайн-кампаній, коли персональні дедалі частіше використовуються для мікротарґетингу виборців, і це часто викликає занепокоєння щодо маніпуляцій та порушення конфіденційності.

Регламент встановлює чіткі правові рамки для унеможливлення незаконного збору та обробки даних виборців, забезпечуючи належне дотримання прав громадян та цілісність виборів. В епоху поширеного застосування техніки мікротарґетингу на основі зібраних персональних даних користувачів для ведення політичних кампаній, GDPR є важливим механізмом для забезпечення дотримання демократичних принципів та основних прав у виборчих агітаційних стратегіях (Monteleone 2019).

Інтегруючи жорсткі принципи захисту персональних даних до правової бази ЄС, GDPR гарантує прозору, доброчесну та підзвітну поведінку політичних акторів, онлайн-платформ та виборчих органів. Такі правові гарантії захищають цілісність виборів, запобігають надмірним впливам на демократичний процес прийняття рішень та зміцнюють верховенство права у межах Союзу.

персональних даних; (d) обмежене у часі зберігання даних; та (e) забезпечення цілісності й конфіденційності використаних даних.

Саме цими принципами унормовується обробка персональних даних. Будь-які обмеження або винятки із зазначених принципів мають бути передбачені законом, переслідувати законну мету, і у кожному окремому випадку оцінюватися як пропорційний захід, необхідний для досягнення цілей демократичного суспільного інтересу (Стаття 23[1] GDPR).

Відтак у контексті вільних і справедливих виборів законність обробки персональних даних виборчими суб'єктами має ґрунтуватися на одній з трьох підстав: (a) юридичне зобов'язання; (б) згода суб'єкта даних; або (в) необхідність реалізації заходів для досягнення законної мети в інтересах суспільства.

Наприклад, для формування надійного списку виборців у конкретному виборчому окрузі ОАВ має повноваження обробляти персональні дані виборців з метою впровадження системи реєстрації та автентифікації виборців. Така обробка

персональних даних може бути дозволена на підставі вільної, інформованої та однозначної згоди (Стаття 4[11] та Стаття 7 GDPR) або ж на підставі національного виборчого законодавства (Рада Європи 2024). За умови дотримання однієї з двох наведених норм, обробка персональних даних виборчими органами у процесі впровадження ШІ або інших цифрових технологій у виборах вважається законною. Іншими словами, за нормами Регламенту, виборчі органи завжди повинні мати чітко визначену правову основу для обробки персональних даних.

У контексті політичної реклами в Інтернеті згода на обробку даних без значущої обізнаності з боку користувача використовується для обходу вимог GDPR та отримання величезних обсягів персональних даних.

2.1.2. **Проблема згоди на обробку даних**

Відповідно до вимог Регламенту, існують обмеження щодо обробки персональних даних. У контексті політичної онлайн-реклами низка суб'єктів розвінчали ілюзію реального отримання вільної, поінформованої та однозначної згоди користувача, необхідної за вимогами GDPR. Наприклад, новий Регламент (ЄС) 2024/900 про прозорість і тарґетинг політичної реклами (TTPA) застерігає від прихованої агітації, яка «намагається або фактично істотно спотворює чи то послаблює прийняття особою незалежного та інформованого рішення» (пункт 75 TTPA). Європейський інспектор із захисту даних (EDPS) підкреслює ризики, пов'язані із «спонуканням користувачів до прийняття ненавмисних, небажаних і потенційно шкідливих рішень щодо надання дозволу на обробку їхніх персональних даних» (Європейський інспектор з захисту даних 2022: 2). Простіше кажучи, згода користувачів використовується для обходу вимог GDPR і отримання величезних обсягів персональних даних для подальшого їх використання для цілей політичної онлайн-агітації без належної обізнаності з боку користувача.

Стосовно особливих категорій персональних даних — як от політичні переконання, етнічна приналежність або сексуальна орієнтація — їхня обробка заборонена як така (Стаття 9 GDPR) без надання явної згоди на обробку таких даних, або ж якщо не застосовуються інші правові підстави, зазначені у Статті 9(2) GDPR. Регламент TTPA застосовує ті ж самі критерії: заборонено використання особливих категорій персональних даних для цілей політичної онлайн-реклами, зокрема для методів тарґетингу та доставки такої реклами, за винятком випадків, коли суб’єкт даних надає явну та окрему згоду на їх використання для політичної реклами (Стаття 18 TTPA).

Можливість отримувати згоду на обробку даних без усвідомленої обізнаності з боку користувача, яка

використовується для обходу вимог GDPR щодо обробки чутливих даних, разом з відсутністю дієвих механізмів для запобігання зловживанням з боку приватних суб'єктів призвели до справжнього буму політичної реклами в Інтернеті. Використання персональних даних для цілей політичної онлайн-агітації змінило методи тарґетування та залучення виборців. Завдяки технікам профілювання в агітаційних онлайн-кампаніях почали використовувати системи штучного інтелекту (ШІ) для мікротарґетингу громадян на платформах соціальних медіа через надсилання персоналізованих політичних повідомлень (Juneja 2024).

Метод мікротарґетингу передбачає:

- збір даних та поділ виборців на сегменти за такими характеристиками, як певні риси особистості, інтереси, походження або попередня виборча поведінка;
- розробку персоналізованого політичного контенту для кожного сегмента; та
- використання каналів комунікації для донесення таких персоналізованих повідомлень до цільових сегментів виборців (International IDEA 2018).

Такі методи можуть бути корисними як для політичних партій, так і для виборчих органів, адже вони спрощують донесення інформації до людей, які зазвичай не беруть участі у виборчих процесах. Однак ці інструменти можна також використовувати для маніпулювання свідомістю громадян та підриву суспільної злагоди через перешкоджання відкритим публічним обговоренням, загострення політичної поляризації та сприяння поширенню дезінформації (Gorton 2016). Використання методів тарґетингу на основі зібраних особистих та конфіденційних даних часто відбувається без згоди або чіткого усвідомлення користувачами (Bashyakarla et al. 2019). Все це може суттєво вплинути на цілісність виборів. Крім того, недобросовісні практики отримання згоди на використання особистих даних створюють уразливості, якими можуть скористатися зловмисники для поширення дезінформації та маніпулятивного контенту.

Недобросовісні практики отримання згоди на використання особистих даних створюють уразливості, якими можуть скористатися зловмисники для поширення дезінформації та маніпулятивного контенту.

2.1.3. **Техніки мікротарґетингу та доставки повідомлень для охоплення виборців: відповідність використання ШІ та автоматизованого прийняття рішень до вимог GDPR**

Загальний регламент про захист даних (GDPR) визнає, що автоматизовані процеси прийняття рішень, як от системи

штучного інтелекту, для профілювання або доставки онлайн-реклами можуть мати серйозні наслідки. Так, Стаття 22 GDPR визначає, що користувач має право не підпадати під рішення, що ґрунтується виключно на автоматизованій обробці даних (без участі людини у процесі прийняття рішення). Однак Стаття 22[1] Регламенту також визначає, що моделі ШІ можуть бути навчені на основі персональних даних у разі існування конкретної законної підстави, як от згода користувача, договір або законний інтерес. Крім того, Регламент також передбачає, що громадяни мають бути поінформовані про намір навчити модель ШІ та мати право на заперечення або відкликання своєї згоди на використання їхніх персональних даних. Нарешті, фізичні особи можуть звернутися до контролера даних за ґрунтовною інформацією про логіку обробки або із проханням про перегляд автоматизованого рішення людиною.

Та попри існування таких правил, організації громадянського суспільства і науковці наголошують на обмеженому застосуванні Регламенту до систем ШІ, як і на негативних наслідках для обсягу прав користувачів. Наприклад, навіть якщо онлайн-платформи гарантують, що певна категорія персональних даних збиратися не буде, це не припиняє отримання та консолідації інших даних, які цілком дозволяють розкривати конфіденційну інформацію про користувачів, як от їхні політичні погляди, яка може бути використана компаніями соціальних медіа, брокерами даних або третіми сторонами. До того ж, з огляду на саму природу інструментів ШІ з поглибленим машинним навчанням, суб'єкти даних (громадяни) не можуть отримати змістовного пояснення щодо процесів обробки їхніх персональних даних, адже системи ШІ за своєю суттю залишаються непрозорими та не піддаються інтерпретації (Juneja 2024: 12; Європейське партнерство за демократію 2022: 5). Більш того, фрагментоване та відтерміноване застосування GDPR у проведенні онлайн-кампаній (Massé 2023: 3–4) ще більше ускладнює дотримання основоположних принципів Регламенту, а саме мінімізацію збираних персональних даних та обмеження цілей їхнього використання.

2.1.4. **Техніки мікротарґетингу та ампліфікації у контексті GDPR**

Як вже зазначалося раніше, методи мікротаргетингу в політичних онлайн-кампаніях дозволяють знаходити користувачів через аналіз особистих та конфіденційних даних для створення персоналізованих профілів на основі їхньої поведінки в Інтернеті (International IDEA 2018). Попри

потенційну користь методів мікротарґетингу для громадян завдяки зростаючим можливостям поширення інформації про виборчі процеси, вони також становлять певну загрозу для прав і свобод, наприклад, через маніпуляції або іноземне втручання (European Parliamentary Research Service 2019: 22). Техніки мікротарґетингу та масштабування не лише підживлюють поляризацію аудиторій через бізнес-моделі великих технологічних компаній, але й базуються на непрозорій структурі, що заважає владі контролювати дотримання правил захисту персональних даних та обіг коштів між виробниками політичної реклами, компаніями соціальних медіа, політичними партіями та іншими суб'єктами політичного процесу (Heinmaa 2023: 15).

Подібні бізнес-моделі значною мірою використовують алгоритми, спрямовані на залучення аудиторій, що зазвичай надають пріоритет емоційно зарядженому або суперечливому контенту — часто згадуваному як «приманка для гніву» — з метою привернути максимальну увагу користувачів та збільшити доходи від реклами. Така динаміка стимулює поширення наративів, спрямованих на поляризацію та поглиблення розломів у суспільстві. Відсутність прозорості щодо методів просування контенту, джерел фінансування та цільових груп користувачів майже унеможливлює розуміння алгоритмічних рішень, а відтак і ким, за яких умов та яка саме інформація була переглянута, що по суті підриває принцип підзвітності та демократичного контролю. Одним з найбільших викликів для виборчих органів є пошук можливостей для контролю над персоналізованою виборчою онлайн-агітацією в умовах непрозорості системи.

Одним з найбільших викликів для виборчих органів є пошук можливостей для контролю над персоналізованою виборчою онлайн-агітацією в умовах непрозорості системи.

2.1.5. **Обмежене використання особливих категорій персональних даних у виборчому контексті**

Як бачимо, застосування вимог GDPR у виборчих процесах може як обмежуватися, так і створювати певні ризики.

У відповідь на значні виклики, пов'язані з використанням персональних даних у політичній онлайн-рекламі — відсутність прозорості, профілювання на основі чутливої інформації та потенційна маніпуляція поведінкою виборців — Європейський інспектор із захисту даних закликав заборонити збирання та обробку окремих категорій персональних даних, включно з інформацією про стан здоров'я, сексуальну орієнтацію та політичну приналежність особи (Європейський інспектор із захисту даних, 2022). Ці рекомендації спричинені

занепокоєнням, що вимог GDPR може бути недостатньо для запобігання використанню чутливих даних у політичних кампаніях. Така позиція, зокрема, узгоджується з положеннями Статті 18 нового Регламенту ЄС 2024/900 про прозорість і тарґетинг політичної реклами (TTPA), якими встановлені більш суворі обмеження на використання подібних даних для здійснення цільового впливу у політичному контексті.

У демократичному суспільстві не може бути виправдання для збирання та обробки чутливих даних з метою ведення політичних кампаній в Інтернеті.

У демократичному суспільстві не може бути виправдання для збирання та обробки чутливих даних з метою ведення політичних кампаній в Інтернеті. Потенційні ризики, пов'язані з техніками мікротарґетингу, неналежним дотриманням вимог GDPR виборчими органами та органами із захисту даних, а також проблеми з отриманням особистої згоди за правилами Регламенту є вагомими аргументами проти дозволу на будь-які винятки щодо використання особливих категорій персональних даних для цілей політичної реклами в Інтернеті.

Підсумовуючи, використання технік мікротарґетингу під час виборів також виявило недостатнє застосуванні правил GDPR щодо політичної реклами в Інтернеті. Обмеження потоку персональних даних між приватними та державними суб'єктами потенційно запобігає тим порушенням основоположних прав, які можуть підірвати виборчий процес. Тож забезпечення ефективного дотримання Регламенту у виборчому контексті є одним із найважливіших викликів для виборчих органів та політиків.

2.1.6. **Контролююча функція виборчих органів: оцінка впливу на захист даних**

У контексті виборів політичні партії, виборчі органи, окремі кандидати, організації громадянського суспільства (спостерігачі) та виробники і розповсюджувачі політичної реклами, серед інших, можуть підпадати під дію GDPR. Відтак, за діючими правилами, державні органи мають мандат і несуть правову відповідальність за дотримання порядку обробки персональних даних, тоді як інші суб'єкти, як от політичні партії, мають отримати на це персональну згоду або ґрунтовно довести свій законний інтерес (Європейська комісія 2018: 5).

Незалежно від того, чи збираються і обробляються дані на підставі юридичних зобов'язань, особистої згоди або ж законного інтересу, ОАВ та інші суб'єкти повинні чітко дотримуватися вимог Регламенту. За визначенням Європейського суду, усі суб'єкти, що беруть участь у зборі та

Вставка 2.2. **Парламентські вибори в Угорщині 2022 року**

Яскравим прикладом недотримання GDPR у виборчому контексті є ретельно задокументований випадок парламентських виборів 2022 року в Угорщині. Слабка система захисту даних у поєднанні з недостатнім контролем уповноваженими органами сприяли зловживанням з боку органів влади, політичних партій та приватних суб'єктів, що уможливило проведення незаконних та оманливих політичних кампанії в Інтернеті. У звіті БДІПЛ ОБСЄ (2022) висвітлено практики незаконного збору та неправомірного використання персональних даних в Інтернеті. Такі порушення підривають цінності та принципи ЄС щодо забезпечення чесних виборів, верховенства права та демократії в цілому.

Human Rights Watch (HRW) задокументувала використання чутливих персональних даних політичною партією «Фідес» та угорським урядом для проведення тарґетованих політичних кампаній під час виборів. За даними HRW (2022), «докази вказують на те, що уряд Угорщини діяв разом із правлячою партією у використанні персональних даних для цілей політичної кампанії».

Відсутність інституційної незалежності угорських ОАВ та органів із захисту даних спричинила занепокоєння щодо збереження конфіденційності виборців (HRW 2022). Схожу стурбованість висловила Європейська спілка громадянських свобод (2022): «У випадках, коли *de jure* незалежні інституції *de facto* перебувають під контролем правлячої партії, ключового значення набуває механізм забезпечення дотримання законодавства на рівні ЄС. Малоймовірно, що національні наглядові органи будуть забезпечувати дотримання законодавства у нейтральний та неупереджений спосіб».

Крім того, роль соціальних медіа у виборах 2022 року виявила неналежне застосування GDPR та виклики для виборчих органів у частині моніторингу політичних кампаній в Інтернеті. Союз громадянських свобод Європи (2022: 17–18) повідомив, що соціальні медіа відіграли вирішальну роль у розробці персоналізованих онлайн-кампаній з порушенням принципів та правил GDPR. Виробники і поширювачі політичної онлайн-реклами мали змогу агітувати окремих осіб на основі аналізу чутливих характеристик, як от стать, сексуальна орієнтація або політична приналежність, використовуючи такі інструменти, як списки клієнтів, налаштовані аудиторії та створені «бульбашки» у соцмережах. Водночас не було чітких доказів отримання цими кампаніями свідомої, вільної та інформованої згоди від осіб, чиї персональні дані були використані. HRW (2022) висловила подібні зауваження, зазначивши, що непрозорий характер онлайн-платформ дозволив політичним партіям тарґетувати політичну рекламу з мінімальною прозорістю.

HRW (2024) також повідомила, що контроль уряду над ЗМІ серйозно вплинув на незалежність журналістики та свободу слова, що безпосередньо позначилося на виборчому процесі. Таке системне підривання свободи ЗМІ є прямою загрозою для

Вставка 2.2. **Парламентські вибори в Угорщині 2022 року (cont.)**

основоположних прав, зокрема тих, що стосуються свободи вираження поглядів та доступу до різних точок зору в контексті виборів.

Відповідь ЄС на обмеження свободи ЗМІ в Угорщині включала застосування механізмів, передбачених Статтею 7 Договору про Європейський Союз для боротьби із системними порушеннями у сфері верховенства права, незалежності судової влади та плюралізму ЗМІ як основоположних цінностей ЄС.

Випадок Угорщини підкреслює взаємопов'язаність цифрової політики та цілісності виборів, коли контроль над ЗМІ — як традиційними, так і цифровими — становить значну загрозу для справедливих виборів.

Уроки, винесені з виборів 2022 року в Угорщині, підкреслюють нагальну потребу у сильній та незалежній нормативно-правовій базі для забезпечення дотримання правил захисту даних у виборчому контексті. Ця база має включати такі заходи:

- суворе дотримання принципів та правил GDPR щодо обробки та обміну персональними даними між державними органами;
- посилене виконання положень GDPR у частині використання чутливих персональних даних для ведення політичних онлайн-кампаній; та
- посилення міжвідомчої взаємодії між органами із захисту даних та ОАВ з метою забезпечення більшої прозорості та підзвітності онлайн-платформ, які відіграють значну роль у сучасних виборчих кампаніях.

обробці персональних даних, кваліфікуються як «контролери», відтак набувають зобов'язань відповідно до законодавства про захист даних[6]. Навіть якщо інша юридична особа обробляє персональні дані від імені та за вказівкою контролера, вона автоматично підпадає під дію GDPR. Наприклад, якщо ОАВ залучає приватну компанію для підготовки біометричного списку виборців, обидві сторони мають обробляти отримані біометричні дані у відповідності до вимог GDPR.

Виконання стандартів GDPR означає дотримання згаданих вище принципів, зокрема мінімізації обсягів та обмеження мети використання збираних персональних даних, підзвітності, прозорості, безпеки та конфіденційності. Це вимагає від виборчих органів реалізації відповідних заходів для зменшення ризиків у сфері захисту даних та впровадження відповідних

6 Справа C-210/16, *Незалежний центр захисту даних Шлезвіг-Гольштейн проти Економічної академії Шлезвіг-Гольштейн* ECLI:EU:C:2018:388, пункт 26.

інструментів для забезпечення конфіденційності даних на етапі підготовки та у контексті проведення виборів.

Так, для випадків, коли обробка даних може потенційно створювати суттєві ризики для прав і свобод фізичних осіб, Регламент вимагає від контролерів проведення попередньої оцінки впливу своїх передбачуваних дій та інструментів захисту персональних даних. Стаття 35 GDPR «Оцінювання впливу на захист даних» визначає необхідність оцінювання не лише ризиків для прав і свобод суб'єктів даних, але також доцільності та пропорційності операцій опрацювання для дотримання вищезазначених принципів.

Якщо далі розглядати ситуацію на прикладі впровадження біометричного списку виборців, для оцінювання впливу на захист даних та з метою дотримання означених принципів АОВ має поставити питання: чи є така процедура необхідною для виконання завдання, пов'язаного з проведенням виборів? (Більш детально про це у розділі 3.3: Обробка даних органами адміністрування виборів).

2.2. **КІБЕРБЕЗПЕКА НА ВИБОРАХ**

У демократичному суспільстві кібербезпека передбачає захист цілісності виборів та «забезпечення прозорої роботи системи управління або цифрових систем, використовуваних для адміністрування виборів».

Виборчі органи, у співпраці з іншими відповідними установами, відповідають за управління та зменшення ризиків, включно із кіберзагрозами, що виникають у зв'язку з організацією та проведенням виборів. У демократичному суспільстві кібербезпека передбачає захист цілісності виборів та «забезпечення прозорої роботи системи управління або цифрових систем, використовуваних для адміністрування виборів» (Агентство Європейського Союзу з кібербезпеки, 2019: 4). Кіберзагрози, як от атаки на конфіденційність, цілісність та доступність пов'язаних з виборами даних або технологій, можуть підірвати вибори як такі (van der Staak and Wolf 2019).

Подібним чином — попри те, що іноземні інформаційні маніпуляції та втручання (FIMI) частіше асоціюються з дезінформацією — така ворожа діяльність також передбачає створення загроз для кібербезпеки та здійснення кібератак, спрямованих на критичну виборчу інфраструктуру. Широко використовувані для експлуатації вразливостей тактики, методи та процедури лише підкреслюють необхідність комплексного підходу до захисту цілісності виборів. Негативний вплив на

цілісність виборчих процесів може здійснюватися і через гібридні загрози: FIMI, поширення дезінформації у соціальних мережах та створення дипфейків з використанням штучного інтелекту.

У контексті регламентів ЄС кібербезпека передбачає захист цілісності, доступності та конфіденційності виборчих процесів на базі комплексного та інтегрованого підходу, який враховує усі потенційні ризики. Попри визнання компетенції та відповідальності кожної окремої країни-члена за організацію і проведення національних виборів, ЄС розробив низку ініціатив для протидії кіберзагрозам. З огляду на широке використання цифрових технологій для підтримки виборчих процесів, сприяння кібербезпеці в ЄС відіграє важливу роль у забезпеченні безпеки виборів в цілому.

Група співробітництва з питань мережевої та інформаційної безпеки (NIS Cooperation Group) — спільний проєкт держав-членів ЄС, Європейської комісії та Агентства Європейського Союзу з кібербезпеки (ENISA) — наголошує на необхідності особливої уваги до загроз у виборчий період, зважаючи на потенційну вразливість використовуваних технологій до «кібератак, системних збоїв, людських помилок, стихійного лиха та подібних непередбачуваних обставин, як от відключення електроенергії та збої у роботі мережі» (NIS Cooperation Group 2024: 4–5). Група співробітництва з питань мережевої та інформаційної безпеки підготувала довідник для забезпечення кібербезпеки виборчого процесу, у якому детально представила опрацьований підхід з урахуванням усіх можливих ризиків, а також роз'яснила основні кіберзагрози впродовж виборчого циклу, включно із спрямованими на політичні партії та політиків як безпосередніх акторів.

З огляду на можливість впливу людського фактору на кібербезпеку під час виборів, ініціативи ЄС закликають до співпраці та обміну знаннями щодо протидії дезінформації в Інтернеті та іншим гібридним загрозам, включно з FIMI. Так, Європейська мережа співпраці з питань виборів закликала до обміну інформацією та провідним досвідом між мережами держав-членів з метою оцінки ризиків та виявлення кіберзагроз або інших інцидентів, які можуть вплинути на цілісність виборів (Європейська мережа співпраці з питань виборів, без дати: 2). Європейська комісія (2023: параграф 20) також заохочує більш тісну «співпрацю між державними та приватними структурами у сфері забезпечення кібербезпеки на виборах» та підвищення

обізнаності про кібергігієну серед політичних партій, кандидатів, працівників ОАВ та інших пов'язаних з виборами структур.

Спільні майданчики для співробітництва є особливо важливими через обмежені повноваження ЄС у питаннях проведення виборів. Розподіл повноважень ґрунтується на положеннях Статей 4 та 5 Договору про Європейський Союз, за якими повноваження, не передані Союзу, залишаються у компетенції держав-членів. Відтак питання виборів значною мірою належать до національних юрисдикцій, що обмежує можливості ЄС приймати прямі законодавчі акти. Однак, у дозволених договорами межах, ЄС відіграє допоміжну роль через сприяння координації, підтримку добровільного співробітництва та заохочення до обміну провідним досвідом на спільних майданчиках для взаємного навчання та політичного діалогу.

Ініціативи ЄС закликають до співпраці та обміну знаннями щодо протидії дезінформації в Інтернеті та іншим гібридним загрозам, включно з FIMI.

Серед успішних прикладів варто згадати плідну міжвідомчу взаємодію між Європейською мережею співпраці з питань виборів та Групою співробітництва з питань мережевої та інформаційної безпеки, а також мережеві ініціативи, спрямовані на посилення стійкості виборчих процесів до кіберзагроз, як от EU-CyCLONe (Європейська мережа органів зв'язку щодо кіберкриз). У боротьбі з кіберзагрозами під час виборів можна також звернутися по допомогу та за узагальненим досвідом країн-членів до таких органів, як от Європейська рада із захисту даних (EDPB), Агентство Європейського Союзу з кібербезпеки, Координаційний центр реагування на надзвичайні ситуації, Європол та мережі регуляторів аудіовізуальних засобів масової інформації (Європейська мережа співробітництва з питань виборів, без дати).

2.3. **ОГЛЯД ПРАВОВОГО РЕГУЛЮВАННЯ ДІЯЛЬНОСТІ ОНЛАЙН-ПЛАТФОРМ У ЄВРОПІ**

Цілісність інформації під час виборів має вирішальне значення для виборчих процесів, особливо у контексті сучасних можливостей інформаційного охоплення в Інтернеті.

Цілісність інформації має вирішальне значення для виборчих процесів, зокрема це стосується і способів поширення необхідної інформації в онлайн-середовищі. В ЄС ці питання регулюються різними законодавчими механізмами, включно з DSA (Європейський Союз 2022).

DSA — це комплексна правова рамка, створена для забезпечення прозорості та цифрової безпеки шляхом визначення відповідальності та підзвітності різних

Вставка 2.3. **Що таке DSA і які його основні цілі?**

Акт про цифрові послуги (DSA) — це прийнятий у 2022 році регламент ЄС, яким визначаються правові стандарти для онлайн-контенту, поширюваного у соціальних мережах ЄС. DSA відіграє важливу роль у захисті демократії та цілісності виборів як регуляторний механізм у частині відповідальності та обов'язків онлайн-платформ і надавачів цифрових послуг. Регламент визначає низку основних принципів і правил для публікації та поширення онлайн-контенту надавачами посередницьких послуг, як от онлайн-платформами (наприклад, Facebook, Instagram або YouTube). Метою впровадження DSA є забезпечення прозорої та відповідальної діяльності цифрових платформ із дотриманням основоположних прав, гарантованих Договорами ЄС та Хартією.

Європейський парламент підкреслив важливість дотримання цінностей, закріплених у Статті 2 Договору про Європейський Союз, і наголосив на необхідності вкорінення в основи успішної та стійкої політики ЄС у сфері цифрових послуг відповідних фундаментальних прав, як от захист приватного життя та персональних даних, а також принципів недискримінації, свободи вираження поглядів та доступу до інформації (Європейський парламент, 2020).

DSA переважно спирається на Статтю 114 ДФЄС, яка надає Союзу повноваження вживати заходів для гармонізації національних законів, які безпосередньо впливають на формування та функціонування внутрішнього ринку. Ця правова основа дозволяє DSA узгоджувати відмінні національні правила, якими унормовані посередницькі послуги — зокрема щодо модерації контенту і запобігання поширенню дезінформації чи то незаконного контенту в Інтернеті — для забезпечення вільного обміну цифровими послугами між державами-членами із збереженням цілісності внутрішнього ринку.

постачальників цифрових послуг, особливо цифрових платформ з понад 45 мільйонами активних користувачів, з інтегрованими пошуковими системами та соціальними мережами, як от Facebook, Instagram та YouTube. З одного боку, DSA можна розглядати як горизонтальний регуляторний механізм, створений на підтримку інших профільних законодавчих актів для забезпечення доброчесності, довіри та безпеки у цифровому середовищі. З іншого боку, DSA визначає зобов'язання для постачальників цифрових послуг з метою запобігти поширенню незаконного або шкідливого онлайн-контенту, відтак захищає основоположні права громадян, верховенство права та демократичні цінності.

Регулювання контенту шляхом модерації за рішенням власників приватних платформ зачіпає сферу основних прав і питань демократії. Повноваження постачальників цифрових послуг

(приватних суб'єктів) дискретно вирішувати, який саме контент має залишатися для розповсюдження в Інтернеті, зачіпає конституційні питання, зокрема забезпечення права на політичні переконання та свободу вираження поглядів. Згідно з вимог ами DSA, «відповідальна та сумлінна поведінка постачальників посередницьких послуг [є] передумовою для безпечного, передбачуваного і надійного онлайн-середовища із одночасним забезпеченням можливості для громадян Союзу та інших осіб вільно користуватися своїми основоположними правами, зокрема свободою вираження поглядів та свободою доступу до інформації» (пункт 3 преамбули DSA). Тож перед ЄС постає непростий виклик, коли йдеться про регулювання онлайн-платформ для захисту, просування та зміцнення закріплених у Хартії основоположних прав та європейських цінностей.

Разом з DSA як першорядним європейським законом для боротьби із шкідницькою діяльністю в Інтернеті, існує низка інших законів ЄС, дотичних до врегулювання потоку інформації під час виборів. І замість розглядати кожний законодавчий акт окремо, цей розділ зосереджується на принципах та загальних правилах, якими унормовується модерація контенту в онлайн-просторі для захисту основоположних прав та забезпечення цілісності виборів.

2.3.1. **Виклики, пов'язані з модерацією онлайн-контенту: DSA та принципи ЄС**

DSA підтримує три загальні принципи, відображені у Директиві 2000/31/ЄС «Про деякі правові аспекти інформаційних послуг [...]» та судовій практиці Європейського суду (Madiega 2022: 2), а саме:

- *Принцип країни походження (параграф 38 DSA):* Постачальники онлайн-послуг мають дотримуватися вимог законодавства держав-членів, у яких вони легально зареєстровані.

- *Режим обмеженої відповідальності (Стаття 9 DSA):* Онлайн-посередники звільняються від відповідальності за переданий та розміщений контент (користувачів) у разі відсутності «фактичної обізнаності» (Стаття 6 DSA) про незаконну інформацію або діяльність на їхніх платформах.

- *Заборона загального моніторингу (Стаття 8 DSA):* Держави-члени мають утримуватися від накладання на онлайн-

посередників загального обов'язку моніторингу всієї інформації, розміщеної на їхніх онлайн-ресурсах.

Ці принципи гарантують переважну відсутність відповідальності для власників онлайн-ресурсів за незаконну діяльність або неправомірний контент, розміщений користувачами (принцип обмеженої відповідальності). Крім того, вони захищають свободу вираження поглядів користувачів в Інтернеті, запобігаючи моніторингу та контролю над створенням контенту з боку приватних онлайн-платформ.

DSA застосовує процедурний підхід для реалізації цих принципів. Замість цензурувати або визначати, який саме контент може залишатися в Інтернеті, ним визначаються конкретні процедури для виявлення незаконного або шкідливого контенту. Такий підхід отримав визначення «процедуризації відповідальності посередників» (Busch and Mak 2021). Відтак, відповідно до принципу країни походження, держави-члени можуть на власний розсуд визначати неправомірність контенту і застосовувати національні регуляторні механізми, які не суперечать основним принципам та правилам DSA. Наприклад, вимоги до ведення політичних кампаній в Інтернеті у рамках національного виборчого законодавства можуть бути приведеними у відповідність до рамок DSA і визначеного ним підходу до модерації контенту у цифровій сфері.

DSA застосовує багаторівневий підхід, за яким обсяг накладених зобов'язань залежить від типу, міри впливу та розміру ресурсів для надання посередницьких онлайн-послуг, що поділяються на три групи:

- *Прості канали.* Надають послуги для забезпечення обміну інформацією у комунікаційній мережі (наприклад, інтернет-провайдери, органи управління DNS, месенджери).

- *Проксі-сервери.* Забезпечують автоматичне, проміжне та тимчасове зберігання інформації третіх сторін (наприклад, мережі доставки контенту).

- *Хостинг-провайдери.* Зберігають інформацію на запит третіх сторін. Це можуть бути пошукові системи, соціальні мережі, сервіси обміну контентом, торгові платформи, дискусійні форуми, хмарні сервіси та магазини додатків. До цієї категорії

відносять як онлайн-платформи, так і дуже великі онлайн-платформи.

Аби краще зрозуміти взаємозв'язок між безпекою висловлювань в Інтернеті та цілісністю виборів, у цьому звіті уваги здебільше надано дуже великим онлайн-платформам (VLOP) та дуже великим онлайн-пошуковим системам (VLOSE), тобто хостинг-провайдерам із понад 45 мільйонами активних користувачів на місяць. Такі онлайн-сервіси створюють особливі ризики щодо поширення дезінформації та неправомірного контенту. Прикладами таких провайдерів можуть бути Google (VLOSE), LinkedIn (VLOP), Facebook (VLOP), Instagram (VLOP) тощо.

Одним з головних завдань DSA є протидія поширенню незаконного контенту в Інтернеті та попередження суспільних ризиків, пов'язаних з дезінформацією. Саме тому правила вимагають від провайдерів у їхніх положеннях та умовах для користувачів докладно інформувати про будь-які обмеження, що можуть бути накладені у зв’язку з використанням послуг (Стаття 14.1 DSA), зокрема про політики модерації контенту, процедури, заходи та автоматизовані інструменти (алгоритми), що використовуються для впровадження та моніторингу дотримання таких умов і положень. Наприклад, Facebook забороняє публікацію оголених зображень, тож за користувацькими умовами будь-який оголений контент блюриться або видаляється за допомогою алгоритмічних інструментів, що не суперечить правилам DSA.

Одним з головних завдань DSA є протидія поширенню незаконного контенту в Інтернеті та попередження суспільних ризиків, пов'язаних з дезінформацією.

Однак будь-які обмеження мають належним чином поважати права та законні інтереси усіх залучених сторін, включно з основоположними правами користувачів, як от вільне вираження поглядів, свобода та плюралізм ЗМІ та інші закріплені у Хартії права і громадянські свободи.

Крім того, DSA вимагає від усіх хостинг-провайдерів та онлайн-платформ, незалежно від їхнього розміру, впроваджувати механізми зворотного повідомлення та вимоги вжити заходів (стаття 16 DSA), докладно і вчасно інформуючи користувачів щодо того, який саме контент може вважатися неправомірним. Іншими словами, користувачам має бути надана можливість у простий та зручний спосіб повідомляти онлайн-платформу (наприклад, Facebook) про розміщення неправомірного контенту (наприклад, заборонених правилами інтимних чи то підроблених матеріалів). І такі механізми також мають відповідати вимогам щодо обґрунтування претензії (Стаття 17 DSA) та іншим

визначеним правилам для захисту прав і законних інтересів усіх зацікавлених сторін, зокрема гарантованих Хартією прав і свобод.

2.3.2. **Модерація контенту для протидії гендерному насильству в Інтернеті**

Такі ж самі принципи і правила DSA застосовуються в рамках Директиви ЄС про протидію насильству щодо жінок та домашньому насильству (Європейський Союз 2024c), зокрема видання розпоряджень або застосування інших заходів для видалення чи то блокування доступу до матеріалів із зображенням та будь-якими проявами гендерного насильства в Інтернеті. У разі, якщо опубліковані матеріали мають ознаки кримінального злочину, їхнє видалення або обмеження доступу має здійснюватися у прозорий спосіб та з належними гарантіями. Кримінальним кібердіянням визнається:

- *розповсюдження інтимних або підроблених матеріалів без згоди особи* (Стаття 5), тобто надання широкого доступу до зображень, відео чи подібних матеріалів, які зображують сексуальні дії або інтимні частини тіла особи за допомогою ІКТ без її згоди;

- *кіберпереслідування* (Стаття 7), що включає публічно доступну загрозливу або образливу поведінку, спрямовану на певну особу, яка завдає їй серйозної психологічної шкоди, або ж надання публічного доступу до приватних даних переслідуваної особи без її згоди;

- *кіберпідбурювання* до насильства або ненависті (Стаття 8) стосується суспільних закликів до насильства та ненависті, зокрема за ознакою статі, проти певної групи осіб або окремого члена такої групи шляхом публічного поширення подібного контенту за допомогою ІКТ.

Користувачам має бути надана можливість у простий та зручний спосіб повідомляти онлайн-платформу (наприклад, Facebook) про розміщення неправомірного контенту.

У контексті виборчих процесів для таких правопорушень обтяжуючими обставинами вважається його вчинення шляхом зловживання визнаною суспільною довірою, владою або впливом (Стаття 11[m] Директиви), або якщо правопорушення вчинено проти особи через її публічне представництво (наприклад, щодо жінки-політикині).

Для цілей цієї Директиви під «компетентними органами» з повноваженнями вимагати видалення або блокування неправомірного матеріалу слід розуміти орган або органи,

призначені відповідно до національного законодавства для виконання обов'язків, передбачених цією Директивою (параграф 14). Відтак, лише національне виборче законодавство може надати ОАВ повноваження вимагати видалення або блокування доступу до перелічених вище неправомірних матеріалів, пов'язаних з виборчим процесом.

2.3.3. **Роль ЗМІ у демократичних виборчих процесах: модерація контенту в онлайн-медіа**

Виняток із загальних правил щодо модерації контенту на VLOP у ЄС стосується порядку модерації медіаконтенту відповідно до Європейського акту про свободу медіа (EMFA) (Європейський Союз 2024b). EMFA є вертикальним регулюванням (тобто його норми та вимоги застосовуються безпосередньо і переважають над національними правилами держав-членів), і цей акт не відміняє, а доповнює регламент DSA. Відповідно до Статті 18(4), VLOP не може призупиняти або обмежувати видимість контенту від самопроголошеного постачальника медіапослуг (такого як *The Guardian, The New York Times* або *France 24*), окрім як за спеціальною процедурою, викладеною у законі. Цією нормою визнається важливість свободи преси, плюралізму ЗМІ та вільної журналістики як основних демократичних інститутів, що гарантують громадянам доступ до достовірних новин.

Навіть більшої ваги ці фундаментальні права набувають у контексті виборів. Тому, на думку законодавців ЄС, самопроголошені постачальники медіапослуг не можуть бути односторонньо заблокованими VLOP виключно на підставі користувацьких умов та положень чи то на інших окремих правових підставах (Nenadić and Brodgi 2023).

У разі наміру призупинити поширення контенту з ознаками дезінформації згідно із встановленими користувацькими умовами, VLOP має попередньо звернутися до постачальника медійних послуг із заявою з поясненням свого рішення та надати 24 години на відповідь. Протягом цього періоду VLOP не може ані видаляти, ані обмежувати поширення контенту.

Однак важливо зазначити, що ця норма не застосовується до контенту, який за законодавством ЄС вважається неправомірним, як от мова ненависті або інтимний чи підроблений матеріал, розміщений без згоди особи. Відтак неправомірний контент, розміщений постачальниками медійних послуг, підпадає під дію правил DSA та користувацьких умов онлайн-платформ. VLOP мають дотримуватися вимог Статті 9

DSA та видаляти незаконний контент на підставі розпоряджень, виданих відповідними судовими або адміністративними органами; запровадити для користувачів механізми для повідомлення про порушення з вимогою вжити заходів; інформувати компетентні національні правоохоронні або судові органи у разі виявлення ознак кримінального правопорушення на їхніх платформах; та блокувати користувачів, які зловживають їхніми послугами через поширення явно неправомірного контенту (Стаття 23 та параграф 62 DSA). Нарешті, VLOP також мають дотримуватися зобов'язань щодо оцінювання та зменшення ризиків для захисту від незаконного контенту (Nenadić і Brodgi 2023).

Неправомірний контент, розміщений постачальником медійних послуг, підпадає під дію правил DSA та користувацьких умов онлайн-платформ.

2.3.4. Зобов'язання належної обачності у рамках DSA: оцінка ризиків та заходи щодо їх пом'якшення

Як зазначалося раніше, DSA застосовує багаторівневий підхід, за яким обсяг накладених зобов'язань залежить від типу, міри впливу та розміру ресурсів для надання посередницьких онлайн-послуг. Зважаючи, що VLOP та VLOE віднесені до категорії найбільших хостинг-провайдерів, вони підлягають

Блок 2.4. Короткий огляд EMFA: забезпечення вільного та відповідального медійного простору в ЄС

EMFA посилює захист плюралізму ЗМІ, редакційної незалежності та безпеки журналістів. Ґрунтуючись на принципах демократії, верховенства права та основоположних прав людини, EMFA керується Статтею 11 Хартії, що гарантує свободу вираження поглядів та інформації, і Статтею 2 Договору про Європейський Союз, яка проголошує демократію однією з основних цінностей ЄС.

EMFA доповнює чинне законодавство ЄС, включно із DSA та GDPR, у вирішенні проблем, пов'язаних з розвитком цифровізації на фоні проявів політичного втручання та економічного тиску на незалежність ЗМІ. Впроваджуючи конкретні запобіжні заходи проти зловживання засобами нагляду, надмірного впливу держави та непрозорої структури власності, EMFA підтримує вільну від втручання журналістику та доступ громадян до достовірної, різноманітної та незалежної інформації.

Запобігаючи політичному та економічному тиску на ЗМІ, посилюючи запобіжні заходи проти зловживань шпигунським програмним забезпеченням та підвищуючи прозорість власності й фінансування засобів масової інформації, EMFA підтримує свободу преси як важливу опору демократії. У поєднанні з DSA та GDPR, EMFA сприяє створенню стійкої та справедливої цифрової інформаційної екосистеми, забезпечуючи захист основоположних прав у дедалі більш цифровому медіапросторі.

особливому унормуванню. Такі корпорації та визначені для них зобов'язання підпадають під компетенцію Європейської комісії.

Одним з найважливіших зобов'язань для VLOP та VLOE є ретельне визначення, аналіз та оцінка будь-яких системних ризиків, що виникають у результаті проєктування або функціонування їхніх платформ, включно з алгоритмічними системами, про що зазначено у Статті 34 DSA. Іншими словами, платформи мають самостійно оцінювати свої системні ризики, включно з такими:

- поширення неправомірного контенту на їхніх ресурсах;
- будь-які фактичні або передбачувані негативні наслідки для належного дотримання основоположних прав, включно із свободою вираження поглядів, плюралізмом ЗМІ та правом громадян голосувати і балотуватися на виборах;
- будь-який фактичний або передбачуваний негативний вплив на громадське обговорення і виборчі процеси; та
- будь-які фактичні або передбачувані негативні наслідки для попередження гендерного насильства.

За результатами проведеного оцінювання мають готуватися звіти з переліком найнебезпечніших та найпоширеніших ризиків за рівнем пріоритетності, а також запропонованими розумними, пропорційними та ефективними пом'якшувальними заходами на випадок інциденту. Крім того, у звітах мають бути відображені кращі практики для VLOP та VLOE, що дозволяють ефективно запобігати та пом'якшувати системні ризики. Звіти мають бути представлені відповідним регулятором цифрових послуг у державах-членах, а на запит — до Європейської комісії (стаття 34[3] DSA).

У разі виявлення ризиків мають бути вжиті розумні, пропорційні та ефективні пом'якшувальні заходи

Деякі з фактичних та потенційних ризиків, серед іншого, включають: відсутність посилання на різноманітні й авторитетні джерела в онлайн-контексті; маніпулятивні техніки мікро- та нанотарґетингу; неналежне позначення політичної реклами; радикалізацію та поляризацію онлайн-просторів; дезінформаційні кампанії та мову ненависті; а також спроби впровадження цензури з боку діючих політиків або кандидатів (Reich and Calabrese 2025).

Вставка 2.5. **DSA як запорука цілісності виборів: випадок Румунії**

24 листопада 2024 року крайній правий екстремістський кандидат Калін Георгеску отримав найбільшу кількість голосів у першому турі президентських виборів у Румунії. Попри відсутність бюджету на виборчу кампанію, він отримав 23% голосів (близько 2 мільйонів виборців) завдяки веденню агітації майже винятково в Інтернеті, головним чином у TikTok.

Згодом інші кандидати у президенти звернулися до суду. На той момент румунські спецслужби звітували про задокументоване використання методів маніпулювання свідомістю виборців через соціальні мережі, кібератаки і втручання з боку Росії у вибори та інші незаконні онлайн-практики. З огляду на обставини, 6 грудня 2024 року Конституційний суд Румунії вирішив скасувати результати виборів *ex officio*.

Численні порушення, виявлені різними державними органами, свідчили про маніпуляції з голосами, недотримання принципів прозорості та вільного і чесного виборчого процесу, зокрема щодо використання цифрових технологій та штучного інтелекту для агітації, а також фінансування кампанії з незадекларованих джерел — все це разом порушувало виборче законодавство та підривало принцип рівних можливостей між політичними конкурентами (Венеціанська комісія, 2025). Зрештою, така сукупність порушень «спотворила вільний і чесний характер голосування, поставила під загрозу прозорість виборів і знехтувала вимогами закону до фінансування передвиборчої кампанії» (Barata and Lazăr 2025).

Щодо ймовірної маніпуляції голосуванням виборців через соціальні медіа, Європейська обсерваторія цифрових медіа повідомила, що у період між 10 і 24 листопада 2024 року кількість підписників на акаунт Георгеску фактично потроїлася (Botan 2024). Брутальна кампанія астротурфінгу (імітація масової громадської ініціативи для створення ілюзії запиту від суспільства), координована через тисячі акаунтів у TikTok і мережу оплачуваних інфлюенсерів, використовувала рекомендаційні системи платформи для штучного підвищення видимості повідомлень Георгеску. Проте кандидат у президенти не задекларував жодних витрат на агітацію (Cornea 2025). У результаті такої онлайн-стратегії хештеги, пов'язані з кампанією Георгеску, посіли дев'яте місце у глобальному рейтингу TikTok (VIGINUM 2025: 7).

Усі подібні механізми штучного підвищення видимості TikTok-акаунтів заборонені користувацькими умовами платформи. Однак створення ботів та залучення інфлюенсерів для експлуатації алгоритмів для ведення виборчої кампанії не визнається незаконною діяльністю ані за DSA, ані за TTPA (огляд технічних маневрів, здійснених кандидатом, див. на Рис. 2.1).

Вставка 2.5. **DSA як запорука цілісності виборів: випадок Румунії (cont.)**

Рисунок 2.1. Схема онлайн-кампанії на підтримку Георгеску, створена VIGINUM

Джерело: VIGINUM, «Маніпулювання алгоритмами та інструментальне використання інфлюенсерів: уроки президентських виборів у Румунії та потенційні ризики для Франції», лютий 2025 р., <https://www.sgdsn.gouv.fr/files/files/Publications/20250204_NP_SGDSN_VIGINUM_Rapport_public_Elections_roumanie_risques_france_VFF.pdf>, дата перегляду: 16 серпня 2025 р.

Відповідно до вимог DSA, Європейська комісія розпочала офіційне провадження проти TikTok, вимагаючи надати інформацію про заходи, реалізовані платформою для зменшення потенційної алгоритмічної упередженості під час виборчого процесу. Іншими словами, TikTok було запропоновано надати детальну інформацію про заходи, вжиті для «управління ризиками, що загрожують виборам або громадському обговоренню» і пов'язані з системами рекомендацій, зокрема з «координованою неавтентичною маніпуляцією або автоматизованим використанням сервісу». Крім того, платформа має надати роз'яснення своїх політиків щодо розміщення і просування політичної реклами та платного політичного контенту (Європейська комісія 2024e).

Цей випадок наочно доводить, як важко передбачити форму і рівень впливу заходів, до яких може вдаватися Європейська комісія проти онлайн-платформ, особливо з огляду на дискретність рішень самих приватних компаній щодо протидії системним ризикам на платформах під час виборів. Попри оприлюднені рекомендації Комісії щодо захисту цілісності виборів в онлайн-середовищі, наразі такі заходи не є юридично зобов'язальними; відтак міра їхнього застосування у кожних окремих виборах суттєво різниться. Крім того, на думку організацій громадянського суспільства, «рекомендації не містять критеріїв, за якими можна оцінити успішність або ж неефективність запропонованих заходів» (Alvarado Rincón 2025). Інші експерти, коментуючи цей випадок, підкреслили, що «майже неможливо упередити певні форми (ймовірно оплаченої) політичної агітації, якщо це просто короткі згадки у довгих відеосюжетах популярних блогерів про сучасні тенденції у макіяжі» (Barata and Lazăr 2025).

Вставка 2.5. **DSA як запорука цілісності виборів: випадок Румунії (cont.)**

Румунські президентські вибори 2024 року показали, як легко оманливі актори можуть використовувати алгоритмічні системи рекомендацій VLOP для маніпулювання виборчим процесом. Особливо варто звернути увагу на відповідальність онлайн-платформ соціальних медіа за гарантії безпечного онлайн-середовища у контексті виборів. Крім того, цей приклад лише підкреслює необхідність взаємодії між Європейською комісією та органами ОАВ й іншими національними акторами для моніторингу подібних інцидентів з метою запобігання порушенням з неповагою до європейських цінностей, включно з проведенням вільних, чесних і прозорих виборів.

2.4. **ПОЛІТИЧНА ОНЛАЙН-РЕКЛАМА: ШЛЯХ ДО ГАРМОНІЗАЦІЇ ЄВРОПЕЙСЬКОГО РЕГУЛЮВАННЯ**

DSA розглядає політичну рекламу в Інтернеті як один із видів онлайн-реклами та контенту. Відтак політична онлайн-реклама має відповідати як загальним правилам розміщення реклами, так і правилам модерації контенту за регламентом DSA (наприклад, користувацьким умовам, наявності механізмів повідомлення про порушення та вжиття відповідних заходів, надійному маркуванню, оцінкам системних ризиків тощо).

Стаття 3(r) DSA визначає рекламу як:

> «інформацію, призначену для просування повідомлення юридичної або фізичної особи, незалежно від комерційних або некомерційних цілей такого повідомлення, і представлену на інтерфейсі онлайн-платформи за винагороду, сплачену за просування цієї інформації».

Це визначення має два ключові елементи:

- чітко згадані «некомерційні цілі» (наприклад, політичний контент) та
- вимогу щодо просування контенту «за винагороду».

Відтак органічний політичний контент (неоплачуваний контент та інформаційні потоки, що керуються алгоритмічними системами рекомендацій) не підпадає під дію правил DSA для онлайн-реклами.

І навпаки, органічний політичний контент може підпадати під дію нового європейського регламенту, TTPA (Европейский Союз 2024a). Визначення політичної реклами за регламентом TTPA включає контент, який «зазвичай поширюється за винагороду» (стаття 3[2]). Іншими словами, органічні політичні висловлювання теоретично можуть підпадати під дію цього регламенту, і це викликає занепокоєння щодо потенційних обмежень свободи вираження поглядів та політичних висловлювань в онлайн-просторі (ARTICLE 19 2023; Heinmaa 2023).

Органічний політичний контент може підпадати під дію нового європейського регламенту про прозорість і тарґетування політичної реклами.

Таке дублювання нормативних положень фактично створює колізію між двома правовими рамками і може вплинути на виконання регламенту DSA. Іншим негативним наслідком може бути виникнення проблем координації між виборчими органами, контролерами цифрових послуг та іншими регуляторними органами (як от спеціалізовані органи з питань ЗМІ), причетними до забезпечення виконання нормативних актів ЄС щодо політичної реклами в Інтернеті (Heinmaa 2023).

Як зазначалося раніше (див. розділ 2.1.5), DSA вимагає від VLOP та VLOE не тарґетувати онлайн-рекламу за допомогою профілювання на основі аналізу спеціальних категорій персональних даних (політичні погляди, сексуальна орієнтація або етнічне походження). Це правило впливає на методи залучення цільових аудиторій та майже персоналізовану доставку політичної реклами; однак його впровадження не мало бажаного ефекту. Завдяки механізмам, що їх використовують великі технологічні компанії для моніторингу та вилучення контенту і збору поведінкових даних, навіть за відсутності профілювання на основі аналізу спеціальних категорій даних, тарґетована реклама як така надалі може залишатися дозволеним інструментом (Duivenvoorde і Goanta 2023: 9–10).

Техніки тарґетування та доставки реклами передбачають збір персональних даних, включно з поведінковими (але не чутливими даними), які однак можуть розкривати певні чутливі аспекти користувачів (Becker Castellaro and Penfrat 2022). Крім того, відповідно до DSA, TTPA та Кодексу поведінки щодо протидії дезінформації, винятком із заборони може бути чітко заявлена згода суб'єкта на обробку його персональних даних для цілей політичної реклами (Європейська комісія 2025c).

Низка організацій громадянського суспільства, разом з Європейською радою із захисту даних, Комітетом з питань

внутрішнього ринку та захисту споживачів Європейського парламенту (2023) та студентською спілкою Juneja (2024), рекомендували заборонити методи мікротарґетингу як такі, що використовують особливі категорії чутливих даних для

Вставка 2.6. **Унормування прозорості тарґетингу політичної реклами для забезпечення чесних і прозорих політичних онлайн-кампаній в ЄС**

Спираючись на Статтю 7 (повага до приватного та сімейного життя), Статтю 8 (захист персональних даних) та Статтю 11 (свобода вираження поглядів та доступу до інформації) Хартії, а також на Статтю 2 Договору про Європейський Союз, яка визначає демократію як основоположну цінність ЄС, TTPA має запобігати маніпуляціям, забезпечувати прозорість та захищати цілісність виборів у цифрову епоху (Європейська комісія, без дати).

Відповідно до Статті 16 TFEU, яка гарантує захист персональних даних, та Статті 8 Хартії, яка закріплює право на захист персональних даних, TTPA доповнює GDPR у частині заборони на незаконне використання персональних даних для політичної реклами в Інтернеті. Регламент визначає запобіжні заходи проти використання чутливих даних, зловживання технологіями мікротарґетингу на основі штучного інтелекту та непрозорого алгоритмічного посилення політичних повідомлень.

Крім того, TTPA доповнює DSA через впровадження більш суворих заходів відповідальності для онлайн-платформ та рекламодавців, вимагаючи чіткого позначення, відслідковування та доступності політичної реклами для громадського контролю. Такий регуляторний підхід запобігає надмірному впливу на демократичні процеси, зміцнює цілісність виборчого процесу та підвищує прозорість політичних онлайн-кампаній.

Вимоги та правила TTPA щодо протидії дезінформації, запобігання маніпуляціям свідомістю виборців на основі зібраних приватних даних та забезпечення об'єктивності політичного обговорення в інтернет-просторі практично сприяють захисту демократичних принципів та основоположних прав у цифрову епоху (Rabitsch and Calabrese 2024: 7).

Прозорість та достовірні дані про поширювану політичну рекламу мають вирішальне значення для оцінки відповідальної поведінки онлайн-платформ у протидії дезінформації.

політичних цілей. Ця рекомендація спрямована на зменшення ризиків поляризації, перешкоджання створенню «ехокамер» та поширенню дезінформації методами тарґетування і доставки реклами (Becker Castellaro та Penfrat 2022).

Однак така заборона не була включена ані до DSA, ані до TTPA.

2.4.1. **Прозорість політичної реклами**

Прозорість та достовірні дані про поширювану політичну рекламу мають вирішальне значення для оцінки

відповідальності онлайн-платформ у протидії дезінформації. Певні вимоги прозорості вже передбачені DSA та Кодексом поведінки щодо дезінформації, зокрема зобов'язання позначати політичну рекламу для користувачів, створювати репозиторії реклами, взаємодіяти з організаціями громадянського суспільства, а також забезпечувати доступ до даних платформ для проведення моніторингу і розслідувань (Європейська комісія 2025c).

У європейській правовій системі прозорість політичної реклами в Інтернеті забезпечується низкою нормативних актів, включно з Кодексом поведінки щодо дезінформації, якими визначаються відповідні заходи та зобов'язання суб'єктів правового регулювання з метою надати громадянам можливість легко розпізнавати політичну онлайн-рекламу.

Наразі TTPA є найважливішим правовим джерелом для розуміння заходів прозорості, що їх онлайн-платформи мають впроваджувати для розміщення політичної реклами. Згідно з положеннями Статті 8 TTPA, ідентифікація політичної реклами має включати такі елементи: (a) зміст повідомлення; (b) спонсор повідомлення; (c) мова поширюваного повідомлення; (d) контекст та період поширення повідомлення; (e) засоби, за допомогою яких виробляється, розміщується, просувається, публікується, доставляється або поширюється повідомлення; (f) цільова аудиторія; та (g) мета повідомлення.

Стаття 7 TTPA вимагає від спонсорів (наприклад, політиків або політичних партій) заявляти про політичний характер реклами, а постачальники послуг (як от VLOP або VLOSE) мають запитувати у спонсора всю необхідну для дотримання правових вимог інформацію після такої заяви. Іншими словами, обов'язок заявляти про політичний характер реклами покладається на спонсорів. Однак організації громадянського суспільства попереджають про можливість уникнення зобов'язань щодо прозорості як спонсорами, так і онлайн-платформами, якщо вони просто не зазначать, «що розміщувана ними реклама є політичною» (Calabrese 2024a: 3).

Крім того, TTPA передбачає створення Європейською комісією публічного репозиторію політичної онлайн-реклами, яка поширюється у країнах Європейського Союзу. Вся інформація має бути загальнодоступною на єдиному порталі у машиночитаному форматі. Для забезпечення прозорості, про

кожну подію політичної онлайн-реклами має бути надана така інформація (Стаття 12[1)] TTPA):

a) особа спонсора та, у відповідних випадках, кінцевий бенефіціарний власник спонсора, включно з назвою/іменем, адресами електронної пошти та поштовою адресою (якщо вона оприлюднена), а також адреса реєстрації, якщо спонсором виступає юридична особа;

b) перелічені у параграфі (a) дані про фізичну або юридичну особу, яка сплачує за послуги політичної реклами, якщо ця особа не є зазначеним спонсором або кінцевим бенефіціарним власником спонсора;

c) період публікації, доставки або поширення політичної реклами;

d) сукупна винагорода та сукупна вартість інших благ, отриманих постачальниками послуг з політичної реклами, включно з отриманими видавцем частково або повністю в обмін на надані послуги з публікації політичної реклами, та, у відповідних випадках, за проведення політичної рекламної кампанії;

e) інформація про публічне або приватне походження коштів та інших благ, зазначених у параграфі (d), та чи виникли вони всередині або за межами Союзу;

f) методологія розрахунку ціни та вартості, зазначених у пункті (d);

g) у відповідних випадках — зазначення виборів або референдумів чи то інших законодавчих або регуляторних процесів, з якими пов’язана політична реклама;

h) посилання на офіційну інформацію про умови участі у конкретних виборах або референдумах, якщо політична реклама пов'язана з цими подіями;

i) у відповідних випадках — посилання на європейський репозиторій політичної онлайн-реклами, зазначеній у Статті 13;

j) інформація про застосування механізмів повідомлення про недотримання вимог, зазначені у Статті 15(1);

k) у відповідних випадках, інформація про призупинення або повне припинення поширення раніше опублікованої політичної реклами або її початкової версії через порушення цього Регламенту;

l) у відповідних випадках — заява про те, що для цілей політичної реклами були використані методи тарґетування або доставки реклами з неправомірним використанням персональних даних, включно з інформацією, зазначеною у Статті 19 (1), параграфи (c) та (e);

m) у відповідних випадках та за технічної можливості, дані про охоплення політичною рекламою, включно з кількістю переглядів та взаємодією користувачів.

TTPA визначає конкретні повноваження виборчих органів для забезпечення дотримання вимог. Відповідно до статті 16, OAB («національні компетентні органи») можуть вимагати від постачальників послуг політичної реклами (таких як VLOP та VLOE) надавати їм будь-яку зазначену вище інформацію. Термін виконання цих вимог становить від 2 до 12 днів, залежно від розміру компанії постачальника. В останній місяць перед днем голосування на виборах або референдумі постачальники послуг політичної реклами має надавати запитувану інформацію протягом 48 годин.

Крім того, кожен постачальник послуг політичної реклами, включно з VLOP та VLOE, має призначити контактну особу для взаємодії з компетентними національними органами. Вищезазначені дані також можуть надаватися перевіреним перевіряльникам, організаціям громадянського суспільства, політичним діячам, національним або міжнародним спостерігачам та журналістам.

Кожен постачальник послуг політичної реклами, включно з VLOP та VLOE, має призначити контактну особу для взаємодії з компетентними національними органами.

2.4.2. **Доступ до даних для перевірки згідно з вимогами DSA та TTPA**

DSA дозволяє і встановлює правила перевірки та вивчення даних третіми сторонами (доступ до даних). За визначенням Європейської комісії (2024c), «постійний та надійний доступ до даних для перевірки третіми сторонами має

надзвичайно важливе значення під час проведення виборів для забезпечення прозорості, кращого розуміння та сприяння подальшому розвитку запобіжних заходів щодо пов'язаних з виборами ризиків». Окрім виконання юридичних зобов'язань, визначених Статтею 40 DSA, Комісія рекомендує VLOP та VLOS забезпечити вільний доступ до даних для вивчення ризиків, пов'язаних з виборчими процесами, включно з ретельним аналізом використання моделей штучного інтелекту, візуальних інформаційних панелей та інших додаткових даних.

Доступ до даних забезпечить систему стримувань і противаг у дотриманні онлайн-платформами вимог DSA та TTPA , а відтак попереджатиме поширення неправомірного контенту і дезінформації. Такий доступ дозволяє перевіреним перевіряльникам оцінювати системні ризики для виборчих процесів та вільного громадського обговорення (серед іншого, FIMI, дезінформації та мови ненависті) і розробляти обґрунтовані політики для зменшення цих ризиків в онлайн-середовищі (див. 3.4.1. Роль OAB в оцінюванні та пом'якшенні ризиків у рамках DSA: Зобов'язання належної обачності VLOP та VLOES у виборчих процесах).

Крім того, держави-члени мають призначити національний компетентний орган, відповідальний за ведення загальнодоступних та машиночитаних онлайн-реєстрів усіх зареєстрованих на їхній території юридичних представників, що підпадають під дію TTPA. Кожен національний компетентний орган зобов'язаний забезпечити належну доступність, повноту та регулярне оновлення такої інформації (стаття 22 TTPA). У цій частині TTPA визначає обмежений перелік повноважень компетентних органів, а саме:

a) вимагати доступ до даних, документів та іншої потрібної інформації, зокрема від спонсора або відповідних постачальників послуг політичної реклами; компетентні органи можуть використовувати отриману інформацію винятково для цілей моніторингу та оцінки дотримання Регламенту, відповідно до чинного законодавства про захист персональних даних та конфіденційної інформації;

b) видавати попередження постачальникам послуг політичної реклами щодо недотримання ними передбачених Регламентом зобов'язань;

c) вимагати припинення порушень та напряму звертатися до спонсорів або постачальників послуг політичної реклами з вимогою вжити необхідних заходів для дотримання Регламенту;

d) накладати або вимагати від судового органу накладання штрафів чи то застосування інших фінансових санкцій і заходів, залежно від обставин;

e) за необхідності накладати штрафні санкції на чітко визначений період, або вимагати таких заходів від національного судового органу;

f) за необхідності застосовувати пропорційні порушенню та необхідні для його ефективного припинення заходи, або вимагати таких заходів від національного судового органу;

g) оприлюднювати заяви із зазначенням юридичної та/або фізичної особи (осіб), які порушили встановлені цим Регламентом зобов'язання, з роз'ясненням характеру такого порушення;

h) проводити перевірки або вимагати від судових органів ордеру/ дозволу на проведення перевірок у будь-яких приміщеннях, що використовуються постачальниками послуг з політичної реклами для ведення ними комерційної, підприємницької, господарської або професійної діяльності ; або вимагати таких дій від інших уповноважених державних органів для перевірки, отримання або створення копій і витягів інформації у будь-якій формі, незалежно від носія інформації.

TTPA наголошує на важливості «регулярного обміну інформацією» між призначеними державами-членами національними уповноваженими і усіляко підтримує обмін провідним досвідом та співробітництво між національними органами влади та Європейською Комісією в усіх аспектах впровадження Регламенту. Таке співробітництво передбачає ефективну взаємодію з Європейською мережею співпраці з питань виборів, Європейською групою регуляторів аудіовізуальних медіапослуг та іншими відповідними мережами чи то установами. Крім того, національні органи влади можуть проактивно взаємодіяти з іншими національними

зацікавленими сторонами для підтримки впровадження і дотримання Регламенту TTPA.

Попри важливу ОАВ у взаємодії з онлайн-платформами та надане їм право на запит інформації з репозиторіїв політичної реклами, головним компетентним наглядовим органом, відповідальним за дотримання онлайн-посередниками зобов'язань щодо прозорості політичної реклами, визнається відповідний координатор цифрових послуг або Європейська комісія (залежно від того, чи визначаються платформи як VLOP або VLOE). Крім того, координатор цифрових послуг має забезпечувати належну координацію з країнами-членами для впровадження заходів щодо прозорості на національному рівні.

2.5. **ШТУЧНИЙ ІНТЕЛЕКТ І ЙОГО ВПЛИВ НА ЦІЛІСНІСТЬ ВИБОРІВ**

Акт про штучний інтелект (Європейський Союз 2024d) є горизонтальним регламентом, який поширюється на системи ШІ, розміщені на європейському ринку. Загальний виняток застосовується до систем ШІ, які використовуються для національної безпеки. Основною метою його впровадження є забезпечення безпечного та прозорого використання таких систем з дотриманням основоположних прав людини. Регламент використовує підхід, заснований на ризиках (*risk-based approach*), тобто оцінює і класифікує системи ШІ за рівнем ризику, який вони становлять для суспільства та прав особи.

Акт про ШІ підтримує основоположні цінності ЄС — демократію та повагу до основних прав і свобод (Bogucki et al. 2022). Він також створює нормативно-правову рамку, яка враховує потенційні ризики від використання систем ШІ для цілісності виборів та гарантує, що технологічний прогрес не зашкодить демократичному процесу.

TTPA наголошує на важливості «регулярного обміну інформацією» між призначеними державами-членами національними уповноваженими.

Регламент розрізняє різні категорії пов'язаних із системами ШІ операторів — постачальників, розробників, імпортерів, дистриб'юторів та виробників продукції на основі штучного інтелекту. Виборчі органи можуть підпадати під одну або декілька з цих категорій.

За визначенням Статті 3(3) Акту про ШІ, постачальники — це фізичні або юридичні особи, державні органи, агентства або

Вставка 2.7. **Європейський щит демократії**

У відповідь на зростаючі системні загрози демократичним процесам Європейська комісія представила Європейський щит демократії (EDS) для протидії «змінюваному характеру загроз [європейській] демократії та виборчим процесам (Європейський парламент, 2025). На момент написання цього огляду Європейський щит демократії перебуває на стадії підготовки і мав бути представлений у завершеному вигляді та повному змісті наприкінці листопада 2025 року. Розпочата незадовго до проведення виборів до Європейського парламенту 2024 року, ініціатива EDS стала частиною Плану дій щодо європейської демократії 2020 року (Європейська комісія 2024d) і доповнює його комплексним пакетом заходів захисту, спрямованих на зміцнення демократичної та соціальної стійкості ЄС, з особливим акцентом на інформаційній безпеці та цілісності виборів.

Застосовуючи цілісний підхід, ЄС визначив своїм пріоритетом захист союзної демократії від FIMI та гібридних загроз. Для досягнення поставленої мети EDS передбачає ефективне впровадження і застосування ключових правових інструментів, впроваджених протягом останніх років: DSA, EMFA, Закону про штучний інтелект, Рекомендації CM/Rec(2024)2 державам членам щодо протидії використанню стратегічних позовів проти участі громадськості (SLAPP) та TTPA. Крім того, EDS передбачає активізацію зусиль у галузі цифрової та медійної грамотності, інтегруючи досвід учасників та організацій громадянського суспільства і фахівців з виявлення дезінформації.

У рамках зусиль щодо захисту Європи від іноземного втручання EDS також передбачає більш широку координацію між різними інституціями. Разом із залученням громадянського суспільства і низки національних та європейських органів до формуванні та впровадження EDS, Європейська комісія створила Проєктну групу з питань демократії, очолювану Майклом Макгратом (комісаром з питань демократії, правосуддя, верховенства права та захисту прав споживачів) і Хенною Вірккунен (виконавчою віцепрезиденткою з питань технологічного суверенітету, безпеки та демократії). Проєктна група сприятиме координації та узгодженню зусиль за різними стратегічними напрямками.

18 грудня 2024 року Європейський парламент створив Спеціальний комітет з питань Європейського щита демократії. До повноважень комітету, серед іншого, віднесено оцінку «відповідного чинного й запланованого законодавства та політик з метою виявлення можливих правових прогалин, недоліків та дублювання, що можуть бути використані для зловмисного втручання у демократичні процеси» (Європейський парламент, 2024), розробку рекомендацій та взаємодію з інституціями ЄС й іншими відповідними громадськими та недержавними партнерами.

інші установи, які розробляють системи ШІ самостійно або виступають у ролі замовника, виводять їх на ринок Союзу або вводять в експлуатацію під своїм ім'ям чи то торговою маркою. Деплоєри (або впроваджувачі) — це фізичні або юридичні особи, державні органи, агентства або інші установи,

які керують впровадженням систем ШІ, за винятком випадків, коли використання цих систем відбувається в особистих, непрофесійних цілях.

Акт про ШІ має регуляторний вплив на використання систем ШІ у контексті виборів; і тут основним завданням є сприяння розвитку ШІ як надійного допоміжного інструмента з одночасним захистом демократичних принципів, верховенства права та основоположних прав, як от права голосу та вільної участі у виборах. Актом про ШІ передбачено диференційоване законодавче регулювання використання ШІ залежно від так званої «зони ризику» для здоров'я, безпеки та основоположних прав громадян. Відтак законом визначаються чотири категорії:

1. *Неприйнятний ризик*: Системи ШІ, які створюють явну загрозу важливим суспільним інтересам Союзу, що захищаються чинним законодавством ЄС (наприклад, соціальний скоринг[7] або маніпулятивний ШІ). Зважаючи, що такі системи не можна розробляти, продавати або використовувати у ЄС, вони підпадають під повну заборону згідно зі Статтею 5 Акту про ШІ.
2. *Високий ризик:* Дозволені системи ШІ, до яких застосовується вимога щодо попередньої оцінки відповідності, включно з оцінкою ризиків та заходами для їхнього пом'якшення (Стаття 6 Акту про ШІ).
3. *Обмежений ризик:* Системи ШІ, до яких застосовуються конкретні зобов'язання щодо прозорості (Параграф 53 Акту про ШІ).
4. *Мінімальний ризик*: Системи ШІ, які переважно не підпадають під правове унормування.

У контексті виборів певні системи ШІ заборонені законом, зокрема такі, що використовують підсвідомі маніпуляції для впливу на поведінку людини і можуть заподіяти значної шкоди, а також системи ШІ, які експлуатують уразливості або використовують біометричну категоризацію для визначення, серед іншого, раси, політичних поглядів, релігійних або світоглядних переконань людини.

7 Соціальний скоринг — це вид скорингу, який оцінює особу за її соціальними характеристиками і прогнозує її поведінку за допомогою аналізу присутності у соціальних мережах.

Однак організації громадянського суспільства висловили занепокоєння щодо такого підходу до заборони систем ШІ. Наприклад, Європейське партнерство за демократію стверджує, що «дуже важко довести наявність реального ризику в контексті виборів, оцінити його як «неприйнятний» або «високий» та довести рівень ймовірності заподіяної шкоди» (Calabrese 2024b: 3). Наприклад, системи ШІ, які випадково видають так звані «галюцинації», тобто генерують неправильну або вигадану інформацію, що може вводити в оману користувачів, не підпадають під цю категорію, адже вони не вважаються «маніпулятивними техніками», відтак не підпадають під заборону згідно з Актом про ШІ (Європейська комісія 2025b: 29).

Деякі системи ШІ, які використовуються для адміністрування правосуддя та в інших демократичних процесах, класифікуються як високоризикові. У контексті виборів, Додаток III, пункт 8(b) Акту про ШІ окремо визначає, які системи ШІ підпадають під заборону:

> «Системи ШІ, призначені для впливу на результати виборів чи то референдумів, або на поведінку фізичних осіб під час голосування на виборах і референдумах. Це не стосується тих систем ШІ, на результати роботи яких не мають прямого впливу жодні фізичні особи, як от цифрові інструменти, що використовуються для організації, оптимізації або структурування політичних кампаній з адміністративної та логістичної точки зору».

Звичайно, потенційні ризики згаданих систем не обмежуються викладеним. Наприклад, системи ШІ з техніками мікро тарґетингу та підсилення повідомлень можуть вважатися «призначеними для здійснення впливу на вибори», адже вони використовуються з метою безпосередньо вплинути на результати голосування. Натомість організаційні системи ШІ для реєстрації та ідентифікації виборців, управління списками виборців та прогнозування логістичних виборчих витрат, серед іншого, не підпадають під цю категорію. Знов-таки, у таких випадках критичним елементом для оцінки ризику та потенційно завданої шкоди має бути намір вплинути на людську свідомість (Calabrese 2024b).

Наприклад, чат-боти ОАВ для інформування громадян про вибори потенційно можуть надавати маніпулятивну інформацію, яка впливає на поведінку виборців. Однак ці чатботи будуть класифіковані радше як організаційні системи, відтак не

підлягатимуть оцінюванню ризиків та, відповідно, вимогам щодо впровадження заходів для пом'якшення ризиків або ж реєстрації у публічній базі даних ЄС.

Проте, якщо такі системи створюються з визначеною метою вплинути на вибори або референдум, або на поведінку виборців (наприклад, за допомогою мікро тарґетнгу цільових груп та технік посилення впливу) і використовуються органами публічного права або приватними суб'єктами, які надають публічні послуги, вони мають пройти процедуру оцінки потенційного впливу на основоположні права громадян. Однак у разі з державними органами та залученими до надання публічних послуг суб'єктами, процес оцінки не передбачає консультацій із зовнішніми зацікавленими сторонами.

Деплоєри та користувачі систем, які генерують або редагують зображення, аудіо- або відеоконтент (наприклад, створюють дипфейки), завжди мають чітко зазначати, що контент є штучним або підробленим.

З іншого боку, Актом про ШІ унормовується синтетичний аудіо-, відео- та текстовий контент, створений за допомогою ШІ. Правила вимагають від систем, які генерують подібний контент, обов'язкового машинозчитуваного позначення такого контенту як штучно згенерованого або перероблено. Користувачі систем, які генерують або редагують зображення, аудіо- або відеоконтент (наприклад, створюють дипфейки), завжди мають чітко зазначати, що контент є штучним або підробленим. Іншими словами, згенерований ШІ контент завжди має бути позначений як такий.

Акт не містить прямої згадки про дипфейки або гендерно обумовлені нападки на жінок-політикинь у контексті виборів. Тут найбільш відповідну правову базу для захисту від контенту, створеного за допомогою штучного інтелекту і спрямованого на підбурювання до гендерного насильства, забезпечує Директива ЄС про протидію насильству щодо жінок та домашньому насильству (Європейський Союз 2024c) (див. 2.3.2: Модерація контенту для протидії гендерному насильству в Інтернеті).

Розділ 3

ПРОБЛЕМНІ ПИТАННЯ ПРАВОЗАСТОСУВАННЯ І РЕАЛІЗАЦІЇ ЧИННОЇ НОРМАТИВНО-ПРАВОВОЇ БАЗИ ЄС У СФЕРІ ЦИФРОВІЗАЦІЇ

Як зазначалося у попередньому розділі, acquis ЄС у сфері цифровізації є однією з найамбітніших світових ініціатив із створення комплексної правової екосистеми для унормування цифрових послуг, захисту даних та онлайн-контенту. Центральним елементом цієї системи є узгоджена архітектура правозастосування для забезпечення належного нагляду на рівні ЄС та значною мірою на рівні держав-членів через гармонізацію національного законодавства.

Цей розділ буде присвячений аналізу та роз'ясненню проблемних питань цієї нової архітектури, зокрема в частині правозастосування та взаємодії між національними та союзними органами влади у контексті виборів. Сподіваємося, це допоможе політикам та органам спостереження за виборами краще розуміти вимоги щодо належного дотримання встановлених регламентів та відповідних стратегій правозастосування.

Окремо будуть розглянуті проблеми з реалізацією низки правових норм та координацією зусиль, особливо важливих у контексті виборів. У розділі представлені практичні висновки та конкретні рекомендації, зроблені на основі вивчення досвіду європейських виборчих комісій. Нарешті, тут наведені приклади міжвідомчої і транснаціональної координації, ефективних практик та типових перешкод, що виникають у процесі впровадження і забезпечення належного дотримання регламентів під час проведення виборів.

3.1. ВПРОВАДЖЕННЯ ЗАХОДІВ ДЛЯ ЗАХИСТУ ДАНИХ У КОНТЕКСТІ ВИБОРІВ

GDPR по суті запропонував проміжну модель правозастосування, побудовану за горизонтальним принципом, що створило виклики для належного впровадження регламенту на рівні усіх країн-членів, тож винесені уроки наразі впливають на подальше удосконалення норм та правил ЄС у сфері цифровізації.

Правозастосування GDPR здебільшого покладається на національні наглядові органи, більше відомі як органи із захисту даних, які здійснюють контроль та нагляд за безпосередніми так званими «контролерами», що збирають і обробляють дані у межах своєї юрисдикції. Крім того, ці органи уповноважені розслідувати та притягати до відповідальності за порушення норм GDPR, включно з тими, що трапляються у виборчому контексті (Європейська комісія, без дати).

3.1.1. Європейська рада із захисту даних та Європейський інспектор із захисту даних

На рівні ЄС існує низка важливих механізмів, які забезпечують єдині стандарти захисту даних як на союзному рівні, так і на рівні держав-членів. Європейська рада із захисту даних (EDPB), до складу якої входять керівники відповідних національних органів із захисту даних, та Європейський інспектор із захисту даних мають власну правосуб'єктність і відповідають за забезпечення послідовного правозастосування GDPR та Директиви про захист даних у всій Європі (стаття 68 GDPR). Вони також забезпечують взаємодію між союзними та національними органами, зокрема щодо забезпечення дотримання GDPR.

EDPB видає загальні настанови, формулює керівні принципи, пропонує рекомендації та кращі практики для гармонізації національних законодавств із чинною правовою базою ЄС про захист даних (Європейська рада з захисту даних, без дати). Наприклад, у березні 2019 року EDPB опублікувала Заяву 2/2019 про використання персональних даних у політичних кампаніях, наголосивши, що дотримання GDPR має вирішальне значення для цілісності демократичного процесу, зважаючи на дедалі ширше використання політичними партіями персональних даних та технік профілювання у сучасних виборах (Європейська рада з захисту даних 2019). EDPB також реагує на конкретні проблеми, як от на суперечливий план Польщі щодо винятково поштового

голосування у 2020 році (Wanat 2020). Європейська рада із захисту даних оприлюднила лист, у якому наголосила, що будь-яке передавання або обробка даних виборців може відбуватися лише на надійних правових засадах, і будь-які рішення мають відповідати вимогам GDPR щодо безпеки та прозорості; окремо наголошувалося, що будь-які пов'язані з виборами надзвичайні заходи не можуть переважати над основними принципами захисту даних (Європейська рада з захисту даних 2020a).

Якщо національні вибори не входять до сфери компетенції Європейського інспектора із захисту даних, то під час проведення виборів до Європейського парламенту саме він здійснював нагляд за захистом даних у виборчому процесі. Яскравим прикладом стало розслідування щодо залучення послуг американської компанії NationBuilde для реалізації мотиваційно-просвітницької кампанії для виборців на сайті Європейського парламенту в 2019 році. Європейський інспектор із захисту даних визнав, що Парламент не забезпечив дотримання вимог (зокрема щодо прозорості та гарантій передавання даних третій стороні), і виніс своє перше в історії зауваження центральному органу ЄС. Усі дані, зібрані через вебсайт компанії, були згодом перенесені на власні сервери Парламенту, а Європейський інспектор із захисту даних домігся від інституцій ЄС зобов'язання надалі «бути зразковим прикладом» у захисті персональних даних під час виборів (Європейський інспектор з захисту даних, 2020).

Однак, зважаючи на транскордонний характер обробки даних, цей процес вимагає одночасного дотримання вимог різними державами-членами, відтак особливого значення набуває взаємодія між низкою відповідних національних органів (Mustert 2023). Тому GDPR передбачає механізм для координації дій національних органів із захисту даних, що дозволяє їм узгоджувати процедури правозастосування у транскордонних випадках (Mustert 2023). За необхідності Європейська рада із захисту даних може втрутитися для вирішення суперечок між залученими національними органами, і винесене нею рішення є обов'язковими до виконання (стаття 65 GDPR).

Зважаючи на транскордонний характер обробки даних, цей процес вимагає одночасного дотримання вимог різними державами-членами, відтак особливого значення набуває взаємодія між низкою відповідних національних органів.

У сучасних виборчих кампаніях часто використовуються онлайн-платформи (як от соціальні та рекламні мережі) з іноземною або міжнародною юрисдикцією. Для таких випадків застосовується «механізм єдиного вікна» GDPR для призначення провідного органу з питань захисту даних (наприклад, Комісії з питань захисту даних Ірландії для Facebook) для проведення

відповідного розслідування (Європейська рада з питань захисту даних n.d.b). Однак у разі якщо очікування на рішення провідного органу може поставити під загрозу проведення виборів, чинні органи із питань захисту даних можуть самостійно вживати термінових заходів для усунення порушень. Наприклад, під час загальних виборів в Італії у 2022 році національний орган (Garante) застосував положення Статті 66 GDPR, зобов'язавши Meta (Facebook) призупинити роботу нової системної функції для залучення виборців, доки не будуть вирішені усі питання щодо законності та прозорості. Garante координувала свої дії з Ірландською комісією із захисту даних, однак не отримала вчасно задовільних відповідей, тож самостійно винесла офіційне попередження та наклала тимчасову заборону на використання цієї системної функції в Італії (GDPR Hub 2023).

Підсумовуючи, можна сказати, що під час виборів саме національні органи із захисту даних тримають лідерство у правозастосуванні, вдаючись до розслідування порушень та застосування санкцій у межах своєї юрисдикції. На рівні ЄС Європейська комісія, Європейська рада із захисту даних та Європейський інспектор із захисту даних надають роз'яснення та рекомендації, сприяють взаємодії та можуть втручатися у конкретні транскордонні або інституційні справи.

3.2. **ВИКЛИКИ ТРАНСКОРДОННОЇ КООРДИНАЦІЇ**

Комплексний механізм забезпечення дотримання законодавства — зокрема необхідність багаторівневої транскордонної координації — зазнає критики через свою процедурну складність, яка створює значні виклики у практичному застосуванні (Gentile and Lynskey 2022; Mustert 2023; Mildebrath 2024). У Статтях 57 та 58 GDPR визначається стандартизований перелік завдань і повноважень для наглядових органів, водночас залишаючи невизначеними численні процедурні кроки, що мають ухвалюватись на національному рівні. Така дискретність призвела до непослідовності практик правозастосування у державах-членах ЄС, зокрема щодо здійснення офіційних розслідувань, їхнього обсягу та суворості вжитих коригувальних заходів (Gentile and Lynskey 2022; Mustert 2023).

Процедурна фрагментованість ускладнює окреслення чітких меж між прийнятними національними відмінностями та практиками, підриваючи принципи ЄС щодо ефективності, пропорційності та стримувального характеру вжитих заходів. Наприклад, національні правила з обмеженими строками подання скарги або стратегії накладання штрафів, значно більших за максимально передбачені у GDPR, створюють практичні перешкоди для ефективної реалізації прав суб'єктами даних (Gentile and Lynskey 2022: 806–07; Mustert 2023).

Іншим структурним недоліком, притаманним архітектурі правозастосування GDPR, є побудована за горизонтальним принципом децентралізована система, що може ускладнювати транскордонну співпрацю та створювати конфлікти і суттєві затримки у прийнятті рішень (Gentile and Lynskey 2022: 800). Саме цей недолік може звести забезпечення дотримання Регламенту до загального мінімального стандарту. Крім того, інституційні дисбаланси — коли головний наглядовий орган може чинити непропорційний вплив на результати розгляду справ — можуть послабити авторитет інших зацікавлених органів (Gentile and Lynskey 2022: 809, 811).

Іншим структурним недоліком, притаманним архітектурі правозастосування GDPR, є побудована за горизонтальним принципом децентралізована система.

Процедурна неузгодженість також негативно впливає на вертикальну співпрацю з Європейською радою із захисту даних (EDPB), яка не має незалежних повноважень для проведення розслідувань і покладається винятково на національні наглядові органи для отримання вичерпної та своєчасної інформації по справах. Невчасно надана або неповна інформація від національних органів часто підриває механізм вирішення спорів самої EDPB, що лише подовжує затримки та збільшує невідповідність у результатах правозастосування (Gentile and Lynskey 2022; Mustert 2023).

Європейська парламентська служба з проведення розслідувань також визначає процедурну неузгодженість та недостатню чіткість як критичну проблему, що перешкоджає ефективному застосуванню GDPR. Неоднозначні процедурні правила можуть посилити розбіжності у поглядах різних наглядових органів і перешкоджати швидкому винесенню єдиного узгодженого рішення у транскордонних справах. Відтак служба рекомендувала провести необхідні реформи для уточнення процедурних зобов'язань, посилення ролі відповідних органів та забезпечення послідовних і своєчасних рішень для належного правозастосування в усіх державах-членах (Mildebrath 2024).

Науковці та практики також закликають до подальшої гармонізації певних процедурних аспектів. Рекомендовані заходи включають стандартизацію критеріїв прийнятності скарг, обов'язкове ухвалення юридично зобов'язуючих рішень за результатами розгляду скарг, які надалі можуть бути оскаржені у судовому порядку, а також уточнення обов'язків щодо взаємодії (зокрема, своєчасного обміну вичерпною інформацією) та досягнення попереднього консенсусу стосовно обсягу розслідування і постійного інформування про перебіг справи (див., наприклад, Mustert 2023).

Відповідно до GDPR, виборчі органи (переважно це державні установи) зазвичай визнаються «контролерами» даних, відтак несуть повну відповідальність за дотримання відповідних правових вимог.

3.3. **ОБРОБКА ДАНИХ ОРГАНАМИ АДМІНІСТРУВАННЯ ВИБОРІВ (ОАВ)**

Як зазначалося раніше, ОАВ — незалежні виборчі комісії, національні міністерства або місцеві органи влади — відповідають за обробку основних виборчих даних, головним чином за реєстрацію виборців та пов'язані з цим процеси. Відтак, згідно з GDPR, виборчі органи (які зазвичай є державними установами) визнаються «контролерами» даних і несуть повну відповідальність за дотримання відповідних правових вимог.

3.4. **РОЛЬ ОАВ У ЗАБЕЗПЕЧЕННІ ДОТРИМАННЯ РЕГЛАМЕНТУ DSA ТА У МІЖВІДОМЧІЙ КООРДИНАЦІЇ**

DSA використовує дворівневий механізм правозастосування — як на національному рівні, так на рівні ЄС. Відтак запроваджується модель «багаторівневої відповідальності» з розподілом обов'язків між національними органами влади та органами на рівні ЄС, залежно від розміру постачальників та впливу цифрових послуг. На практиці це означає, що повсякденний нагляд за діяльністю більшості онлайн-посередників здійснюється регуляторними органами, тобто координаторами цифрових послуг у кожній окремій державі-члені, а найбільші платформи — VLOP та VLOE — безпосередньо контролює Європейська комісія. Такий дворівневий підхід вимагає тісної координації між національними регуляторними органами та Комісією, особливо під час проведення виборів,

Таблиця 3.1. **Основні зобов'язання та їхні наслідки для ОАВ**

Принципи та правила GDPR	**Обов'язки та повноваження ОАВ**
Стаття 5(1)(a) та (b): Принципи законності та обмеження цілі використання даних	Зазвичай за виборчим законодавством ОАВ обробляють дані виборців відповідно до юридичного зобов'язання або в інтересах суспільства. GDPR наголошує, що зібрані для адміністрування виборів дані не можуть бути використаними для інших цілей, несумісних з першочерговим призначенням. Попереджувальний приклад стався у Бельгії, де один з мерів скористався доступом до даних громадян (зібраних для адміністративних цілей) для розповсюдження листів виборцям у ході своєї виборчої кампанії, і був визнаний винним у порушенні принципу GDPR щодо обмеження цілей використання персональних даних. Тож у 2019 році орган із захисту даних Бельгії наклав на посадовця перший штраф за порушення GDPR, чітко давши зрозуміти, що навіть обрані державні посадовці не мають права повторно використовувати дані виборців для ведення виборчої кампанії без належних правових підстав (Hunton 2019). ОАВ мають забезпечити, що будь-яке використання інформації про виборців суворо відповідає виборчим цілям (наприклад, для повідомлень про виборчі дільниці або для розсилки бюлетенів) і не використовується для отримання переваг у виборчих кампаніях.
Стаття 5(1)(a): Принцип прозорості Статті 13 та 14: Право суб'єкта бути поінформованим про використання його персональних даних	ОАВ зобов'язані інформувати виборців про те, яким чином будуть використані їхні персональні дані у виборчому процесі. Зазвичай виборче законодавство або угода про конфіденційність містять інформацію про те, які дані відображені у виборчому списку, хто має до них доступ і як довго вони будуть зберігатися. Виборці мають право на доступ до своїх персональних даних та вимагати необхідних виправлень (що є надзвичайно важливим для усунення помилок у реєстрі виборців). У деяких випадках виборці можуть відмовитися передавати певну інформацію іншим суб'єктам. Наприклад, у Німеччині громадяни можуть заперечувати проти передавання їхніх адрес політичним партіям для цілей виборчої кампанії (розділ 50, параграф 5, речення 2 Федерального закону про реєстрацію та розділ 36, параграф 2, речення 2 Федерального закону про реєстрацію). Тут органи із захисту даних наголошують на критичній необхідності чіткого роз'яснення цілей використання. Так, у Франції Національна комісія з інформаційних технологій та громадянських свобод у 2024 році оштрафувала одну з політичних асоціацій на 20 000 євро за неналежне інформування про використання персональних даних для політичної агітації (CNIL 2025). Відтак виборчі органи мають постійно нагадувати виборцям про забезпечення конфіденційності персональних даних, з одного боку, і заперечувати проти використання даних виборців для інших цілей — з іншого. Наприклад, виборець може відмовитися від оприлюднення його даних з публічних реєстрів чи то від внесення до списку агітаційних розсилок.

Таблиця 3.1. **Основні зобов'язання та їхні наслідки для ОАВ (cont.)**

Принципи та правила GDPR	Обов'язки та повноваження ОАВ
Стаття 5(1)(f): Принцип безпеки даних Стаття 5(a)(d): Принцип надійності даних Стаття 5(1)(d): Принцип підзвітності Стаття 33: Повідомлення про персональні дані наглядовому органу Стаття 34: Оповіщення суб'єкта даних про порушення безпеки його персональних даних	Захист конфіденційності та цілісності даних виборців має критичну вагу. ОАВ мають вживати відповідних заходів безпеки (контроль доступу, шифрування цифрових баз даних, безпечне зберігання паперових документів) для запобігання несанкціонованому доступу або витоку інформації. Будь-яке порушення цілісності даних у виборчому реєстрі (наприклад, витік списку виборців або злам виборчої IT-системи), може підірвати довіру громадськості і навіть вплинути на цілісність виборів як таких. У подібних випадках застосовуються правила GDPR щодо повідомлення про порушення: виборча комісія має негайно повідомити орган із захисту даних (і, можливо, виборців, яких це стосується), якщо виявлене порушення створює певні ризики (Стаття 33 GDPR). Європейський суд у справі C-340/21[1] роз'яснив, що навіть у разі, коли порушення спричинено технічною помилкою або зовнішньою атакою, контролери можуть бути притягнуті до відповідальності за незабезпечення належних заходів безпеки. Це рішення лише підкреслює важливість підзвітності та управління ризиками з боку державних органів, включно з ОАВ.
Стаття 5(2): Принцип підзвітності Стаття 24: Відповідальність контролера та обробника Статті 35 та 36: Оцінка впливу на захист даних та попередні консультації Стаття 25: Захист даних за замовчуванням та на етапі проєктування	ОАВ мають проводити оцінку впливу нових виборчих технологій (наприклад, систем електронного голосування, біометричних посвідчень виборців) на захист даних, аби завчасно виявити та зменшити потенційні ризики. Результати оцінювання мають бути представлені у зрозумілій та доступній формі, аби суб'єкти даних мали можливість повною мірою реалізувати свої права, визначені GDPR. Захист прав громадян вимагає впровадження відповідних технічних та організаційних заходів (див. Статті 26 та 28 GDPR). Згідно з регламентом GDPR, ОАВ також мають постійно розвивати інституційну та технічну експертизу для забезпечення захисту даних за замовчуванням при впровадженні нових виборчих технологій. ОАВ також мають призначити відповідального за захист даних (це обов'язкова вимога, адже ОАВ є державним органом) для нагляду за належним дотриманням вимог та забезпечення зв'язку з головним органом із захисту даних (стаття 37 [1][a] GDPR).

1 Справа C-340/21, *VB проти Національного податкового агентства* ECLI:EU:C:2023:986.

Таблиця 3.1. **Основні зобов'язання та їхні наслідки для ОАВ (cont.)**

Принципи та правила GDPR	Обов'язки та повноваження ОАВ
Стаття 5(2): Принцип підзвітності Стаття 26: Спільний контролер Стаття 24: Відповідальність контролера та обробника Стаття 29: Обробка даних контролером або відповідальним користувачем під наглядом контролера	ОАВ часто передають на аутсорсинг певні завдання, як от друк бюлетенів або виборчих карток, обслуговування ІТ-інфраструктури або надання поштових послуг. Згідно з Регламентом, будь-який постачальник, що обробляє особисті дані виборців від імені ОАВ, має підписати юридично зобов'язальну угоду про обробку даних і діяти виключно за вказівками виборчого органу (стаття 28[3] GDPR). Важливість цієї вимоги можна зрозуміти на прикладі спроби Польщі організувати голосування поштою у 2020 році. Уряд доручив національній поштовій службі (третій стороні) розіслати бюлетені усім виборцям, для чого намагався отримати дані про виборців від місцевих муніципалітетів. Багато мерів відмовилися надати такі дані, посилаючись на відсутність правових підстав та недостатній рівень безпеки (запит надійшов у вигляді непідписаного електронного листа з проханням надати незашифровані файли з даними про громадян) (Wanat 2020). Так само, якщо ОАВ залучає ІТ-компанію, має бути здійснена перевірка протоколів і практик безпеки постачальника. Будь-яке неналежне поводження з даними підрядником може призвести до відповідальності ОАВ як уповноваженого контролера, а будь-яке відхилення від Регламенту може стати приводом для розслідування з боку органу із захисту даних.

коли дезінформація або незаконний контент в Інтернеті можуть загрожувати демократичним процесам.

Для забезпечення координації та узгодженості у цій дворівневій системі DSA також створює новий орган — очолювану Європейською комісією Європейську раду з цифрових послуг, до складу якої входять представники національних регуляторних органів (координатори цифрових послуг). Рада була створена як незалежна консультативна група, що об'єднує усіх національних координаторів цифрових послуг (по одному представнику від кожної держави-члена) з Європейською Комісією і забезпечує колективні зусилля в інтересах ЄС. Вона створена за моделлю Європейської ради із захисту даних (EDPB) і так само координує зусилля різних країн для правозастосування узгодженого законодавства на єдиному ринку Союзу.

3.4.1. **Роль ОАВ в оцінюванні та пом'якшенні ризиків у рамках DSA: зобов'язання належної обачності VLOP та VLOE у виборчих процесах**

Як зазначається у Статті 34 DSA, одним із найважливіших зобов'язань VLOP та VLOE є ретельне виявлення, аналіз

та оцінка будь-яких системних ризиків, що виникають у результаті проєктування або надання ними послуг, включно з алгоритмічними системами.

Аби допомогти VLOP та VLOE сумлінно виконувати це зобов'язання, 26 березня 2024 року Європейська комісія опублікувала керівні принципи, спрямовані на зменшення системних онлайн-ризиків, які впливають на вибори, відповідно до регламенту DSA (Європейська комісія 2024b). Ці настанови рекомендують VLOP та VLOE усувати ризики для цілісності виборів шляхом сприяння прозорості політичної реклами, протидії дезінформації та створеному ШІ контенту, а також посилювати співпрацю з відповідними органами влади для забезпечення виконання Регламенту з одночасним захистом свободи вираження поглядів (Європейська комісія 2024b).

Керівні принципи пропонують заходи, що охоплюють повний виборчий цикл — передвиборчий, виборчий та післявиборчий періоди — і застосовуються на місцевому, регіональному, національному та європейському рівнях. У керівних принципах наголошується на таких системних ризиках, як FIMI, поширення контенту для підживлення екстремізму та радикалізації, а також маніпулятивного контенту, створеного за допомогою інструментів штучного інтелекту (наприклад, дипфейків). Цей перелік не є вичерпним, і ОАВ разом з іншими органами влади можуть визначати інші системні ризики для цілісності виборів.

VLOP та VLOES мають створити «спеціалізовані внутрішні команди з чітко визначеними завданнями», які взаємодіятимуть з ОАВ для зміцнення демократичних виборчих процесів на місцевому, регіональному та національному рівнях.

Європейська Комісія також закликає до посилення внутрішніх процесів контролю під час проведення виборів, водночас наголошуючи на необхідності поширення корисної інформації для учасників виборів. Тому VLOP та VLOE мають збирати і висвітлювати важливу для виборчих процесів інформацію: програми, події чи то заяви політичних партій; офіційну інформацію про вибори від ОАВ, зокрема з роз'ясненням процедури голосування та ключових правових аспектів; та посилання на офіційні канали комунікації. Крім того, VLOP та VLOE заохочуються до збору контекстної інформації та аналізу ризиків на національному, регіональному та місцевому рівнях з урахуванням конкретних умов проведення виборів (Європейська комісія 2024b). Відтак VLOP та VLOSE мають створити «спеціалізовані внутрішні команди з чітко визначеними завданнями» (Європейська комісія 2024b), які взаємодіятимуть з ОАВ для зміцненням демократичних виборчих процесів на місцевому, регіональному та національному рівнях.

Комісія також закликає до впровадження Кодексу практик щодо дезінформації (механізм внутрішнього регулювання, оновлений у 2022 році на основі рекомендацій Європейської комісії, а у 2025-му інтегрований до Акту про цифрові послуги (DSA) як Кодекс поведінки щодо дезінформації, Європейська Комісія 2025d) та інших відповідних галузевих кодексів ЄС, як от Кодексу поведінки щодо протидії забороненій мові ненависті в Інтернеті, кращих практик у рамках Незалежної від контенту системи забезпечення цілісності виборів для онлайн-платформ, а також рекомендацій організацій громадянського суспільства та інших зацікавлених сторін. Керівні принципи, серед інших, передбачають такі заходи: (a) ініціативи з медіаграмотності; (b) фактчекінг; (c) позначення акаунтів та контенту, створеного за допомогою штучного інтелекту; (d) позначення офіційних акаунтів; і (e) допоміжні інструменти та інформація для користувачів для оцінювання надійності джерел інформації (Європейська комісія 2024b).

Комісія також наголошує на важливості взаємодії та структурованого діалогу між національними органами влади, включно з ОАВ та координаторами цифрових послуг, наприклад, через забезпечення регулярних каналів комунікації між зацікавленими сторонами, розробку механізмів реагування на інциденти та створення робочих груп для координації зусиль ключових зацікавлених сторін у виборчому процесі.

Європейська Комісія підкреслює важливість співпраці та структурованого діалогу між національними органами влади, включно з ОАВ та координаторами цифрових послуг.

3.4.2. **Кодекс поведінки щодо дезінформації як зобов'язання належної обачності для виявлення та пом'якшення системних ризиків у громадському дискурсі та виборчих процесах**

Як згадувалося раніше, VLOP та VLOE зобов'язані проводити оцінювання для виявлення та пом'якшення системних ризиків на своїх платформах, включно з поширенням дезінформації. Аби допомогти їм сумлінно виконувати це зобов'язання, Європейська рада з цифрових послуг інтегрувала добровільний Кодекс практик щодо дезінформації до Акту про цифрові послуги (DSA). Інакше кажучи, Кодекс практик став еталоном дотримання вимог DSA у виявленні та зменшенні системних ризиків дезінформації.

Кодекс забезпечує структуровану базу з більш детальними та технічними рекомендаціями, включно з конкретними кількісними та якісними ключовими індикаторами ефективності, які можуть бути використані платформами для протидії поширенню і впливу дезінформації. Підписанти Кодексу

погоджуються впроваджувати низку заходів для пом'якшення ризиків, як от демонетизація джерел дезінформації, забезпечення прозорості політичної реклами, підтримка цілісності послуг та розширення можливостей користувачів і фактчекерів.

Кодекс поведінки розглядає дезінформацію у виборчі періоди як один з ключових викликів, однак ОАВ відведено мінімальну роль у забезпеченні впровадження та дотримання кодексу як такого. Однак певні його положення можуть перетинатися з інтересами та компетенціями виборчих органів. До прикладу, у рамках «зобов'язань громадянського суспільства» підписанти мають посилити нагляд за політичною рекламою в Інтернеті, вживати спільну термінологію стосовно маніпулятивних дій та практик , а також надавати докази щодо використання недоброчесних тактик, технік і процедур. Та попри це перетинання, ОАВ не відведено офіційної ролі у рамках кодексу.

Однак виборчі органи можуть певним чином впливати на рішення Постійної робочої групи з питань Кодексу — головного органу, відповідального за моніторинг виконання його положень (Зобов'язання 37). Наприклад, для протидії поширенню дезінформації в Інтернеті робоча група має залучати «до [своєї] діяльності відповідних експертів … та … [організовувати] обмін інформацією з третіми сторонами, інформувати їх про останні події та збирати відомості, пов'язані з дезінформацією як явищем» (Європейська комісія 2025c). Кодекс також закликає підписантів «співпрацювати та координувати свою роботу в особливих ситуаціях, як от вибори або кризи» (Захід 37.2). Відтак виборчі органи можуть виступати за свою участь у таких обговореннях або ж пропонувати спільні заходи з Європейською мережею співпраці з питань виборів, прагнучи більш активної ролі та використання набутого досвіду у виборчих питаннях.

3.4.3. **Можливості правозастосування для виборчих органів у рамках DSA**

Попри те що Актом про цифрові послуги перш за все унормовується діяльність онлайн-посередників, він також створює потенційні нові ролі та обов'язки для ОАВ у сфері нагляду за політичними кампаніями в Інтернеті. ОАВ можуть адаптувати свої правові та операційні практики у спосіб, що дозволить їм скористатися механізмами DSA для ефективної боротьби з дезінформацією та мовою ворожнечі в Інтернеті.

Таблиця 3.2. **Основні положення DSA та їхня вага для ОАВ**

Норма DSA	Зобов'язання/роль ОАВ
Стаття 9: Розпорядження про видалення незаконного контенту	ОАВ може видавати розпорядження про видалення контенту лише у разі отримання відповідних повноважень як компетентного органу у межах національної юрисдикції. Наприклад, якщо виборче законодавство надає ОАВ повноваження вимагати видалення незаконних онлайн-матеріалів про вибори, відповідно ОАВ може вчиняти такі дії також на підставі Статті 9 DSA. В іншому випадку ОАВ не може дискретно видавати обов'язкові розпорядження і має передати справу до відповідного органу (наприклад, до суду або іншого регуляторного органу з відповідними повноваженнями).
Стаття 10: Розпорядження про надання інформації	ОАВ може видати розпорядження про розкриття даних лише у разі отримання відповідних повноважень як компетентного органу в межах національної юрисдикції (наприклад, для виявлення джерела неправомірного агітаційного контенту). За відсутності таких законних повноважень ОАВ не може вимагати від платформи розкриття інформації; натомість у таких випадках ОАВ має координувати свої дії з правоохоронними органами або іншим уповноваженим органом.
Статті 11–13: Уповноважені представники та прямі канали комунікації	DSA вимагає від усіх онлайн-платформ призначити уповноваженого представника у ЄС, який буде офіційною контактною особою для взаємодії з органами влади. Ця вимога значно допомагає виборчим органам, адже забезпечує єдиний офіційний канал комунікації з кожною платформою під час проведення виборів для обміну повідомленнями з нагальних питань або ж для надсилання офіційних розпоряджень. На практиці ОАВ мають підтримувати актуальні списки контактів з уповноваженими представниками основних платформ і розробляти процедуру комунікації (особливо у виборчий період), аби забезпечити вчасний обмін повідомленнями та виконання виданих розпоряджень. Ця нова оперативна норма DSA вимагає відходу від переважно кризового електронного спілкування до більш структурованої та постійної комунікації для ефективної взаємодії.

Таблиця 3.2. **Основні положення DSA та їхня вага для OAB (cont.)**

Норма DSA	Зобов'язання/роль OAB
Стаття 22: Довірені флагери (повідомлювачі)	ЗМІ (або пов'язані з ними організації) можуть подати заявку на отримання статусу «довіреного флагера» щодо неправомірного контенту, пов'язаного з виборами, а в окремих випадках — для контенту, що порушує умови використання онлайн-платформ. Статус довіреного флагера надається національним координатором цифрових послуг; для платформ це означає, що повідомлення від таких ЗМІ про певний контент вимагає пріоритетного реагування. Для отримання такого статусу ЗМІ повинні мати належний досвід, бути незалежними і дотримуватися стандартів надійності та об'єктивності. Команда модераторів акредитованого ЗМІ зможе швидко позначати, скажімо, дописи про залякування виборців або незаконно розміщену платну рекламу, на що платформа має без зайвої затримки «відреагувати та прийняти рішення». Довірені флагери можуть суттєво допомогти OAB у протидії шкідливому контенту без офіційних розпоряджень. Однак це не звільняє виборчі органи від обов'язку відповідально позначати неправомірний контент і видавати розпорядження з достатніми доказами та належним юридичним обґрунтуванням. Потенційно OAB мають змогу долучатися до вироблення політик щодо модерації контенту на онлайн-платформах (як от Facebook, X, YouTube тощо) через позначення неправомірного контенту та звернення із скаргами до національного координатора цифрових послуг. Нарешті, онлайн-платформи набувають зобов'язань інформувати відповідні органи правопорядку в разі підозри про вчинення серйозних кримінальних правопорушень, які становлять загрозу безпеці окремих осіб (наприклад, через прояви гендерно зумовленого насильства в Інтернеті).
Стаття 34: Системна оцінка ризиків (для виборів)	VLOP мають оцінювати «будь-які фактичні або передбачувані негативні наслідки для громадського обговорення та виборчих процесів» на своїх ресурсах. Хоча це зобов'язання покладається безпосередньо на платформи, OAB можуть відігравати проактивну роль у належному інформуванні та оцінюванні пов'язаних з виборами ризиків. Так, вони можуть повідомляти як платформам, так і координаторам цифрових послуг про специфічні місцеві чинники ризику для виборів (наприклад, відомі схеми поширення дезінформації або виявлені у минулому тактики зовнішнього втручання). Вони також можуть відігравати активну роль у взаємодії з незалежними аудиторами платформ або аналогічними регуляторними органами і надавати експертні роз'яснення щодо впливів алгоритмів або окремих видів послуг на національні вибори. По суті, OAB виступають зацікавленою стороною у процесі оцінки ризиків, допомагаючи платформам визначати пов'язані з виборами виклики (як от пропаганда з використанням дипфейків або мікро тарґетинг для демотивації виборців від участі у голосуванні).

Таблиця 3.2. **Основні положення DSA та їхня вага для OAB (cont.)**

Норма DSA	Зобов'язання/роль OAB
Стаття 36: Механізм реагування на кризові ситуації	У виняткових випадках (наприклад, за виникнення безпекової кризи, що впливає на вибори) Європейська комісія може оголосити про застосування кризових норм DSA і вимагати від платформ вжити надзвичайних заходів протягом певного часового періоду. Наприклад, якщо цілісність виборчого процесу в одній із держав-членів була підірвана раптовою масованою дезінформаційною атакою ззовні, такий інцидент може вимагати застосування Статті 36. У подібних сценаріях AOB можуть вдатися до більш тісної координації своїх дій з Європейською комісією та координатором цифрових послуг, вчасно надаючи докази та допомагаючи з рішеннями про необхідні тимчасові заходи (як от швидке видалення конкретного контенту або введення алгоритмічних обмежень), а також широко інформуючи громадськість про наслідки таких заходів (наприклад, якщо на час вирішення надзвичайної ситуації певні функції платформи будуть обмежені). Цей протокол дій не є рутинною процедурою, однак OAB мають бути готовими до подібних надзвичайних ситуацій і розробляти власні плани кризової комунікації у координації з відповідними європейськими установами та онлайн-платформами.
Стаття 40: Доступ до даних для розслідувачів	Попри те, що Стаття 40 надає повноваження перевіреним розслідувачам, а не OAB, вона створює опосередковані переваги для виборчих органів. OAB можуть співпрацювати з органами розслідування[1], які отримують доступ до даних для виявлення та аналізу системних ризиків у рамках Союзу, а також для оцінки пропорційності, ефективності та впливу заходів щодо пом'якшення ризиків у контексті виборів. Висновки таких розслідувань (наприклад, детальний аналіз механізмів поширення дезінформації на онлайн-платформі під час проведення виборів) можуть бути використані для майбутньої розробки і впровадження адекватних регуляторних заходів або ж для реформи правового забезпечення OAB. Відтак виборчі органи мають бути добре обізнані з цими положенням і підтримувати діяльність органів розслідування, які вивчають інциденти та порушення у виборчих онлайн-кампаніях за принципом прозорості, якого вимагає DSA.

1 Як це визначається Статтею 2(1) Директиви 2019/790 Європейського Парламенту та Ради Європи від 17 квітня 2019 року про авторське право та суміжні права на єдиному цифровому ринку та про внесення змін до відповідних Директив 96/9/ЄС та 2001/29/ЄС.

3.5. **МІЖВІДОМЧА КООРДИНАЦІЯ**

У контексті впровадження заходів з пом'якшення ризиків для виборчих процесів на національному рівні самими VLOP та VLOE, Європейська рада з цифрових послуг та Європейська

комісія підготували Добірку інструментів DSA для координаторів цифрових послуг у виборах. Спираючись на Керівні принципи Комісії у проведенні демократичних виборів, пропонована добірка інструментів окреслює заходи для забезпечення цілісності виборчих процесів, зокрема для протидії поширенню мови ненависті, дезінформації та оманливого контенту, створеного за допомогою штучного інтелекту, або ж інших форм FIMI.

Згідно з представленими рекомендаціями, роль координаторів цифрових послуг спирається на чотири основні принципи: (a) управління зацікавленими сторонами через налагодження взаємодії для обміну знаннями та ресурсами; (b) комунікація та медіаграмотність через інформування, просвіту та побудову довіри; (c) моніторинг та аналіз пов'язаних з виборами ризиків через сприяння громадському контролю й оцінюванню ефективності заходів VLOP і VLOE щодо зменшення ризиків; та (d) реагування на інциденти завдяки підготовці, швидкій взаємодії та належній підтримці під час кризи.

За усіма чотирма напрямками слід заохочувати ОАВ відігравати центральну роль у забезпеченні цілісності виборів та посилювати інституційну експертизу у співпраці з ключовими зацікавленими сторонами для зміцнення їхнього потенціалу щодо захисту та збереження цілісності виборчої інформації в Інтернеті, зокрема протидіяти операціям з поширення дезінформації, мови ненависті, FIMI тощо.

Міжвідомча взаємодія координаторів цифрових послуг, ОАВ та інших відповідних органів створює можливості для усунення існуючих прогалин в адмініструванні виборів з одночасним набуттям ОАВ нового інституційного досвіду. Для наближення такої перспективи Міжнародний інститут демократії та сприяння виборам (International IDEA) розробив модель міжвідомчої взаємодії у сфері кібербезпеки (van der Staak and Wolf 2019), яку можна адаптувати і застосовувати для пом'якшення інших ризиків у виборчих процесах.

Стосовно впровадження DSA, Європейська комісія вже розпочала розробку «архітектури міжвідомчої комунікації», відображену у нашій піраміді як «рівні міжвідомчої взаємодії» (див. Рисунок 3.1). Європейська рада із цифрових послуг створила робочу групу із забезпечення цілісності інформаційного простору, що також охоплює виборчі процеси, FIMI, дезінформацію та інші види громадського обговорення

Рисунок 3.1. **Модель міжвідомчої взаємодії**

Джерело: С. ван дер Стаак і П. Вольф, *Кібербезпека на виборах: моделі міжвідомчої взаємодії* (Стокгольм: International IDEA, 2019), <https://doi.org/10.31752/idea.2019.23>.

(Європейська комісія 2025a). Робоча група має допомогти усім зацікавленим сторонам отримати спільне розуміння оцінки ризиків та створити дієві механізми для запобігання і реагування на потенційні інциденти у координації з ОАВ. Ключову роль тут може відігравати Європейська мережа співпраці з питань виборів. Хорошим прикладом для наслідування є організація навчання з кібербезпеки для оцінки ризиків та підсилення цільових антикризових заходів під час проведення європейських виборів, що демонструє важливість та позитивні результати міжвідомчої взаємодії для захисту цілісності виборів в Європі.

Спільні зусилля ОАВ, координаторів цифрових послуг та онлайн-платформ можуть сприяти посиленню стійкості усіх зацікавлених сторін для належної відповіді на основні цифрові виклики для цілісності виборів.

Підсумовуючи, захист цілісності виборчої інформації є складним і довгостроковим завданням, що вимагає координації дій різних національних і європейських інституцій для обміну провідним досвідом, інформацією та ресурсами, а також для забезпечення ситуаційної обізнаності. Спільні зусилля ОАВ, координаторів цифрових послуг та онлайн-платформ можуть сприяти посиленню стійкості усіх зацікавлених сторін для належної відповіді на основні цифрові виклики для цілісності виборів.

3.6. **РОЛЬ ВИБОРЧИХ ОРГАНІВ У РАМКАХ ЗАКОНУ ПРО ШТУЧНИЙ ІНТЕЛЕКТ**

Стосовно інституційного забезпечення належної реалізації законодавства, Акт про ШІ (Стаття 70) вимагає від кожної держави-члена ЄС призначити національний наглядовий орган для відповідного впровадження та нагляду. Зазвичай ОАВ не виступають у ролі такого наглядового органу, однак активно залучаються до міжвідомчої координації, особливо якщо ШІ використовується для логістичного забезпечення виборів або ж моніторингу виборчих кампаній. Наприклад, ОАВ можуть бути зобов'язані проводити аудит та оцінку відповідності використовуваних систем ШІ, або ж співпрацювати з органами із захисту даних, якщо використання ШІ стосується обробки персональних даних (Європейська рада із захисту даних та Європейський інспектор із захисту даних, 2021).

Крім того, положення Акту перетинаються з іншими відповідними правовими інструментами, зокрема GDPR та DSA. Поєднання цих законодавчих актів створює єдиний правовий контекст, що вимагає належного дотримання вимог усіма учасниками виборчого процесу та онлайн-платформами; і ОАВ у межах своїх мандатів тут часто виступатимуть як у ролі безпосереднього суб'єкта повноважень, так і у ролі посередника.

Акт про ШІ першочергово спрямований на вирішення проблеми використання маніпулятивного або оманливого контексту і неправомірних технік у політичній комунікації. Так, Стаття 5 забороняє використання систем ШІ, які приховано змінюють поведінку людей або ж використовують вразливості аудиторії; це безпосередньо стосується емоційно переконливих дипфейків або штучно створених ботів для поширення дезінформації (Floridi et al. 2018). Хоча ОАВ не відповідають за дотримання

цих заборон, вони мають здійснювати моніторинг виборчого середовища — зокрема виявляти підозрілий контент, сприяти прозорості виборчих кампаній і проводити просвіту виборців щодо маніпулятивного характеру створених за допомогою ШІ матеріалів — та співпрацювати з відповідними регуляторними органами для усунення виявлених порушень.

Водночас впровадження цих правових інструментів у контексті виборів створює низку інституційних та практичних викликів, переважно через їхню фрагментованість. Так, Акт про штучний інтелект не надає чіткого визначення ролі ОАВ у системі забезпечення дотримання визначених заборон, що може призвести до прогалин у нагляді або, навпаки, до дублювання зусиль (Iwańska et al. 2024: 18–19). Крім того, значна частина ОАВ наразі не мають технічних можливостей для належної оцінки дотримання стандартів системами ШІ або для впевненого визначення, чи є використання певної системи ШІ для цілей виборчої кампаній законним або ж неправомірним.

Акт про ШІ не надає чіткого визначення ролі ОАВ у системі правозастосування, що може призвести до прогалин у нагляді або, навпаки, до дублювання зусиль.

Крім того, виникає проблема стислих термінів і оперативності: виборчі періоди мають жорсткі часові рамки, і чинні механізми правозастосування у сфері ШІ можуть виявитися недостатньо гнучкими для належного реагування на швидкоплинні маніпулятивні практики у режимі реального часу.

З огляду на означені виклики, ОАВ мають завчасно готуватися до виконання регуляторних вимог, впроваджених Актом про ШІ. Процес підготовки передбачає створення інституційного потенціалу для оцінки ризиків використання систем ШІ, розробку процедури передвиборчого аудиту, а також активну участь у спільних робочих групах з органами із захисту даних та національними наглядовими органами з питань використання ШІ. Підготовка до виконання регуляторних вимог вимагає колективних зусиль, що передбачають ефективні механізми міжвідомчої взаємодії (див. 3.5: Міжвідомча координація).

Ефективне правозастосування Акту про ШІ вимагає, серед іншого, постійної міжвідомчої комунікації, напрацювання та обміну досвідом, а також проведення спільних навчань з вирішенням потенційно реальних сценаріїв. Не менш необхідною видається співпраця і між недержавними суб'єктами, як от політичними партіями, приватними компаніями та організаціями громадянського суспільства. Також ОАВ мають підтримувати вимоги прозорості для політичних кампаній, які використовують ШІ — наприклад, обов'язково позначати штучно

створений контент або розкривати інформацію про інструменти поведінкового тарґетингу. Довіра громадськості до виборів дедалі більше залежить не лише від процедурної цілісності, але й від сприйняття доброчесності всієї інформаційної екосистеми, у якій приймаються політичні рішення.

Акт про ШІ забезпечує надійну нормативно-правову базу, яка — хоч і не розроблена спеціально для виборів — має важливе значення для цілісності виборчого процесу.

Акт про ШІ забезпечує надійну нормативно-правову базу, яка — хоч і не розроблена спеціально для виборів — має важливе значення для цілісності виборчого процесу. Відтепер ОАВ мають опанувати інструменти правової екосистеми, у якій неправомірне використання систем ШІ визнається джерелом як технологічних, так і нормативних ризиків для демократичної участі. Попри визначення правозастосування офіційним обов'язком національних наглядових органів, ОАВ та інші відповідні регулятори насправді є безпосередньо зацікавленими сторонами у належному дотриманні вимог, що не дозволяють технологіям ШІ підривати вільні та чесні вибори. Проактивна участь ОАВ у забезпеченні виконання встановлених правил, нагляді та просвіті виборців матиме вирішальне значення для демократичної легітимності унормування ШІ в ЄС.

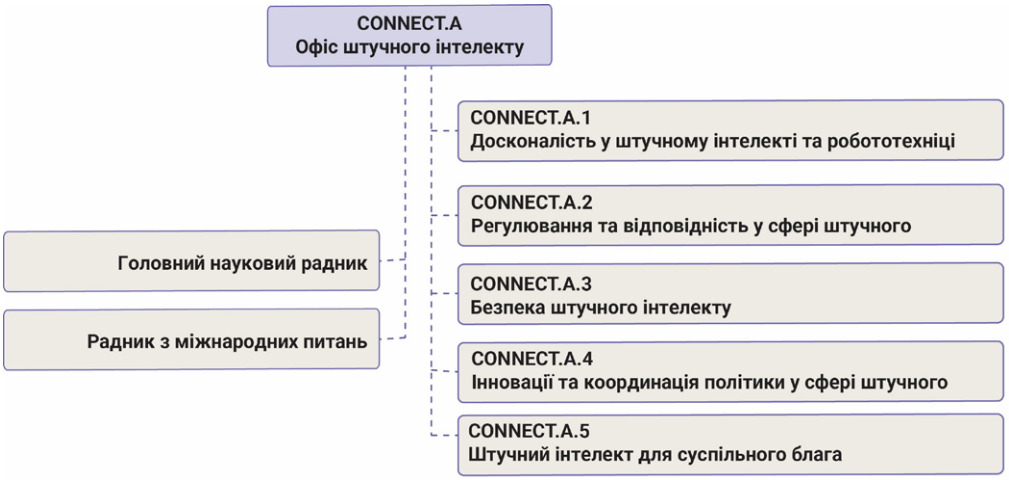
3.6.1. **Взаємодія ОАВ з Європейським офісом з питань ШІ**

Основною відповідальною установою за впровадження та забезпечення дотримання Акту про ШІ визнається Європейська комісія, яка у рамках Генерального директорату з питань комунікаційних мереж, контенту та технологій (DG CONNECT) створила спеціальний орган — Європейський офіс з питань ШІ — завданнями якого є координація політики в галузі ШІ на рівні ЄС, розвиток потенціалу та експертизи, а також допомога у виконанні інших пов'язаних завдань Комісії.

Для забезпечення дотримання Акту про ШІ у контексті виборів, ключовою контактною групою для ОАВ є підрозділ CONNECT A.3, відповідальний за безпечне використання штучного інтелекту. Цей підрозділ у складі Офісу з питань ШІ має взаємодіяти з експертами, громадянським суспільством та іншими відповідними зацікавленими сторонами, співпрацюючи з Генеральним директоратом з питань юстиції та захисту прав споживачів (DG JUST) Комісії та іншими союзними органами, як от з Агентством ЄС з основних прав (FRA) та Європейським інспектором із захисту даних (EDPS).

Нарешті, Стаття 77 Акту про ШІ передбачає, що національні державні органи, відповідальні за нагляд або правозастосування законодавства ЄС щодо захисту

Рисунок 3.2. **Схема Європейського офісу з питань ШІ у рамках DG CONNECT**



Джерело: Іванська та інші, «На шляху до впровадження закону про штучний інтелект, що служить людям і суспільству: стратегічні завдання для громадянського суспільства та спонсорів щодо виконання Акту ЄС про штучний інтелект», Європейський фонд штучного інтелекту та суспільства при Європейському центрі некомерційного права, серпень 2024 р., с. 19, <https://ecnl.org/sites/default/files/2024-09/AIFUND_ECNL_AI_ACT_Enforcement_2024.pdf>, дата перегляду: 22 вересня 2025 р.
Примітка: Крім того, Стаття 65 Акту про штучний інтелект засновує Європейську раду з питань ШІ, яка має забезпечити узгодженість та координацію між національними компетентними органами у державах-членах для належного виконання правових положень. Попри відсутність прямої згадки про моніторинг виборів, Рада має взаємодіяти з відповідними органами та мережами ЄС, включно з Європейською мережею співпраці з питань виборів та національними ОАВ.

основоположних прав, мають повноваження вимагати та отримувати доступ до будь-якої документації, створеної чи то збереженої у рамках дії цього закону. Така інформація має надаватися державним органам доступною мовою та у доступному форматі, коли це необхідно для ефективного виконання ними повноважень у межах встановленої юрисдикції. Про такі запити має бути поінформований відповідний орган з ринкового нагляду.

Це положення дозволяє ОАВ отримувати доступ до відповідної документації та інформації для цілей захисту основоположних прав у виборчому контексті, тобто у межах їхнього мандату щодо захисту права громадян обирати та бути обраними. Реалізація таких повноважень має відбуватися у співпраці та координації з іншими установами з питань забезпечення основних прав,

як от органи з питань гендерної рівності, органи із захисту даних та інші відповідні суб'єкти, включно з організаціями громадянського суспільства.

3.6.2. **Можливості правозастосування для виборчих органів у рамках Акту про штучний інтелект**

Акт про ШІ є значним досягненням у сфері регулювання, що визначає ЄС першою юрисдикцією, яка запровадила комплексну правову базу для ШІ. Хоча цей закон розроблявся як міжгалузевий регламент, він має як прямі, так і опосередковані наслідки для виборчих процесів та державних ОАВ. Виборчі процеси не є основним предметом Акту про ШІ як такого, однак його фокус на ризик-орієнтованому нагляді, захисті основних прав та діяльності управлінських структур значною мірою перетинається з регуляторними потребами демократичних виборів. Детальніше про основні положення Акту про ШІ див. таблицю 3.3.

3.7. **ПРАВОВІ НОВАЦІЇ З ТОЧКИ ЗОРУ ОАВ У ДЕРЖАВАХ-ЧЛЕНАХ ЄС**

Для вироблення цього звіту план нашого дослідження передбачав серію інтерв'ю із зацікавленими сторонами у виборчому процесі у державах-членах ЄС, включно з представниками ОАВ Естонії, Фінляндії, Німеччини та Ірландії. Далі представлені основні погляди та ключові висновки щодо впровадження правових новацій у сфері цифровізації та їхнього впливу на вибори.

- Наразі інноваційність та неусталеність впроваджувальної регуляторної бази ЄС у сфері цифровізації є викликом навіть для найрозвинутіших держав-членів ЄС, яким доводиться швидко адаптувати свої складні правові, технічні та інституційні екосистеми у постійно змінюваному контексті розвитку ІКТ.

- Інституційна архітектура та повноваження ОАВ у різних країнах ЄС є досить неоднаковими. У деяких державах-членах виборчі органи мають ширший мандат щодо впровадження цифрових регламентів ЄС, які впливають на вибори. В інших країнах такі повноваження розподілені між широкою мережею інституцій — від профільних міністерств

Таблиця 3.3. **Основні положення Акту про ШІ та можливості правозастосування для ОАВ**

Положення Закону про ШІ	Можливості правозастосування для ОАВ
Стаття 5: Заборонені практики у сфері ШІ	Акт про ШІ забороняє випуск на ринок, введення в експлуатацію або використання систем ШІ, які застосовують підсвідомі маніпулятивні техніки для впливу на поведінку людини або експлуатують індивідуальні уразливості (такі як вік, інвалідність або соціально-економічний статус) для істотного впливу на поведінку людини, зокрема у спосіб, що знижує якість прийнятих рішень (Стаття 5[1][a]–[b]). Під заборону також підпадають системи ШІ, які застосовують техніку соціального скринінгу та біометричної категоризації осіб, якщо це призводить до невиправданого до них ставлення або надмірної уваги (стаття 5[1][c]). Ці заборони особливо актуальні для виборів, коли генеровані ШІ дипфейки, переконливі чат-боти та віртуальні боти можуть поширювати дезінформацію, маніпулювати свідомістю виборців або використовувати їхні уразливості. Хоча ОАВ не визнаються офіційними органами правозастосування, відповідно до Статті 5 вони мають щільно координувати свої дії з органами із захисту даних та національними органами нагляду за ШІ, особливо протягом чутливого періоду виборчої кампанії.
Стаття 6 та Додаток III: Класифікація ШІ з високим рівнем ризику	Системи ШІ відносяться до «зони високого ризику», якщо вони використовуються основними державними службами, включно з правоохоронними органами, критичною інфраструктурою, судочинством та з метою демократичних процесів (Додаток III, розділ 8). Якщо виборчі органи використовують або закуповують такі системи, вони мають дотримуватися зобов'язань, передбачених статтями 8 — 15, а саме: • впроваджувати систему управління ризиками; • забезпечувати цілісність та ефективність управління даними; • вести офіційні журнали відстеження та реагування на інциденти; • гарантувати прозорість використання та контроль людини. Крім того, ОАВ мають забезпечити оцінку відповідності таких систем перед впровадженням, яка може здійснюватися призначеними органами або власними силами (якщо це дозволено за класифікацією системи). Такі зобов'язання значно збільшують регуляторне навантаження на ОАВ у разі цифровізації частини процесу голосування. Нарешті, використання систем ШІ може розширити зону ураження для кібератак, що вимагає від ОАВ забезпечення регулярного навчання з кібербезпеки та підвищення стійкості до стандартних вразливостей.
Стаття 27: Оцінка впливу на основоположні права	Стаття 27 вимагає від будь-якої установи при впровадженні у державному секторі систем ШІ з високим рівнем ризику, проводити оцінку впливу таких систем на основоположні права (FRIA) перед введенням їх в експлуатацію. Ця вимога поширюється на ОАВ, якщо вони використовують ШІ для виборчих цілей, як от реєстрація виборців, цифрова верифікація особи або аналіз даних, пов'язаних з проведенням виборів. У контексті виборів має бути оцінений фактичний або потенційний вплив на такі основні гарантії, як право на приватність, недискримінація, свобода вираження поглядів та політична участь. Хоча Акт про ШІ не передбачає обов'язкового проведення публічних консультацій, він вимагає документування виявлених ризиків та запланованих заходів щодо їх пом'якшення. Закон не передбачає обов'язкового оприлюднення результатів оцінювання впливів на основоположні права громадян. Щодо виборчих органів, FRIA є важливим інструментом для виявлення та пом'якшення ризиків для прав виборців, доброчесності та інклюзивності виборів; це особливо важливо для прав різних меншин або вразливих груп населення. Однак, через відсутність стандартизованих шаблонів та процедурних гарантій, ОАВ доводиться виходити за межі базових вимог шляхом: • встановлення надійних процедур внутрішнього контролю; • заохочення прозорості; та • залучення наглядових органів для перевірки. За доцільності ОАВ також можуть вдаватися до гендерної розбивки зібраних даних для виявлення та упередження непропорційного впливу систем ШІ на політичну участь жінок та інших вразливих груп. Такий аналіз даних може допомогти у виявленні й зменшенні алгоритмічної упередженості, відтак сприяти доброчесності та інклюзивності виборчих процесів.
Статті 16–29: Обов'язки впроваджувачів (користувачів) систем ШІ з високим рівнем ризику	Якщо ОАВ використовує систему ШІ з високим рівнем ризику, відповідно до Акту про ШІ він юридично визнається «користувачем» і має забезпечити дотримання таких вимог: • контроль людини (Стаття 14); • реєстрація та ведення обліку (Стаття 12); • моніторинг після розгортання та повідомлення про інциденти (Статті 72, 73); та • забезпечення технічної документації (Стаття 11). Цими положеннями встановлюється юридична відповідальність ОАВ, навіть якщо вони використовують інструменти ШІ, розроблені сторонніми постачальниками. Виборчі органи мають оновити свою закупівельну політику і вимагати від постачальників надання документації про відповідність, включно з маркуванням CE або записами внутрішнього аудиту, і забезпечити відповідність систем до визначених законом вимог.

Таблиця 3.3. **Основні положення Акту про ШІ та можливості правозастосування для ОАВ (cont.)**

Положення Закону про ШІ	Можливості правозастосування для ОАВ
Стаття 50: Зобов'язання прозорості щодо контенту, створеного за допомогою ШІ	Закон вимагає від користувачів систем ШІ, які генерують штучний або змінений контент (наприклад, дипфейки, синтетичні відео, людиноподібні боти), чітко маркувати інформацію, створену за допомогою ШІ (статті 52—54). Це положення стосується політичних партій та виборчих кампаній, які використовують створені за допомогою ШІ медіа. ОАВ, у межах до своєї відповідальності за моніторинг ведення кампаній, можуть забезпечувати дотримання цих стандартів прозорості, як от вимагати від учасників виборів маркувати такий політичний контент, а також оновлювати правила ведення кампаній із забороною непозначеного використання ШІ.
Стаття 74: Правозастосування	Закон вимагає від держав-членів призначити національні наглядові органи для забезпечення виконання Акту про ШІ (Стаття 70). Зазвичай ОАВ не виступають у ролі безпосереднього регулятора, однак національні уряди можуть делегувати їм допоміжні або консультативні повноваження у частині нагляду за системами ШІ, які використовуються у виборах. Для забезпечення ефективної координації ОАВ мають взаємодіяти з: • національними наглядовими органами щодо використання ШІ; • органами із захисту даних; та • координаторами цифрових послуг (у рамках DSA). Така міжвідомча взаємодія є особливо важливою у періоди проведення виборів.
Статті 72–73: Моніторинг роботи систем після впровадження та повідомлення про інциденти	ОАВ, які використовують системи ШІ з високим рівнем ризику, мають здійснювати постійний моніторинг, вести журнали інцидентів та повідомляти про серйозні збої у роботі системи, що можуть фактично або потенційно вплинути на безпеку або права користувачів. Ці заходи є особливо актуальними під час виборів, коли технічна надійність набуває вирішального значення для забезпечення часом хиткої довіри громадськості. ОАВ зобов'язані: • вести внутрішній реєстр ризиків ШІ; • проводити технічний аудит після завершення виборів; та • розробляти плани реагування на інциденти згідно з протоколами управління кризами у виборах (van der Staak and Wolf 2019).
Стаття 57: Регуляторні пісочниці	Закон заохочує інноваційні рішення через створення регуляторних пісочниць (Стаття 57), що надає змогу ОАВ тестувати певні інструменти ШІ (наприклад, для просвіти виборців, забезпечення доступності виборів або виявлення шахрайства) під наглядом відповідних регуляторних органів. ОАВ мають подавати заявки на участь у регуляторних пісочницях на національному або європейському рівні та отримувати необхідну підтримку для експериментального тестування інструментів ШІ задля мінімізації можливих юридичних ризиків.

до груп швидкого реагування на інциденти комп'ютерної безпеки та агентств із захисту персональних даних тощо.

- Така неоднаковість мандатів обумовлює роль кожного ОАВ та рівень його взаємодії з національними та європейськими інституціями у формуванні та правозастосуванні нових цифрових регламентів ЄС. Виборчі органи з більш широкими повноваженнями правозастосування нормативно-правової бази ЄС зазвичай підтримують безпосередній зв'язок та пряму взаємодію з відповідними інституціями на рівні Союзу. І навпаки, ОАВ з обмеженими мандатами через розподіл повноважень між іншими установами — органами із захисту даних, агентствами з інформаційної безпеки

або регуляторами ЗМІ — меншою мірою безпосередньо долучаються до таких процесів.

- Першочергові інституційні заходи у державах-членах ЄС спрямовані на захист персональних даних та дотримання вимог GDPR. Відтак ОАВ повідомляють про заборону публікації списків виборців, обмежений доступ до реєстрів та особливі процедури для обережної обробки таких даних.

- Щодо загроз виборчим процесам, деякі ОАВ повідомили про відсутність кібератак на свої системи, однак відзначили важливу роль органу з інформаційної безпеки та тісну співпрацю у цій царині з європейськими структурами, як от з Європейською мережею співпраці з питань виборів та Європейським агентством з кібербезпеки. Водночас інші ОАВ повідомили про інциденти з кібербезпекою, зокрема про атаки на сайти політичних партій. Варто зазначити, що такі інциденти не створили загроз цілісності виборів як таких.

- Виборчі органи застосовують різні підходи до модерації контенту, і деякі з них використовують інструменти моніторингу для виявлення дезінформації або неправомірних висловлювань (у контексті виборів) у соціальних мережах. Деякі ОАВ залучають приватні компанії для моніторингу ЗМІ, які мають команду власних експертів для виявлення та вчасного видалення дезінформації чи то іншого незаконного контенту. Представник одного з ОАВ розказав, що за оновленими правилами ведення виборчої кампанії партії були зобов'язані позначати будь-який контент, створений за допомогою штучного інтелекту. Водночас низка ОАВ взагалі не вважають моніторинг соціальних мереж під час виборів частиною своїх повноважень, адже у їхніх країнах це зона відповідальності інших компетентних органів.

- Щодо впровадження систем ШІ для цілей проведення виборів, ОАВ переважно не виявляють бажання користуватися таким інструментом як чат-боти, попри проведення попередніх обговорень стосовно можливостей використання ШІ виборчими органами. Представник лише одного з ОАВ розказав про успішне використання таких інструментів, однак із дотриманням безпекового підходу. Переважно ШІ використовується ОАВ для проведення просвітницьких та мотиваційних кампаній, які також навчають громадян виявляти недостовірну інформацію та відверту дезінформацію.

ОАВ з більш широкими повноваженнями правозастосування нормативно-правової бази ЄС зазвичай підтримують безпосередній зв’язок та пряму взаємодію з відповідними інституціями на рівні Союзу.

ОАВ у державах-членах ЄС в основному усвідомлюють ризики та виклики, з якими стикаються їхні колеги у країнах-кандидатах на членство в ЄС, як і транскордонний характер цифрових загроз у виборчих процесах.

- Щодо координації на рівні ЄС, виборчі органи активно взаємодіють з такими платформами як Європейська мережа співпраці з питань виборів, а також повідомляють про свій внесок у європейську ініціативу «Щит демократії» та формування законодавства ЄС через співпрацю з відповідними міністерствами.

- ОАВ у державах-членах ЄС переважно усвідомлюють ризики та виклики, з якими стикаються їхні колеги у країнах-кандидатах на членство в ЄС, як і транскордонний характер цифрових загроз у виборчих процесах.

Розділ 4

ВИСНОВКИ

Цифрова трансформація виборчих процесів створює як безпрецедентні можливості, так і серйозні виклики для стійкості демократії. Наразі виборчі процеси залишаються у компетенції національних органів влади, а ЄС поступово вибудовує міцну правову та інституційну основу для зміцнення демократичних цінностей та захисту основних прав у цифровому середовищі. Впроваджуючи такі базові принципи, як прозорість, підзвітність та захист даних у свої цифрові регламенти, ЄС сприяє створенню цілісного простору, у якому цифрові технології поставлені на службу демократичним процесам, а не підривають їх зсередини чи то ззовні.

Через впровадження таких правових інструментів, як Загальний регламент про захист даних (GDPR), Акт про цифрові послуги (DSA), Регламент прозорості й тарґетування політичної реклами (TTPA), Європейський закон про свободу медіа (EMFA) та Акт про штучний інтелект (AI Act), ЄС створив комплексну правову архітектуру, яка дозволяє протидіяти основним загрозам для цілісності виборчого процесу, починаючи від зловживання даними та маніпулювання алгоритмами і закінчуючи дезінформацією та непрозорістю онлайн-платформ. Ці правові інструменти не лише визначають стандарти для постачальників цифрових послуг, але й забезпечують необхідні гарантії для громадян та демократичних інститутів.

Крім того, спільні ініціативи ЄС, включно з міжвідомчими мережами та майданчиками для обміну провідним досвідом, посилюють здатність держав-членів належно реагувати на транскордонні виклики, координувати нагляд та забезпечувати безпеку і прозорість виборчих екосистем. Такі зусилля є життєво

Спільні ініціативи ЄС посилюють здатність держав-членів належно реагувати на транскордонні виклики, координувати нагляд та забезпечувати безпеку і прозорість виборчих екосистем.

важливими в епоху, коли інформаційні потоки та ворожі операції впливу набувають дедалі більшого міжнародного характеру.

У перспективі ефективне впровадження та узгоджена реалізація нового законодавства матиме вирішальне значення для упередження нових ризиків, у тому числі пов'язаних з розвитком генеративного штучного інтелекту та стратегій мікро тарґетингу. Посилення співпраці між національними органами влади, інституціями ЄС, громадянським суспільством та цифровими платформами залишається безальтернативною передумовою розбудови стійких демократичних суспільств. У сучасному спільному цифровому та регуляторному просторі ЄС відіграє ключову роль у підтримці зусиль усіх держав-членів щодо забезпечення вільних, доброчесних та прозорих виборів і одночасно виступає гарантом відповідності цифрових інновацій основоположним цінностям демократії, верховенства права та основних прав людини.

Глосарій

Техніки доставки реклами	Техніки оптимізації, які використовуються для збільшення тиражу, охоплення або помітності політичної реклами на основі автоматизованої обробки персональних даних і уможливлюють адресну доставку політичної реклами до конкретної особи або групи (Стаття 3[12] TTPA).
Система штучного інтелекту/ генеративний ШІ	Машинна система, яка з явними або прихованими цілями на основі аналізу вхідних даних генерує вихідний результат — як от прогнози, контент, рекомендації або рішення — що може впливати на фізичне або віртуальне середовище. Системи ШІ різняться за рівнем своєї автономності та адаптивності після впровадження (OECP, без дати).
Астротурфінг	Обманна імітація громадської ініціативи та створення ілюзії масової підтримки чи засудження для цілей лобіювання із замовчуванням спонсорів організованого повідомлення (наприклад, політичної, економічної, рекламної, релігійної або організації із зв'язків з громадськістю). Ця практика може набувати різних форм, зокрема створення активних фальшивих акаунтів у соціальних мережах (ботоферм), залучення оплачуваних інфлюенсерів та фальшиві коментарі. Астротурфінг використовується для підсилення авторитетності певних заяв або організацій з приховування справжніх фінансових джерел та вигодонабувачів.
Поведінкове тарґетування	Метод націлювання реклами — часто через «реальні торги» — на аудиторію вебсайту, сегментовану на основі аналізу онлайн-поведінки користувачів. Наприклад, Facebook пропонує інструмент під назвою Facebook Pixel — фрагмент коду, який рекламодавці можуть встановлювати на вебсайт для відстеження дій відвідувачів та вимірювання ефективності реклами.
Темні шаблони (патерни)	Темний шаблон (dark pattern) — це інтерфейс сайту або додатку, розроблений з метою спонукати користувача до дії, яку б він не вчинив за інших обставин (наприклад, купити продукт або підписатися на послугу). Організація економічного співробітництва та розвитку (OECP) у своєму визначенні зазначає, що ця техніка дозволяє схиляти, обманювати, примушувати або маніпулювати користувачами для прийняття рішень, які суперечать їхнім інтересам.

Дипфейк	Контент, згегнерований штучним інтелектом чи то методом поєднання і накладення одних зображень або відео на інші, що нагадує реальну особу, об'єкт, місце або подію і виглядає автентичним або правдивим (Стаття 3[60] Акту про штучний інтелект).
Дезінформація	Сфабрикована інформація або навмисно спотворений аудіовізуальний контент (наприклад, навмисно вигадані теорії змови або чутки). Такий контент може виглядати законним, але насправді він призначений для заподіяння шкоди.
Інформаційні маніпуляції та іноземне втручання	Модель поведінки, яка загрожує або може негативно вплинути на цінності, процедури та політичні процеси. Такі дії мають маніпулятивний характер і здійснюються навмисно та скоординовано державними або недержавними суб'єктами, включно з їхніми представниками, на території та поза межами власної країни (Європейська служба зовнішніх справ 2023).
Виведені дані	Інформація, отримана розпорядником на основі аналізу вхідних даних, наданих самим суб'єктом даних або отриманих за результатами спостережень розпорядника.
Цілісність інформації	Організація Об'єднаних Націй визначає цілісність інформації як збереження її точності, повноти та достовірності. Інформаційній цілісності загрожує дезінформація, викривлена інформація та мова ворожнечі.
Хибна інформація (мізінформація)	Неправдива або неточна інформація, яка поширюється без злого наміру ввести в оману і не передбачає свідомого створення маніпулятивного контенту. Прикладами тут можуть бути ненавмисні помилки, як от некоректно підписані фотографії, зазначені дати та статистичні дані, а також неправильний переклад чи то сприйняття за правду сатиричного контенту.
Видимі (спостережувані) дані	Інформація, надана самим суб'єктом даних — наприклад, користувачем соціальної мережі — під час користування послугою або пристроєм (лайки, репости, переглянутий контент тощо) (Європейська рада із захисту даних 2020b: 12).

Рекомендаційна система	Повністю або частково автоматизована система фільтрації даних, що використовується онлайн-платформою для доставки конкретної інформації користувачам за рейтингом їхніх вподобань, визначеним на основі аналізу пошукових запитів, переглядів та іншої інформації з профілю користувача (Стаття 3[s] DSA).
Техніки тарґетингу	Техніки, що використовуються для адресної доставки політичної реклами певній особі або групі осіб, або ж для виключення особи чи то групи із цільової аудиторії охоплення на основі обробки персональних даних (стаття 3[11] TTPA).

Посилання

Access Now, *«Комісар Бретон: Припиніть політизувати Акт про цифрові послуги»,* 19 серпня 2024 р., <https://www.accessnow.org/press-release/commissioner-breton-stop-politicising-the-digital-services-act/>, дата перегляду: 30 березня 2025 р.

Д. Альварадо Рінкон, *«Сам по собі DSA не врятує демократію, але у взаємодії з верховенством права може вийти»,* Democracy Reporting International, квітень 2025 р., <https://democracyreporting.s3.eu-central-1.amazonaws.com/images/67ecf2669e5db.pdf>, дата перегляду: 8 Серпень 2025 р.

СТАТТЯ 19, *«Наслідки запропонованого регулювання політичної реклами в ЄС для свободи вираження поглядів»,* серпень 2023 р., <https://www.article19.org/wp-content/uploads/2023/08/A19-The-implications-of-the-Proposed-EU-Political-Advertising-Regulation-A19_clean.pdf>, дата перегляду: 3 березня 2025 р.

Дж. Барата та Е. Лазар, *«Чи врятує DSA демократію? Перше випробування нещодавніми президентськими виборами у Румунії»,* Tech Policy Press, 27 січня 2025 р., <https://www.techpolicy.press/will-the-dsa-save-democracy-the-test-of-the-recent-presidential-election-in-romania>, дата перегляду: 8 березня 2025 р.

В. Башякарла, С. Хенкі, А. Макінтайр, Р. Ренно та Г. Райт, *«Персональні дані: політичні переконання як «гачок» в індустрії впливу. Як це працює»* (Tactical Tech, 2019), <https://cdn.ttc.io/s/tacticaltech.org/influence-industry.pdf>, дата перегляду: 31 березня 2025 р.

С. Бекер Кастелларо та Дж. Пенфрат, *«DSA не здатен контролювати найбільш шкідливі цифрові платформи, та попри це є корисним»,* Verfassungsblog, 8 листопада 2022 р., <https://verfassungsblog.de/dsa-fails>, дата перегляду: 1 квітня 2025 р.

А. Богуцький, А. Енглер, К. Перарно та А.Ренда, *«Акт про штучний інтелект та нове законодавство ЄС у сфері цифровізації: дублювання, прогалини та колізії»,* Центр європейських політичних досліджень, вересень 2022 р., <https://cdn.ceps.eu/wp-content/uploads/2022/09/CEPS-In-depth-analysis-2022-02_The-AI-Act-and-emerging-EU-digital-acquis.pdf>, дата перегляду: 1 квітня 2025 р.

М. Ботан, *«Вплив алгоритмів на вибори: висновки з практичного кейсу Румунії»,* Європейська обсерваторія цифрових медіа, 9 грудня 2024 р., <https://edmo.eu/blog/algorithmic-influence-on-elections-insights-from-romanias-case-study>, дата перегляду: 1 квітня 2025 р.

С. Бредшоу та П.Н. Говард, *«Виклик істині та довірі: глобальний перелік організованих маніпуляцій у соціальних медіа»,* Оксфордський інститут інтернету, робочий документ 2018.1, <https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2018/07/ct2018.pdf>, дата доступу: 10 квітня 2025 р.

Г. Берк, *«Випробування Європейського щита демократії»,* Інститут міжнародних та європейських справ, березень 2025 р., <https://www.iiea.com/images/uploads/resources/Democracy_shield_explainer_final.pdf>, дата перегляду: 9 квітня 2025 р.

К. Буш, К. та В. Мак, *«Огляд Акту про цифрові послуги у чинному контексті: подолання розриву між законодавством ЄС про захист прав споживачів та регулюванням онлайн-платформ»,* Journal of European Consumer and Market Law, 109, (2021), <https://doi.org/10.2139/ssrn.3933675>

С. Калабрезе, *«Коментар: Політична угода щодо регулювання прозорості й тарґетування політичної реклами»,* Європейське партнерство за демократію, 10 січня 2024a, <https://epd.eu/content/uploads/2024/01/Political-Advertising-Reaction-Paper-1.pdf>, дата перегляду: 1 квітня 2025 р.

«Чи є захист цілісності виборів невід'ємною частиною Акту про штучний інтелект?», Європейське партнерство за демократію, 2024b, <https://epd.eu/content/uploads/2024/07/Is-election-integrity-integral-to-the-Artificial-Intelligence-Act_-1-1-7.pdf>, дата перегляду: 16 березня 2025 р.

Центр демократії та технологій, *«Попередній аналіз першої серії звітів про оцінку ризиків відповідно до Акту ЄС про цифрові послуги»,* березень 2025 р., <https://cdt.org/wp-content/uploads/2025/03/RA-Report-Assessment-Report.pdf>, дата перегляду: 1 квітня 2025 р.

Союз громадянських свобод Європи, *«Політична реклама у Facebook під час проведення парламентських виборів в Угорщині 2022 року: звіт по країні»,* вересень 2022 р., <https://www.liberties.eu/f/fs3mhp>, дата перегляду: 1 квітня 2025 р.

Національна комісія Франції з інформатики та свобод (CNIL), *«Санкції, накладені CNIL»,* 2 січня 2025 р., <https://www.cnil.fr/en/investigating-and-issuing-sanctions/sanctions-issued-cnil>, дата перегляду: 30 березня 2025 р.

Р. Корнеа, *«Войовнича румунська демократія в дії: захист демократичної системи від підриву та скасування виборів»*, Verfassungsblog, 1 квітня 2025 р., <https://doi.org/10.59704/1a0400f2b9629e46>

Рада Європи, Консультативний комітет Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних, *«Конвенція 108: Керівні принципи щодо захисту осіб у зв'язку з обробкою персональних даних для цілей реєстрації та аутентифікації виборців»,* T-PD(2023)2rev6, 7 червня 2024 р., <https://rm.coe.int/tpd-2023-2rev6-processing-pd-in-vote-and-elections-en-final/1680b1511c>, дата перегляду: 31 березня 2025 р.

Суд Європейського Союзу (CJEU), Директорат з розслідувань та документації, *«Сфера застосування Хартії основоположних прав Європейського Союзу»,* березень 2021 р., <https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-05/fiche_thematique_-_charte_-_en.pdf>, дата перегляду: 1 квітня 2025 р.

Ф. Каннінгем, *«Які країни вже призначили своїх координаторів із цифрових послуг відповідно до DSA?»,* Bird&Bird, 27 жовтня 2023 р., <https://www.twobirds.com/en/insights/2023/global/which-countries-have-already-designated-their-digital-services-coordinators-under-the-dsa>, дата перегляду: 30 березня 2025 р.

Б. Дуйвенвоорде та К. Гоанта, *«Унормування цифрової реклами відповідно до DSA: критична оцінка»,* Computer Law & Security Review, 51 (2023), <https://doi.org/10.1016/j.clsr.2023.105870>

Європейська комісія, *Демократія та виборчі права*, [без дати], <https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/democracy-eu

-citizenship-anti-corruption/democracy-and-electoral-rights_en>, дата перегляду: 1 квітня 2025 р.

Правова база ЄС щодо захисту даних, [без дати], <https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en>, дата перегляду: 1 квітня 2025 р.

Керівний документ *«Керівні рекомендації Комісії з реалізації законодавства Союзу про захист даних у виборчому контексті»,* документ COM/2018/638, Офіційний вісник Європейського Союзу (12 вересня 2018 р.), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0638>, дата перегляду: 5 березня 2025 р.

Рекомендація Комісії ЄС 2023/2829 від 12 грудня 2023 року щодо забезпечення інклюзивних та стійких виборчих процесів у Союзі та посилення європейського характеру й ефективності у проведенні виборів до Європейського парламенту, документ C/2023/8626, Офіційний вісник Європейського Союзу (20 грудня 2023 року), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202302829>, дата перегляду: 5 березня 2025 р.

«Питання та відповіді щодо Акту про цифрові послуги», 22 лютого 2024a, <https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2348>, дата перегляду: 30 березня 2025 р.

«Комісія опублікувала керівні принципи щодо зменшення системних онлайн-ризиків для виборів згідно Акту про цифрові послуги», 26 березня 2024b, <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1707>, дата перегляду: 1 квітня 2025 р.

«Керівні принципи Комісії для провайдерів дуже великих онлайн-платформ та дуже великих пошукових онлайн-систем щодо зменшення системних ризиків для виборчих процесів відповідно до Статті 35(3) Регламенту (ЄС) 2022/2065», Документ C/2024/3014, *Офіційний вісник Європейського Союзу* (26 квітня 2024c), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52024XC03014&qid=1714466886277>, дата перегляду: 5 березня 2025 р.

Лист-доручення, 17 вересня 2024d, <https://commission.europa.eu/document/download/907fd6b6-0474-47d7-99da-47007ca30d02_en?filename=Mission%20letter%20-%20McGRATH.pdf>, дата перегляду: 10 квітня 2025 р.

«Комісія розпочинає офіційне провадження проти TikTok через створення ризиків для виборів відповідно до Акту про цифрові послуги», 17 грудня 2024 року, <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6487>, дата перегляду: 8 березня 2025 року

«Робочі групи при Європейській раді з цифрових послуг», останнє оновлення від 12 лютого 2025 року, <https://digital-strategy.ec.europa.eu/en/policies/dsa-board-working-groups>, дата перегляду: 14 квітня 2025 року

«Керівні принципи Комісії щодо заборонених практик у сфері штучного інтелекту, встановлені Регламентом (ЄС) 2024/1689 (Акт про ШІ)», Документ C(2025) 884, 27 липня 2025b, <https://ec.europa.eu/newsroom/dae/redirection/document/112367>, дата перегляду: 1 квітня 2025

«Кодекс поведінки щодо дезінформації», 2025c, <https://crta.org.cy/assets/uploa d s/pdfs/Code_of_Conduct_on_Disinformation_FoMhXqsV0yrrqv7x7rydctBc4_112678.pdf>, дата перегляду: 16 березня 2025 р.

«Комісія вітає інтеграцію добровільного Кодексу практик щодо дезінформації до Акту про цифрові послуги», 2025d, <https://digital-strategy.ec.europa.eu/en/news/commission-endorses-integration-voluntary-code-practice-disinformation-digital-services-act>, дата доступу: 27 серпня 2025 р.

Європейська комісія з питань демократії через право (Венеціанська комісія), *«Терміновий звіт: про скасування результатів виборів конституційними судами»*, CDL-AD(2025)003, Висновок № 1218/2024, 27 січня 2025 р., <https://www.coe.int/en/web/venice-commission/-/urgent-report-on-the-cancellation-of-election-results-by-constitutional-courts>, дата перегляду: 14 квітня 2025 р.

Європейська мережа співпраці з питань виборів, Технічне завдання, [без дати], <https://commission.europa.eu/document/download/f6b67fff-e28d-4af2-aac6-deb836da7f82_en?filename=terms_of_reference.pdf>, дата перегляду: 5 березня 2025 р.

Європейський суд з прав людини, *«Рекомендації щодо реалізації Статті 3 Протоколу № 1 до Європейської конвенції з прав людини: Право на вільні вибори»,* 31 серпня 2024 р., <https://ks.echr.coe.int/documents/d/echr-ks/guide_art_3_protocol_1_eng>, дата перегляду: 10 квітня 2025 р.

«Європейська рада із захисту даних: завдання та обов'язки», [без дати], <https://www.edpb.europa.eu/about-edpb/what-we-do/tasks-and-duties_en>, дата перегляду: 30 березня 2025 р.

«Європейська рада із захисту даних: забезпечення рівних прав для всіх суб'єктів», [без дати], <https://www.edpb.europa.eu/system/files/2021-06/2020_06_22_one-stop-shop_leaflet_en.pdf>, дата перегляду: 30 березня 2025 р.

«Заява 2/2019 щодо використання персональних даних у політичних кампаніях», 13 березня 2019 р., <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf> дата перегляду: 30 березня 2025 р.

«Європейська рада із захисту даних (EDPB) видає лист-розпорядження щодо розкриття даних про президентські вибори у Польщі та обговорює останні накази уряду Угорщини щодо заходів під час надзвичайного стану через епідемію коронавірусу», 8 травня 2020 року, <https://www.edpb.europa.eu/news/news/2020/edpb-adopts-letter-polish-presidential-elections-data-disclosure-discusses-recent_en>, дата перегляду: 30 березня 2025 р.

«Керівні принципи 8/2020 щодо тарґеування користувачів соціальних мереж», версія 1.0., вересень 2020b, <https://www.edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202008_onthetargetingofsocialmediausers_en.pdf>, дата перегляду: 1 квітня 2025 р.

Європейська рада із захисту даних та Європейський інспектор із захисту даних, *«Спільна думка EDPB-EDPS 5/2021 щодо пропозиції Регламенту Європейського парламенту та Ради гармонізувати правила використання штучного інтелекту (Акт про штучний інтелект)»,* 18 червня 2021 р., <https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en>, дата перегляду: 10 квітня 2025 р.

Європейський інспектор із захисту даних, *«Захист даних»,* [без дати], <https://www.edps.europa.eu/data-protection/data-protection_en>, дата перегляду: 1 квітня 2025 р.

«Європейський інспектор із захисту даних закриває розслідування щодо дій Європейського парламенту під час виборів 2019 року», 23 березня 2020 р., <https://www.edps.europa.eu/press-publications/press-news/press-releases/2020/edps-closes-investigation-european-parliaments_en>, дата перегляду: 30 березня 2025 р.

«Керівні принципи 3/2022 щодо протидії темним шаблонам в інтерфейсах соціальних медіа-платформ: як їх розпізнати та уникнути», версія 1.0, 14 березня 2022 р., <https://www.edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf>, дата перегляду: 31 березня 2025 р.

Європейська служба зовнішніх справ, *«Перший звіт про зовнішнє маніпулювання інформацією та іноземне втручання: на шляху до створення системи мережевої оборони»,* лютий 2023 р., <https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023.pdf>, дата перегляду: 27 серпня 2025 р.

Європейський парламент, *«Резолюція від 20 жовтня 2020 року щодо Акту про цифрові послуги і дотримання основних прав»,* документ P9_TA(2020)0274, 20 жовтня 2020 р., <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0274_EN.pdf>, дата перегляду: 10 квітня 2025 р.

«Депутати Європарламенту посилюють правила щодо політичної реклами», прес-реліз, 24 січня 2023 р., <https://www.europarl.europa.eu/news/en/press-room/20230123IPR68616/meps-toughen-rules-on-political-advertising>, дата перегляду: 13 травня 2025 р.

«Створення спеціальної комісії з питань Європейського щита демократії та визначення її мандату, чисельності та терміну повноважень», документ 2024/2999(RSO), 18 грудня 2024 р., <https://www.europarl.europa.eu/doceo/document/TA-10-2024-0065_EN.html>, дата перегляду: 9 квітня 2025 р.

«Європейський щит демократії», Розклад роботи над планом впровадження, 20 березня 2025 р., <https://www.europarl.europa.eu/legislative-train/package-european-democracy-action-plan/file-european-democracy-shield>, дата перегляду: 9 квітня 2025 р.

Дослідницька служба Європейського парламенту, *«Поляризація та використання ІКТ у політичних кампаніях та комунікаціях»*, документ PE634.414, березень 2019 р., <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634414/EPRS_STU(2019)634414_EN.pdf>, дата перегляду: 1 квітня 2025 р.

Європейське партнерство за демократію, *«Тарґетинг та ампліфікація в політичній онлайн-рекламі»,* березень 2022 р., <https://epd.eu/content/uploads/2023/08/Targeting-and-amplification-in-online-political-advertising.pdf>, дата перегляду: 1 квітня 2025 р.

Європейський Союз, *«Регламент (ЄС) 2016/679 Європейського Парламенту та Ради Європи від 27 квітня 2016 року про захист прав фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загального регламенту захисту даних)»,* Офіційний вісник Європейського Союзу (27 квітня 2016 р.), <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>, дата перегляду: 5 березня 2025 р.

«Регламент (ЄС) 2019/790 Європейського Парламенту та Ради Європи від 17 квітня 2019 року про захист авторських та суміжних прав на єдиному ринку цифрових послуг; внесення змін до директив 96/9/ЄС та 2001/29/ЄС», Офіційний вісник

Європейського Союзу (17 квітня 2019 р.), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0790>, дата доступу: 27 серпня 2025 р.

«Регламент (ЄС) 2022/2065 Європейського Парламенту та Ради Європи від 19 жовтня 2022 року про єдиний ринок цифрових послуг та внесення змін до Директиви 2000/31/ЄС (Акт про цифрові послуги)», Офіційний вісник Європейського Союзу (27 жовтня 2022 року), <https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng>, дата перегляду: 5 березня 2025 р.

«Регламент (ЄС) 2024/900 Європейського Парламенту та Ради Європи від 13 березня 2024 року про прозорість і таргетування політичної реклами», Офіційний вісник Європейського Союзу (20 березня 2024a), <https://eur-lex.europa.eu/eli/reg/2024/900/oj/eng>, дата перегляду: 5 березня 2025 р.

«Регламент (ЄС) 2024/1083 Європейського Парламенту та Ради Європи від 11 квітня 2024 року про встановлення спільної рамки для медійних послуг на внутрішньому ринку та внесення змін до Директиви 2010/13/ЄС (Європейський зак он про свободу ЗМІ)», Офіційний вісник Європейського Союзу (17 квітня 2024b), <https://eur-lex.europa.eu/eli/reg/2024/1083/oj/eng>, дата перегляду: 5 березня 2025 р.

«Директива (ЄС) 2024/1385 Європейського Парламенту та Ради Європи від 14 травня 2024 року про боротьбу з насильством щодо жінок та домашнім насильством», Офіційний вісник Європейського Союзу (24 травня 2024c), <https://eur-lex.europa.eu/eli/dir/2024/1385/oj/eng>, дата перегляду: 5 березня 2025 р.

—, «Регламент (ЄС) 2024/1689 Європейського Парламенту та Ради від 13 червня 2024 року, що встановлює гармонізовані правила щодо штучного інтелекту та змінює регламенти (ЄС) № 300/2008, (ЄС) № 167/2013, (ЄС) № 168/2013, (ЄС) 2018/858, (ЄС) 2018/1139 та (ЄС) 2019/2144, а також директиви 2014/90/ЄС, (ЄС) 2016/797 та (ЄС) 2020/1828 (Закон про штучний інтелект)», *Офіційний вісник Європейського Союзу* (12 липня 2024d), <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>, дата перегляду: 5 березня 2025

Агентство Європейського Союзу з кібербезпеки, *«Кібербезпека виборів: виклики та можливості»,* лютий 2019 р., <https://www.enisa.europa.eu/sites/default/files/all_files/2019-02-28%20ENISA%20Opinion%20Paper-%20Election%20Cybersecurity.pdf>, дата перегляду: 5 березня 2025 р.

Агентство Європейського Союзу з основоположних прав (FRA) та Рада Європи (CoE), «*Керівництво з реалізації європейського законодавства про захист даних*» (Люксембург: Видавничий офіс Європейського Союзу, 2018), <https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition>, дата перегляду: 30 березня 2025 р.

Л. Флоріді, Дж. Коулс, М. Белтраметті, Р. Чатіла, П. Шазеран, В. Дігнум, К. Лютге, Р. Маделін, У. Пагалло, Ф. Россі, Б. Шафер, П.Вальке та Е. Ваєна, «*AI4People — етична рамка для гармонійного суспільства епохи штучного інтелекту: можливості, ризики, принципи та рекомендації»,* Minds and Machines, 28/4 (2018), с. 689–707, <https://doi.org/10.1007/s11023-018-9482-5>

GDPR Hub, «*Гарантії захисту персональних даних (Італія)*» [Італійський орган із захисту даних], 23 лютого 2023 р., <https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_9853406>, дата перегляду: 30 березня 2025 р.

Дж. Джетіле та О. Линскі, *«Недосконалий за задумом? Транснаціональна реалізація GDPR»,* International and Comparative Law Quarterly, 71 (2022), с. 799–830, <https://doi.org/10.1017/S0020589322000355>

У.А. Гортон, *«Маніпулювання свідомістю громадян: як використання поведінкових соціальних технік у політичних кампаніях шкодить демократії»,* New Political Science, 38/1 (2016), с. 61–80, <https://doi.org/10.1080/07393148.2015.1125119>

А. Гросс, *«Проєкт звіту про дотримання строків та перелік політичних критеріїв для оцінки виборів»,* Європейська комісія з питань демократії через право (Венеціанська комісія), документ CDL-EL(2010)021, 27 травня 2010 р., <https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-EL(2010)021-e>, дата перегляду: 10 квітня 2025 р.

П. Хаєк, «Румунія створює перше велике випробування для європейської кіберполіції», *POLITICO*, 12 грудня 2024 р., <https://www.politico.eu/article/romania-election-eu-digital-services-act-social-media-tiktok-calin-georgescu>, дата перегляду: 30 березня 2025 р.

Т. Хайнмаа, «*Вигравати вибори за правилами: унормування політичної онлайн-реклами в Європі та окремих країнах світу*» (Стокгольм: International IDEA, 2023), <https://doi.org/10.31752/idea.2023.77>

Human Rights Watch (HRW), *«Мережева пастка: неправомірне використання персональних даних під час виборів 2022 року в Угорщині»,* 1 грудня 2022 р., <https://www.hrw.org/report/2022/12/01/trapped-web/exploitation-personal-data-hungarys-2022-elections>, дата перегляду: 1 квітня 2025 р.

«Я не можу виконувати свою роботу журналіста»: Систематичні утиски свободи ЗМІ в Угорщині, 13 лютого 2024 р., <https://www.hrw.org/report/2024/02/13/i-cant-do-my-job-journalist/systematic-undermining-media-freedom-hungary>, дата перегляду: 14 квітня 2025 р.

Гантон, *«Перший штраф, накладений бельгійським органом із захист у даних після впровадження GDPR»,* 4 червня 2019 р., <https://www.hunton.com/privacy-and-information-security-law/first-fine-imposed-by-the-belgian-dpa-since-gdpr>, дата перегляду: 30 березня 2025 р.

Управління комісара з питань інформації, *«Керівництво з використання персональних даних у політичних кампаніях»,* [без дати], <https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guidance-for-the-use-of-personal-data-in-political-campaigning-1>, дата перегляду: 30 березня 2025 р.

International IDEA, База даних про використання ІКТ у виборах, [без дати], <https://www.idea.int/data-tools/data/icts-elections-database>, дата перегляду: 16 серпня 2025 р.

«Цифрове мікротаргетування: Посібник з інноваційних технік для політичних партій» (Стокгольм: International IDEA, 2018), <https://doi.org/10.31752/idea.2018.32>

К. Іванська, В. Скорич, Ф. Фануччі, Б. Кескіндемір та С. Коккула, *«На шляху до впровадження закону про штучний інтелект, що служить людям і суспільству: стратегічні завдання для громадянського суспільства та спонсорів щодо виконання Акту ЄС про штучний інтелект»,* Європейський центр некомерційного права, серпень 2024 р., <https://ecnl.org/sites/default/files/2024-09/AIFUND_ECNL_AI_ACT_Enforcement_2024.pdf>, дата перегляду: 10 квітня 2025 р.

П. Джунеджа, *«Використання штучного інтелекту в адмініструванні виборів»* (Стокгольм: International IDEA, 2024), <https://doi.org/10.31752/idea.2024.31>

Т. Мадієга, *«Акт про цифрові послуги»,* Дослідницька служба Європейського парламенту, документ PE 689.357, листопад 2022 р., <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689357/EPRS_BRI(2021)689357_EN.pdf>, дата перегляду: 1 квітня 2025 р.

Е. Массе, *«П'ять років реалізації GDPR у ЄС: успіхи правозастосування»,* Access Now, травень 2023 р., <https://www.accessnow.org/GDPR-5-years>, дата перегляду: 31 березня 2025 р.

Г. Мільдебрат, *«Аналіз щойно запропонованих правил для посилення правозаст осування GDPR у розгляді транскордонних справ»,* Європейський парламент, документ PE 757.613, квітень 2024 р., <https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/757613/EPRS_BRI%282024%29757613_EN.pdf>, дата перегляду: 1 квітня 2025 р.

С. Монтелеоне, *«Штучний інтелект, захист даних та вибори»,* Дослідницька служба Європейського парламенту, документ PE 637.952, травень 2019 р., <https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637952/EPRS_ATA%282019%29637952_EN.pdf>, дата перегляду: 1 квітня 2025 р.

Л. Мустерт, *«Ефективність та процедурний захист у транскордонному застосуванні GDPR»*, EU Law Enforcement, 31 грудня 2023 р., <https://eulawenforcement.com/?p=8739>, дата перегляду: 27 березня 2025 р.

Г. Нетсон, *«Оцінка діяльності координаторів цифрових послуг в ЄС щодо ресурсного забезпечення та готовності до змін»,* Tech Policy Press, 28 травня 2024 р., <https://www.techpolicy.press/assessing-the-eus-digital-services-coordinators-on-resourcing-and-readiness>, дата перегляду: 30 березня 2025 р.

І. Ненадіч та Е. Брогі, *«Чому ЗМІ потребують гарантій, забезпечених Ст аттею 17 Європейського закону про свободу ЗМІ»,* Центр плюралізму та свободи ЗМІ, 16 листопада 2023 р., <https://cmpf.eui.eu/why-news-media-need-article-17-of-the-european-media-freedom-act>, дата перегляду: 1 квітня 2025 р.

«Настільна гра: роль органів влади в узгодженні Акту про цифрові послуги та Закону про свободу ЗМІ для захисту вільних медіа», Медійне законодавство: право і регулювання ЗМІ у порівняльній перспективі, 28 серпня 2024 р., <https://www.medialaws.eu/the-game-of-boards-the-role-of-authorities-in-concerting-the-digital-services-act-and-the-media-freedom-act-for-protecting-media-freedom>, доступ 1 квітня 2025 р.

NIS Cooperation Group (координаційна група, створена в Європейському Союзі згідно з Директивою про кібербезпеку), *«Компендіум з кібербезпеки та стійкості виборів»,* останнє оновлення 2024 р., <https://ec.europa.eu/newsroom/dae/redirection/document/103148>, доступ 1 квітня 2025 р.

Організація економічного співробітництва та розвитку (ОЕСР), *«Огляд принципів ОЕСР щодо використання штучного інтелекту»,* [без дати], <https://oecd.ai/en/ai-principles>, дата перегляду: 1 квітня 2025 р.

Організація з безпеки та співробітництва в Європі (ОБСЄ), Бюро з демократичних інститутів і прав людини (БДІПЛ), *«Угорщина, парламентські вибори та референдум,*

3 квітня 2022 року: Заключний звіт місії спостереження за виборами», 29 липня 2022 р., <https://www.osce.org/odihr/elections/523568>, дата перегляду: 8 жовтня 2025 р.

А. Рабіч та С. Калабрезе, *«Акт ЄС про штучний інтелект та його вплив на виборчі процеси: підхід, заснований на правах людини»,* Європейське партнерство за демократію та спостереження за виборами, вересень 2024 р., <https://epd.eu/content/uploads/2024/09/AI-and-elections.pdf>, дата перегляду: 1 квітня 2025 р.

О. Райх та С. Калабрезе, *«Громадський дискурс та виборчі процеси у звітах про оцінку ризиків та заходи щодо їх пом'якшення відповідно до Акту про цифрові послуги»,* Європейське партнерство за демократію та Союз громадянських свобод Європи, березень 2025 р., <https://www.liberties.eu/f/ielo4z>, дата перегляду: 1 квітня 2025 р.

Р. Тіньєр, *«Застосування прецедентного права ЄСПЛ Європейським Судом: інструменталізація чи прагнення автономії та легітимності?», European Papers*, 8/1 (2023), с. 323–30, <https://doi.org/10.15166/2499-8249/654>

С. Ван дер Стаак та П. Вольф, «*Кібербезпека під час виборів: моделі міжвідомчої взаємодії*» (Стокгольм: International IDEA, 2019), <https://doi.org/10.31752/idea.2019.23>

М. Веале та Ф.З. Боргезіус, *«Розвінчання міфів про проєкт Акту ЄС про штучний інтелект: аналіз позитивних, негативних та невизначених елементів запропонованого підходу»,* Computer Law Review International, 22/4 (2021), с. 97–112, <https://doi.org/10.9785/cri-2021-220402>

VIGINUM, *«Маніпулювання алгоритмами та інструментальне використання інфлюенсерів: уроки президентських виборів у Румунії та ризики для Франції»,* лютий 2025 р., <https://www.sgdsn.gouv.fr/files/files/Publications/20250204_NP_SGDSN_VIGINUM_Rapport_public_Elections_roumanie_risques_france_VFF.pdf>, дата перегляду: 16 серпня

З. Ванат, *«Польське голосування поштою викликає занепокоєння щодо збереження конфіденційності даних»,* POLITICO, 24 квітня 2020 р., <https://www.politico.eu/article/polish-postal-vote-raises-data-privacy-concerns>, дата перегляду: 30 березня 2025 р.

П. Вольф, А. Алім, Б. Касаро, М. Санім, П. Намугера та Т. Зорігт, *Впровадження біометричних технологій у виборах* (Стокгольм: International IDEA, 2017), <https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf>, дата перегляду: 1 квітня 2025 р.

Про авторів

Себастіан Бекер Кастелларо, асоційований координатор програми з питань цифровізації та демократії в International IDEA. Основні сфери експертизи: вплив технологій на демократії в усьому світі, проведення досліджень, аналіз політики та проєктна діяльність. Має ступінь магістра міжнародного права Брюссельського вільного університету та ступінь магістра публічного права Чилійського університету.

Гладіола Ллеші, асоційована координаторка проєктів, що реалізуються International IDEA в рамках Регіональної програми для Європи. Основні сфери експертизи: правова система ЄС у сфері цифровізації та розширення, зокрема впливи новітніх технологій на виборчі процеси. Раніше працювала в Європейському органі з питань страхування та професійних пенсій, спеціалізуючись на ключових регуляторних рамках ЄС щодо штучного інтелекту та у більш широкому правовому ландшафті цифровізації.

Юліане Мюллер, асоційована координаторка проєкту, що реалізується у рамках програми з питань цифровізації та демократії в International IDEA. Основні сфери експертизи: наслідки впровадження новітніх технологій, зокрема штучного інтелекту, для демократії з фокусом на правах людини та цілісності виборчого процесу. Наразі її робота зосереджена на реалізації глобальної ініціативи з розбудови потенціалу в галузі штучного інтелекту для ОАВ, включно з дослідженнями та аналізом політик. Має ступінь магістра міжнародного права Единбурзького університету та ступінь бакалавра права Манхаймського університету.

Про International IDEA

Міжнародний інститут демократії та сприяння виборам (International IDEA) — це міжурядова організація з 35 державами-членами, заснована в 1995 році з метою підтримки сталої демократії в усьому світі.

ЩО МИ РОБИМО

Ми розробляємо сприятливі для політики дослідження, пов'язані з виборами, парламентами, конституціями, диджиталізацією, зміною клімату, інклюзивністю та політичним представництвом, і все це під егідою Цілей сталого розвитку ООН. Ми оцінюємо стан демократії в усьому світі за допомогою наших унікальних Глобальних індексів стану демократії та Демократичного трекера.

Ми забезпечуємо розвиток потенціалу та надаємо експертні консультації демократичним суб'єктам, включаючи уряди, парламенти, виборчі комісії та громадянське суспільство. Ми розробляємо інструменти та публікуємо бази даних, книги та посібники кількома мовами на різні теми — від явки виборців до гендерних квот.

Ми об'єднуємо державні та недержавні суб'єкти для діалогу та обміну досвідом. Ми виступаємо і висловлюємо свою позицію, щоб просувати та захищати демократію в усьому світі.

ДЕ МИ ПРАЦЮЄМО

Наш головний офіс розташований у Стокгольмі, а регіональні та національні представництва — в Африці та Західній Азії, Азії та Тихоокеанському регіоні, Європі, Латинській Америці та Карибському басейні. International IDEA є постійним спостерігачем при Організації Об'єднаних Націй та акредитована при установах Європейського Союзу.

НАШІ ПУБЛІКАЦІЇ ТА БАЗИ ДАНИХ

На нашому сайті є каталог з більш ніж 1 000 публікаціями та понад 25 базами даних. Більшість наших публікацій можна завантажити безкоштовно.

<https://www.idea.int>

International IDEA
Strömsborg
SE-103 34 Stockholm
SWEDEN
+46 8 698 37 00
info@idea.int
www.idea.int

У звіті представлений аналіз європейської нормативно-правової системи у сфері цифровізації та її впливу на цілісність виборів. За допомогою комплексного підходу розглядається чинна та перспективна спроможність нових регламентів ЄС врегулювати основні виклики для наших (цифрових) демократій: загрози належному захисту персональних даних, кібератаки, модерація контенту, гендерне насильство в Інтернеті, використання штучного інтелекту в управлінні виборами, виборчі онлайн-кампанії та використання створеного з використанням ШІ контенту під час виборів.

Хоча організація виборів залишається суверенною справою європейських держав-членів, виборчі органи мають розробити механізми для ефективної взаємодії з відповідними союзними органами для належного реагування на цифрові загрози. Цей звіт закликає усі зацікавлені сторони у виборах сприяти впровадженню нового цифрового регламенту ЄС через посилення міжвідомчої взаємодії для обміну досвідом та можливостями між ОАВ та відповідними регуляторами ЄС,

ISBN: 978-91-8137-130-7 (PDF)