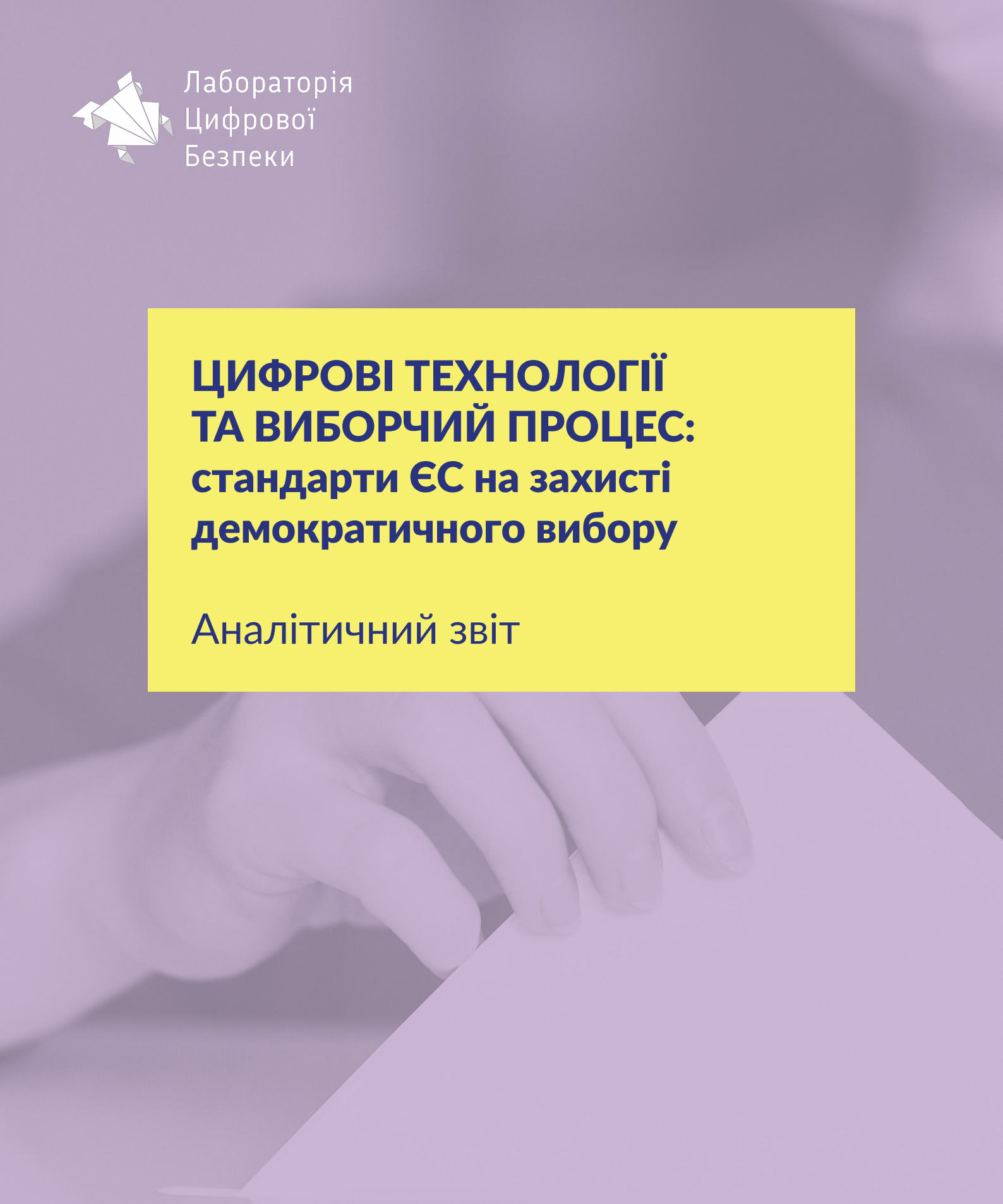
Лабораторія
Цифрової
Безпеки

ЦИФРОВІ ТЕХНОЛОГІЇ ТА ВИБОРЧИЙ ПРОЦЕС: стандарти ЄС на захисті демократичного вибору

Аналітичний звіт



За підтримки

ПРЯМУЄМО РАЗОМ

МІЖНАРОДНИЙ ФОНД ВІДРОДЖЕННЯ

Цифрові технології та виборчий процес: стандарти ЄС на захисті демократичного вибору. Аналітичний звіт – Київ: ГО «Лабораторія цифрової безпеки», 2022 р.

Автори: Анна Людва, Максим Дворовий
Рецензенти: Сергій Савелій, Віта Володовська

Використання алгоритмів онлайн-платформ для просування дезінформаційних наративів, мікротаргетинг політичної агітації та профілювання виборців, боти та діпфейки – нині невід'ємна частина політичних процесів. Після скандалу з Cambridge Analytica очевидною стала необхідність системної відповіді на нові виклики на найвищому рівні. Провідну роль в цьому процесі взяв на себе Європейський Союз як один із найбільших цифрових ринків. Аналітичний звіт включає огляд законодавства ЄС та окремих держав-членів ЄС у площині протидії загрозам використання цифрових технологій для втручання у виборчі процеси, зокрема, підходів до запровадження прозорості політичної реклами в Інтернеті, встановлення відповідальності за координовану неавтентичну поведінку та інші зловживання. На основі проаналізованих підходів у звіті також окреслено загальні рекомендації для оновлення українського законодавства у відповідь на наявні та потенційні цифрові виклики на шляху держави до інтеграції з ЄС.

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

Європейський Союз складається з 27 держав-членів та їхніх народів. Це унікальне політичне та економічне партнерство, засноване на цінностях поваги до людської гідності, свободи, рівності, верховенства права і прав людини. Понад п'ятдесят років знадобилось для створення зони миру, демократії, стабільності і процвітання на нашому континенті. Водночас нам вдалось зберегти культурне розмаїття, толерантність і свободу особистості. ЄС налаштований поділитись своїми цінностями та досягненнями з країнами-сусідами ЄС, їхніми народами, та з народами з-поза їхніх меж.

Міжнародний фонд «Відродження» – одна з найбільших благодійних фундацій в Україні, що з 1990-го року допомагає розвивати в Україні відкрите суспільство на основі демократичних цінностей. За час своєї діяльності Фонд підтримав близько 20 тисяч проектів, до реалізації яких долучилися понад 60 тисяч активістів та організацій України на суму понад 200 мільйонів доларів США.

Сайт: www.irf.ua
Facebook: www.fb.com/irf.ukraine

Виклики цифрових технологій для демократії

Вплив цифрових технологій на політичні, соціокультурні, економічні відносини у сучасному світі важко переоцінити. Технології сприяють об'єднанню людей під час революцій і протестів проти влади, поширенню важливої суспільної інформації професійними та громадськими журналістами, отриманню освіти чи самореалізації. З іншого боку, можливості технологій так само легко перетворюються на зброю у руках зловмисних акторів.

Використання технологій для прогнозування поведінки користувачів та впливу на неї є предметом численних досліджень та навіть темою популярних документальних фільмів.[1] Не є таємницею, що великі компанії (на кшталт Google, Meta та Apple) постійно збирають та зберігають дані своїх споживачів не лише для цілей маркетингу або реклами, а й задля вдосконалення обслуговування клієнтів та розвитку нових напрямків діяльності як-то створення віртуальної реальності.[2] Наприклад, WhatsApp зберігає номери телефонів, специфікації пристрою, інші дані користувачів та ділиться цією інформацією із компаніями мережі Meta.[3] Facebook на основі цих даних покращує свій маркетинг та бізнес-ефективність, створюючи персоналізований контент та досвід для користувачів.

Персоналізація буденного досвіду взаємодії з платформами дозволяє користувачам легше знаходити контент та товари, які найточніше відповідають їх вподобанням. Проте у масштабах суспільно-політичних процесів на глобальному рівні, на рівні держави чи навіть місцевих громад, така "зручність" може мати неочікувані наслідки, що відображається на результатах волевиявлення.

Наприклад, за результатами референдуму про вихід Великої Британії з ЄС у 2016 році, розрив у голосуванні склав всього 3% (51% – «за» та 48% – «проти»). Дослідники вважають, що така поляризація думок – наслідок активного поширення таргетованої реклами у Facebook як з боку кампаній на підтримку однієї з позицій, так і британських політичних акторів.[4]

Схожі тенденції мали місце і під час президентських виборів у США 2016 року, коли за крісло змагалися Дональд Трамп та Гілларі Клінтон. Вибори назвали найбільш "технологічно просунутими" за всю історію їх проведення.[5] Так, під час виборчої кампанії кандидати активно використовували соціальні мережі – не лише традиційні Twitter та Facebook, а і наприклад, Pinterest, який дозволив Клінтон охопити потрібну цільову аудиторію серед жінок. Крім цього, кандидати залучали технології реєстрації виборців, аналітику великих даних, створювали мобільні застосунки. Все це дозволило командам кандидатів отримати не лише загальні дані про вік, матеріальний стан та культурні особливості потенційних виборців, але і моделювати агітаційні повідомлення на основі інформації про контент, якому надають перевагу користувачі, аналізу їх пошукових запитів та навіть опублікованих ними коментарів.[6]

Результатом обох політичних кампаній стало накопичення приватних даних мільйонів користувачів Facebook без їх згоди для подальшого використання та досі відкриті дискусії щодо легітимності «Брекзиту» і перемоги Трампа на виборах.

[1] URL: https://www.thesocialdilemma.com
[2] URL: https://about.facebook.com/metaverse/
[3] Квач С., Тайхон П., Мартін К.Д. та інші / Цифрові технології: напруження щодо приватності та даних. Журнал Академії маркетингових наук (2022).
URL: https://link.springer.com/article/10.1007/s11747-022-00845-y
[4] Боссетта М., Сегестен А. Д., Тренц Г. / Політична участь у Facebook під час Brexit: чи залучення користувачів на сторінках ЗМІ стимулює залучення до кампаній? Журнал мови та політики 17(2) (2017).
URL:https://www.researchgate.net/publication/321172860_Political_participation_on_Facebook_during_Brexit_Does_user_engagement_on_media_pages_stimulate_engagement_with_campaigns
[5] Фірлей, Миколай. "Три способи, якими технології окреслюють президентську кампанію у США 2016 року". Blavatnik School of Government, 25 жовтня 20 16.
URL:https://www.bsg.ox.ac.uk/blog/three-ways-which-technology-shaping-2016-us-presidential-campaign
[6] "Соціальні мережі, електронна пошта та дані: стратегія цифрових медіа на президентських виборах 2016 року". Upland.
URL:https://uplandsoftware.com/postup/resources/blog/social-email-and-data-the-digital-media-strategy-of-the-2016-presidential-election/

Побудова більш прицільної та ефективної кампанії, що ґрунтується на масивах персональних даних користувачів, очевидно, створює загрози для базових засад свободи волевиявлення. Цей виклик ускладнюється неможливістю належно врегулювати онлайн-інструменти на державному рівні. Так, під час використання традиційних медіа, наприклад, телебачення, політичну рекламу бачить вся виборча аудиторія, на яку транслюється відповідний канал. Така реклама може поширюватися виключно протягом виборчого періоду, передбаченого законом. У випадку порушення правил висвітлення виборів чи агітації, відповідні національні органи можуть швидко відреагувати, відслідкувати замовника та вжити заходів для притягнення його до відповідальності. Заборона на поширення політичної реклами застосовується і до агітації іноземними гравцями.

Онлайн-реклама, на відміну від телевізійної чи опублікованої в друкованих медіа, спрямована на вужчі категорії виборців, тому вона не потраплятиме до новинних стрічок нерелевантних виборців. Онлайн-реклама не має ані кордонів, ані часових обмежень, тому вона може неосяжно розповсюджуватися у будь-який період часу з будь-якого куточка світу. Як наслідок, відслідкувати, яку саме категорію осіб для таргетування було обрано і на основі яких даних, чому та хто оплатив агітацію, практично неможливо, що тільки поглиблює проблему зловживання онлайн-інструментами зі сторони зловмисних гравців.

Описані виклики є надзвичайно актуальними для України. Держава-агресор не припиняє використовувати цифрові технології для поширення дезінформації, пропаганди війни, розпалювання ворожнечі та закликів до проведення псевдореферендумів на тимчасово окупованих територіях. Після початку повномасштабного вторгнення компанія Meta звітувала про низку мереж російських ботів, які цілеспрямовано зловживали механізмами скарг для видалення контенту українських користувачів про війну[7] або ж поширювали повідомлення на підтримку війни Росії в Україні[8]. Можна припустити, що і після закінчення війни існуватиме постійний ризик іноземного втручання у внутрішні політичні процеси.

Попри воєнний стан, що забороняє проведення виборів, досвід попередніх кампаній та нинішні тенденції свідчать про необхідність не зволікати із запровадженням правового регулювання, яке забезпечуватиме прозорість, справедливість та доброчесність виборчого процесу в онлайн-вимірі. З огляду на наданий Україні статус держави-кандидата на вступ до Європейського Союзу, таке законодавство має прийматися з урахуванням чинних міжнародних стандартів та законодавства ЄС щодо цифрових послуг, яке нині активно розвивається.

Аналітичний звіт включає огляд законодавства ЄС та окремих держав-членів Європейського Союзу щодо протидії загрозам використання цифрових технологій для втручання у виборчі процеси, зокрема, підходів до забезпечення прозорості політичної реклами в Інтернеті, встановлення відповідальності за координовану неавтентичну поведінку та інші зловживання. На основі проаналізованих підходів у звіті також окреслено загальні рекомендації для оновлення українського законодавства у відповідь на вже наявні та потенційні цифрові виклики.

[7] Німмо, Бен, Аграновіч, Девід та інші. “Звіт Meta про конкурентні загрози, перший квартал 2022 року”. Meta, 7 квітня 2022. URL: https://about.fb.com/news/2022/04/metas-adversarial-threat-report-q1-2022/

[8] Німмо, Бен, Аграновіч, Девід та інші. “Звіт Meta про конкурентні загрози, другий квартал 2022 року”. Meta, 4 серпня 2022. URL: https://about.fb.com/news/2022/08/metas-adversarial-threat-report-q2-2022/

Підхід Європейського Союзу

Дискусії довкола потреби врегулювати використання цифрових технологій, які можуть зашкодити демократичним процесам, тривають у ЄС вже не перший рік. Ще у березні 2018 року Експертна група щодо фейкових новин та дезінформації висловлювала занепокоєння з огляду на загрози безпеці ЄС через масове поширення неправдивої інформації.[9] Результати тривалих обговорень між експертами та законодавцями знайшли своє відображення у Плані Дій проти Дезінформації.[10] Його було розроблено задля зменшення негативного впливу дезінформації на виборах до Європейського парламенту, що мали відбутися у 2019 році.

Перш за все, документ вказує на загрозу розповсюдження неправдивих відомостей через онлайн-платформи, адже у довгостроковій перспективі це може негативно вплинути на загальне сприйняття інформації громадянами ЄС. Автори документу зосереджують свою увагу також на дезінформаційних кампаніях, проведених третіми країнами. Проявами таких кампаній є гібридні кібератаки та злами мереж. Ці ж тенденції продовжилися у 2020 році під час спалаху COVID-19, коли спостерігалася хвиля кібератак на ЄС з боку Російської Федерації з поширенням дезінформації щодо вірусу, що лише підкреслює важливість адекватного реагування на цей виклик.

У відповідь на поширення подібних тенденцій у 2018 році було прийнято Кодекс ЄС з протидії дезінформації, що заохочує до прозорості політичної реклами та закриття фейкових акаунтів, які поширюють неправдиві свідчення або викривлену інформацію.[11] Варто зауважити, що у 2022 році Кодекс було оновлено: його положення додатково встановлюють більш чіткі вимоги до прозорості політичної реклами та заохочують постійну роботу спільнот, які здійснюють фактчекінг. Завдяки появі попереджувального маркування, що ідентифікує дезінформацію, користувачі отримують можливість розуміти, що взаємодіють із потенційно неправомірним контентом.

Паралельно з цим унаочнилася потреба не лише у боротьбі з онлайн-дезінформацією, а й необхідність протидіяти іншим зловживанням цифровими технологіями, що ставлять під загрозу справедливість та відкритість виборів.[12] З розвитком нових технологій все більше політичних гравців пристосували свої агітаційні кампанії до використання Інтернету, позбавивши ЄС можливості відслідковувати шляхи фінансування політичної агітації та притягувати до відповідальності винних у разі виявлення порушення. Про це йдеться у Плані дій щодо Європейської демократії.[13]

Особлива увага в документі зосереджена на небезпеці маніпулювання виборцями, до чого вдаються політичні актори, щоб отримати результати голосування на свою користь. Автори Плану дій наголошують, що завдяки цифровим інструментам з'явилася можливість поєднати персональні дані та штучний інтелект, створивши техніку мікротаргетингу і психологічного профілювання. Таким чином, передвиборна агітація націлюється на виборця, використовуючи його особисту інформацію та часто нав'язуючи суперечливі наративи. Зокрема, різним аудиторіям від одного й того ж замовника політичної реклами можуть надходити протилежні меседжі, які переконуватимуть виборців, що саме цей замовник є виразником та захисником їх інтересів.

Таке маніпулювання публічною думкою порушує основні принципи виборів, що полягають у відкритих дебатах, вільному виборі та плюралізмі думок. У зв'язку з поширенням цифрових

[9] Боротьба з дезінформацією в Інтернеті: експертна група виступає за більшу прозорість між онлайн-платформами. Прес-реліз Європейської комісії від 12 березня 2018 року. URL:https://ec.europa.eu/commission/presscorner/detail/en/ip_18_1746

[10] План дій проти Дезінформації. Спільна комунікація до Європейського парламенту, Європейської ради, Європейського економічного та соціального комітету і комітету регіонів від 5 грудня 2018 року. URL:https://www.eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf

[11] Кодекс ЄС про протидію дезінформації від 26 вересня 2018 року. URL: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454

[12] Стан Союзу 2018: Європейська комісія пропонує заходи для забезпечення вільних і чесних виборів до Європейського Союзу. Прес-реліз Європейської комісії від 12 вересня 2018 року. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_18_5681

[13] План дій щодо Європейської демократії. Комунікація Комісії до Європейського парламенту, Європейської ради, Європейського економічного та соціального комітету і комітету регіонів від 3 грудня 2020 року. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0790&from=EN

технологій в електоральному полі, виникла потреба у належному правовому регулюванні, яке забезпечило б чесні вибори та активну демократичну участь, а також сприяло б протидії дезінформації.

У 2020 році було опубліковано Проєкт Акту про цифрові послуги – документ, що найбільш широко та детально регулює цифрові послуги онлайн-платформ.[14] Зокрема, проєкт покладає обов'язки на онлайн-платформи та посередників, що надають послуги хостингу, і зобов'язує їх видаляти протиправний контент у разі його виявлення. Передбачаються також вимоги до прозорого звітування онлайн-платформ, згідно з якими слід надавати інформацію про кількість повідомлень, судових наказів та скарг щодо виявленого протиправного контенту.

Вже за рік було опубліковано Проєкт Регламенту Європейського парламенту та Ради щодо прозорості та таргетування політичної реклами.[15] Він містить низку правил правомірного таргетування аудиторії онлайн-платформами, а також акцентує увагу на вимогах до прозорості та правової визначеності політичної реклами.

У 2022 році держави-члени ЄС, США та низка інших країн, включно з Україною, підписали Декларацію про майбутнє Інтернету для забезпечення використання цифрових технологій з метою посилення, а не послаблення демократії та поваги до прав людини.[16] Згідно з Декларацією, урядам, органам влади та звичайним користувачам слід "утримуватися від використання Інтернету для підриву виборчої інфраструктури, виборів та політичних процесів, у тому числі шляхом прихованих інформаційних маніпуляцій".

У сфері регулювання цифрових технологій нещодавно також було прийнято низку рекомендацій Ради Європи. Як відомо, ЄС регулярно посилається на стандарти та принципи Ради Європи під час підготовки власних нормативних документів,[17] а їх дія поширюється на всі держави-члени ЄС, які одночасно входять до Ради Європи. Серед релевантних документів варто згадати Рекомендації CM/Rec(2022)12 Комітету міністрів державам-членам щодо виборчої комунікації та висвітлення виборчих процесів у ЗМІ, які встановлюють окремі вимоги до публікації матеріалів передвиборної агітації, а також до прозорості при використанні алгоритмічних систем та технік мікротаргетингу.[18] У свою чергу, Рекомендації CM/Rec(2020)1 Комітету міністрів державам-членам про вплив алгоритмічних систем на права людини містять стандарти та обмеження, спрямовані на зменшення негативного впливу цифрових технологій на повсякденне життя людей.[19]

Отже, сьогодні формування та уніфікація законодавства про використання цифрових технологій у виборчому контексті лише починається. Наразі можемо спостерігати створення ініціатив, що концентруються на регулюванні правил використання окремих практик у виборчих процесах.

Як вбачається з підходу Європейського Союзу, регулювання поки що відбувається здебільшого за допомогою рекомендацій, встановлення орієнтирів та керівних принципів, що часто не є обов'язковими до виконання. Втім, такі документи містять базові положення та правила, котрі національні країни повинні враховувати при зміні внутрішнього законодавства.

---

[14] Проєкт Регламенту Європейського парламенту та Ради щодо єдиного ринку цифрових послуг (Акт про цифрові послуги) та внесення змін до Директиви 2000/31/ЄС від 15 грудня 2020 року.
URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&from=en

[15] Проєкт Регламенту Європейського парламенту та Ради щодо прозорості та таргетування політичної реклами від 25 листопада 2021 року.
URL: https://ec.europa.eu/info/sites/default/files/2_1_177489_pol-ads_en.pdf

[16] Декларація про майбутнє Інтернету від 28 квітня 2022 року.
URL: https://digital-strategy.ec.europa.eu/en/library/declaration-future-internet

[17] "Рада Європи та Європейський Союз: різні ролі, спільні цінності". Рада Європи та Європейський Союз. URL: https://www.coe.int/en/web/portal/european-union

[18] Рекомендації CM/Rec(2022)12 Комітету міністрів державам-членам щодо виборчої комунікації та висвітлення виборчих кампаній у ЗМІ від 6 квітня 2022 року.
URL: https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a6172e

[19] Рекомендації CM/Rec(2020)1 Комітету міністрів державам-членам про вплив алгоритмічних систем на права людини від 8 квітня 2020 року.
URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016809e1154

Після системного аналізу документів на рівні Європейського Союзу, можемо виділити низку основних тактик, що використовуються для маніпулювання громадською думкою та розглядаються Євросоюзом у якості загроз доброчесності виборчих процесів:

- **поширення дезінформації** – неправдивої інформації, що свідомо (та часто приховано) має на меті вплив на громадську думку або приховування правди;
- **координована неавтентична поведінка** – створення мереж облікових записів або сторінок, які працюють, щоб ввести в оману публіку для досягнення специфічної мети;
- **створення і використання діпфейків** – фіктивного відеоконтенту, що неправдиво відображає висловлювання відомих осіб;
- **зловживання політичною рекламою** – поширення неідентифікованих повідомлень, що промотують певну політичну позицію чи кандидата та здатні впливати на результати виборів чи референдумів, законодавчий чи нормативний процес або поведінку при голосуванні;
- **мікротаргетинг** – використання даних користувачів для виявлення їхніх інтересів з метою впливу на думку, поведінку або ставлення;
- **зловживання алгоритмами онлайн-платформ** – маніпуляція публічною думкою через використання можливостей, що їх надають соцмережі;
- **маніпулятивні опитування**, а також хибні інтерпретації результатів опитувань та умисні помилки при презентації даних.

Дезінформація у виборчому процесі

У межах Європейського Союзу дезінформація визначається як неправдива або оманлива інформація, що створена, представлена та поширена з метою отримання економічної вигоди або навмисного введення в оману громадськості, та може завдати публічної шкоди.[20]

У 2018 році Європейська Комісія у своїй Комунікації "Боротьба з дезінформацією в Інтернеті: європейський підхід" наголосила на необхідності розробки правового регулювання протидії дезінформації.[21] Очевидно, що стрімкий розвиток онлайн-платформ та, як наслідок, звернення до онлайн-новин як основного джерела інформації, суттєво сприяє швидкому поширенню дезінформації. Техніки націлювання (таргетингу) та координована поведінка (наприклад, використання ботів) надають можливість розповсюджувати недостовірні відомості з нечуваною швидкістю, впливаючи на свідомий вибір користувачів та їх здатність до прийняття інформованих рішень. Таким чином, перед національними законотворцями з'явилося надскладне завдання: зберегти баланс між забороною цензури і втручання у плюралізм свободи вираження думок та потребою обмежити поширення шкідливого контенту, що містить дезінформацію. Саме у Комунікаціях були вперше окреслені способи боротьби з дезінформаційними кампаніями. Серед пропозицій містилися: підвищення прозорості, надійності та підзвітності онлайн-платформ, а також організація безпечніших та стійкіших виборчих процесів. Держави-члени ЄС мали б імплементувати відповідні вимоги у національне законодавство для забезпечення достовірності інформації, що використовується для впливу на суспільну думку під час виборчих процесів.

Перший проєкт Кодексу практики щодо онлайн-дезінформації спирався на цілі та завдання, проголошені у Комунікаціях, а саме: прозорість наданої інформації та забезпечення надійної і доброчесної передвиборної агітації під час виборів до Європарламенту у 2019 році.[22] Проєкт передбачав правила розміщення політичної реклами задля отримання лише достовірних свідчень про кандидатів, а також прозорості діяльності онлайн-платформ під час розповсюдження інформації. Однак більш детальні правила щодо запобігання поширенню дезінформації Європейська комісія презентувала у вересні 2018 року у вигляді Кодексу ЄС з протидії

[20] Боротьба з дезінформацією в Інтернеті: європейський підхід. Комунікація Комісії до Європейського парламенту, Ради, Європейського економічного та соціального комітету і комітету регіонів від 26 квітня 2018 року.
URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0236&from=EN

[21] Там само

[22] Драфт Кодексу ЄС щодо протидії дезінформації.
URL:https://ec.europa.eu/information_society/newsroom/image/document/2018-29/msf_on_disinformation_17_07_2018_-_proofread_99F78DB7-9133-1655-990805803CDCCB67_53545.pdf

дезінформації. Його підписали найбільші технологічні компанії задля встановлення зобов'язуючих правил.[23] Серед першочергових підписантів були Facebook (у тому числі Instagram), Google (у тому числі YouTube), Mozilla та Twitter.

Кодекс містить зобов'язання підписантів щодо забезпечення прозорості політичної та тематичної реклами, підвищення активності боротьби із поширенням фейкових акаунтів, протидії ботам та пріоритезації достовірної інформації у новинній стрічці. Одним із основних завдань Кодексу є пріоритезація прозорості та створення надійних індикаторів фактчекінгу, аби у користувачів була можливість отримувати виключно релевантну та верифіковану інформацію у своїй стрічці. При цьому Кодекс заохочує співпрацю підписантів з державами-членами для забезпечення доброчесності виборчої інфраструктури від кібератак.

Зі звітів Європейської комісії вбачається, що прийняття Кодексу справило позитивний вплив на виборчий процес.[24] Відповідно до звітів соціальних мереж (як-от Facebook, Google та Twitter), напередодні виборів онлайн-платформи виявили та видалили понад 600 сторінок та груп, які поширювали дезінформацію та мову ворожнечі навіть після маркування таких матеріалів як політичної реклами. Більше того, було виявлено додаткові випадки широкомасштабних спроб маніпулювати поведінкою під час голосування щонайменше у 9 державах-членах.

Проте маніпулювання інформацією виявилося не єдиною проблемою після прийняття Кодексу. Оцінка ефективності впровадження Кодексу ЄС з протидії дезінформації від Комісії, проведена у 2020 році, продемонструвала наявні прогалини та недоліки чинного Кодексу.[25] Так, на момент оцінки все ще існувала потреба в уточненні процедур прозорості та зобов'язань онлайн-платформ. Основна проблематика була пов'язана зі звітністю онлайн-платформ: через ненадання останніми доступу до релевантних даних, незалежні дослідники були позбавлені можливості моніторити нові тенденції та загрози онлайн-дезінформації. У зв'язку з цим постала потреба у створенні більш структурованої моделі співпраці між дослідницькою спільнотою та онлайн-платформами.

У 2021 році було запущено процес посилення ефективності механізмів Кодексу у зв'язку з прогалинами у регулюванні. Тривалі обговорення представників сторін-підписантів були відображені у Вказівках для посилення Кодексу практики щодо дезінформації.[26] У Вказівках запропоновано покращити процес демонетизації дезінформації, якість звітності онлайн-платформ на національному рівні, а також індивідуальну оцінку впроваджених правил. Крім того, пропонується надати більше можливостей користувачам для реагування на потенційно протиправний контент та удосконалити процедури фактчекінгу.

Пізніше всі пропозиції були імплементовані у Посилений Кодекс ЄС щодо протидії дезінформації від 2022 року.[27] Дублюючи положення від 2018 року, новий Кодекс встановлює чіткішу процедуру звітування для онлайн-платформ, а також деталізує деякі правила щодо прозорості політичної реклами, співпраці зі спільнотами, що здійснюють фактчекінг, а також надання доступу до інформації для дослідників.

[23] Кодекс ЄС щодо протидії дезінформації від 26 вересня 2018 року.
URL: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454

[24] Звіт про виконання Плану дій проти дезінформації. Спільна комунікація до Європейського парламенту, Європейської ради, Європейського економічного та соціального комітету і комітету регіонів від 14 червня 2019 року.
URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019JC0012&rid=8

[25] Оцінка Кодексу практики щодо дезінформації – досягнення та сфери для подальшого вдосконалення. Робочий документ Комісії від 10 вересня 2020 року.
URL:https://digital-strategy.ec.europa.eu/en/library/assessment-code-practice-disinformation-achievements-and-areas-further-improvement

[26] Вказівки Європейської комісії щодо посилення Кодексу практики щодо дезінформації 26 травня 2021 року.
URL: https://digital-strategy.ec.europa.eu/en/library/guidance-strengthening-code-practice-disinformation

[27] Посилений Кодекс ЄС щодо протидії дезінформації від 16 червня 2022 року.
URL: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation

Перш за все, Кодекс віднині поширюється не лише на великі онлайн-платформи, але й на інших гравців: рекламні агентства, компанії, що займаються рекламними технологіями та вибором рекламного простору, а також органи, які беруть участь у сертифікації рекламних послуг. При розміщенні політичної реклами забороняється отримання будь-якої грошової винагороди у випадку поширення дезінформації в рамках такої реклами.

У контексті демонетизації підписантам слід розробити внутрішні політики перегляду контенту ("content review"), що публікується для рекламних цілей, з метою відслідковування зловмисних гравців, що поширюють дезінформацію. У випадку купівлі політичної реклами підписанти повинні розміщувати таку рекламу виключно через тих рекламодавців, котрі вживають всіх прозорих заходів, аби не публікувати рекламний контент поряд з дезінформацією. Крім того, підписанти, що здійснюють звітування щодо монетизації, повинні вжити технічних заходів, аби надавати всі комерційно прийнятні та достовірні дані незалежним стороннім аудиторам.

Своєю чергою, користувачі отримують більше інструментів для розпізнавання дезінформації. Наприклад, спеціальні позначення на політичній рекламі даватимуть можливість розпізнати платний контент та одразу ідентифікувати політичну рекламу. Таке позначення може також містити інформацію про осіб, які замовили розміщення відповідного контенту.

Для забезпечення прозорості, користувачі отримуватимуть інформацію про політичну або будь-яку тематичну рекламу, яку вони бачитимуть у мережі. Така інформація міститиме дані про особу, що оплатила рекламу, період показу, витрати на рекламу та зведену інформацію про отримувачів оголошення. Чіткою, простою і зрозумілою мовою буде пояснюватися, чому користувачі бачать рекламу у своїй стрічці та які інструменти було використано (географічні, демографічні дані тощо), аби саме ця реклама відображалась у соцмережі.

Дослідницьким спільнотам має надаватися кращий доступ до баз даних платформ, що міститимуть деперсоналізовані та анонімізовані, зведені або явно оприлюднені дані. Такий доступ надається винятково для досліджень з метою відслідковування вжитих заходів та тенденцій для віднайдення ефективної стратегії боротьби з дезінформацією. Прикметно, що доступ до даних надається лише на некомерційній основі. Кодекс не поширює це положення на державні та правоохоронні органи. В рамках дослідження дезінформації надається відкритий доступ до контенту, який було розміщено відповідними онлайн-платформами разом із розумними запобіжними заходами для усунення ризиків зловживань. Надана інформація може також включати облікові записи публічних діячів (наприклад, обраних посадовців), новинні видання та державні облікові записи урядів.

Крім того, розширюється простір для діяльності організацій з фактчекінгу (перевірки достовірності фактів): підписантам слід встановити чітку та регулярну співпрацю з фактчекерськими спільнотами, особливо у тих державах-членах ЄС, де механізму фактчекінгу ще не запроваджено. При здійсненні фактчекінгу в сервісах онлайн-платформ, цей механізм додатково повинен застосовуватися у системах, що програмують рекламу, та у відеоконтенті.

Кодекс також встановлює процедуру моніторингу виконання положень Кодексу з боку підписантів шляхом аналізу отриманих звітів та індивідуальної оцінки власних зобов'язань підписантами. Таким чином, моніторинг дозволяє забезпечити ефективну імплементацію Кодексу по всій території ЄС.

Очевидно, що поява міжнародних стандартів боротьби з дезінформацією супроводжувалася низкою законодавчих ініціатив для протидії цьому явищу на національному рівні. Прикметно, що Кодекс ЄС не встановлює стандартів відповідальності за дезінформацію, а виключно передбачає низку правил, до яких мають вдатися платформи задля запобігання її поширенню.

У Спільній заяві про свободу вираження думки та "фейкові новини", дезінформацію та пропаганду Спеціального доповідача ООН з питань свободи думки і вираження поглядів та його колег з ОБСЄ, Організації Американських Держав та Африканської комісії з прав людини та народів, проголошується, що "кримінальне законодавство про дифамацію є надмірно обмежуючим і має бути скасовано.

Правила цивільного законодавства про відповідальність за неправдиві та наклепницькі твердження є законними, лише якщо відповідачі за повної можливості не можуть довести правдивість цих заяв, а також отримання вигоди від інших засобів захисту, таких як чесний коментар".[28]

На жаль, на практиці трапляються випадки повної криміналізації діяння, що виглядає найпростішим способом протидії дезінформації. Через те, що під термін "дезінформація" потрапляє різний контент, така жорстока заборона несе ризики свавільного обмеження свободи вираження поглядів. Яскравим прикладом цього є Угорщина, законодавство якої передбачало покарання у вигляді 5 років ув'язнення за розповсюдження фейкових новин про боротьбу держави з COVID-19.[29] Таким чином, під приводом боротьби з пандемією було запроваджено сувору систему цензури, що підірвала незалежність медіапростору.

Практика окремих держав демонструє декілька спроб врегулювання цієї тактики впливу на вибори на національному рівні. До прикладу, слід згадати закон Франції про боротьбу з маніпулюванням інформацією.[30] Згідно з його положеннями, французькі суди володіють дискрецією щодо обмеження поширення фейкових новин протягом виборчого періоду, якщо вони широкомасштабно розповсюджуються та можуть негативно вплинути на результат виборів.[31] Закон також встановлює обов'язок онлайн-платформ до кооперації задля спільної боротьби з дезінформацією та фейковими новинами. Своєю чергою, за виконанням зазначених правил слідкує Аудіовізуальна рада Франції.[32] Вищезгаданий закон зазнав різкої критики, а французьку владу звинувачували у створенні так званої "поліції думок" ("thought police"), що може цензурувати будь-який контент, який їй не подобається.[33]

В Італії немає спеціального закону про протидію дезінформації. Водночас, під час виборчої кампанії 2018 року існував Протокол дій щодо боротьби з розповсюдженням фейкових новин у мережі, затверджений Міністерством внутрішніх справ Італії.[34] Згідно з регуляторним документом, користувачі мали змогу повідомляти про недостовірні або неправдиві відомості через спеціальний Інтернет-портал, а поліція отримала повноваження здійснювати перевірку "фейкових новин". Лише поліція визначала, яка інформація є упередженою, необґрунтованою або дифамаційною, а також притягувала до відповідальності, якщо така інформація порушує публічний порядок. Очевидно, що такий протокол є проблемним через надання дискреційних повноважень поліції щодо закриття сайтів у разі, якщо інформацію визнають неправдивою. Втім, після виборів 2018 року відповідний портал перестав працювати, а такі вимоги щодо фактчекінгу не застосовувалися. Згадані зауваження до регуляцій є більш ніж доречними, тому законодавцям слід належним чином аналізувати повноваження, надані спеціальним органам з протидії дезінформації під час виборчого процесу, аби уникнути свавільного обмеження свободи вираження поглядів з боку медіа.

[28] "Спільна заява про свободу вираження думки та "фейкові новини", дезінформацію та пропаганду". ООН, 3 травня 2017, Твердження 2(b).
URL:https://www.ohchr.org/en/press-releases/2017/03/freedom-expression-monitors-issue-joint-declaration-fake-news-disinformation

[29] Волкер, Шон. "Угорські журналісти побоюються, що закон про коронавірус може бути використаний для їхнього ув'язнення". The Guardian, 3 квітня 2020.
URL:https://www.theguardian.com/world/2020/apr/03/hungarian-journalists-fear-coronavirus-law-may-be-used-to-jail-them

[30] Закон Франції про боротьбу з маніпулюванням інформацією № 2018-1202 від 22 грудня 2018 року.
URL: https://www.legifrance.gouv.fr/eli/loi/2018/12/22/MICX1808389L/jo/texte

[31] Закон Франції про боротьбу з маніпулюванням інформацією № 2018-1202 від 22 грудня 2018 року, стаття 1(2).
URL: https://www.legifrance.gouv.fr/eli/loi/2018/12/22/MICX1808389L/jo/texte

[32] Рекомендація Вищої аудіовізуальної ради Франції операторам онлайн-платформ як частина обов'язку співпраці в боротьбі з поширенням неправдивої інформації № 2019-03 від 15 травня 2019 року.
URL:https://www.csa.fr/Reguler/Espace-juridique/Les-textes-adoptes-par-l-Arcom/Les-deliberations-et-recommandations-de-l-Arcom/Recommandations-et-deliberations-du-CSA-relatives-a-d-autres-sujets/Recommandation-n-2019-03-du-15-mai-2019-du-Conseil-superieur-de-l-audiovisuel-aux-operateurs-de-plateforme-en-ligne-dans-le-cadre-du-devoir-de-cooperation-en-matiere-de-lutte-contre-la-diffusion-de-fausses-informations

[33] Фіорентіно, Майкл-Росс. "У Франції ухвалили суперечливий закон про фейкові новини". Euronews, 22 листопада 2018.
URL: https://www.euronews.com/2018/11/22/france-passes-controversial-fake-news-law

[34] Верца Софія "Боротьба з фейковими новинами по-італійськи" / Ресурсний центр свободи медіа в Європі (2018).
URL: https://www.rcmediafreedom.eu/Tools/Legal-Resources/Tackling-fake-news-the-Italian-way

Боти та координована неавтентична поведінка у виборчому процесі

Іншою неправомірною практикою, поширеною під час виборчих кампаній, є використання ботів або систем координованої неавтентичної поведінки ("Coordinated Inauthentic Behaviour"). Ботами називають елементи програмного забезпечення, призначені для автоматизації повторюваних завдань, наприклад, розміщення контенту в Інтернеті. У соціальних мережах боти часто видають себе за справжніх користувачів з метою обдурити як людей, так і алгоритми. Використання ботів є частиною комп'ютеризованої пропаганди ("computational propaganda") – застосування алгоритмів та автоматизованих програмних продуктів, навмисно спрямованих на управління та поширення оманливої інформації у соціальних мережах, а також на імітацію користувачів задля маніпулювання громадською думкою на різних платформах.[35]

Технологічні рішення під час використання ботів є настільки розвинутими, що ті можуть поводитися як справжні люди, засуджуючи або просуваючи інтереси того чи іншого політичного актора. Так звані "політичні боти" створюють ілюзію громадської підтримки певної політичної партії або ідеї. Їх також можуть створювати для роботи над скаргами на правомірний, але некомфортний для замовників контент, використовуючи вразливості онлайн-платформ. Такі боти також можуть використовуватися для поширення протиправного контенту, зокрема спаму та пропаганди. Все це здійснюється під виглядом дій справжнього користувача шляхом розміщення повідомлень та взаємодії з іншими користувачами та контентом. Таким чином, маніпуляції ботів можна спостерігати здебільшого у соцмережах та на інших онлайн-платформах.

Попри те, що практика використання ботів вже не є новою, законодавство на рівні ЄС, покликане врегулювати проблему їх масового використання, все ще знаходиться на стадії формування. Побічно про ботів згадується в окремих документах, проте уніфікованих правил та умов щодо використання координованої неавтентичної поведінки поки що не спостерігається. Основним документом, до якого слід звертатися, залишається Посилений Кодекс ЄС щодо протидії дезінформації від 2022 року. Кодекс зобов'язує підписантів вживати заходів для протидії такій маніпулятивній поведінці, як ампліфікація контенту (збільшення його видимості для користувачів в мережі) за допомогою ботів. Згідно з Кодексом, його підписанти (зокрема й онлайн-платформи) мають розробити та імплементувати чітку політику щодо неприпустимості маніпулятивної поведінки та практик в рамках використання їхніх послуг, яка має базуватися на найновіших даних про поведінку та тактику ботів.[36]

Крім того, про ботів згадується у Рекомендаціях CM/Rec(2022)12 Комітету міністрів державам-членам щодо виборчої комунікації та висвітлення виборчих кампаній у ЗМІ.[37] Документ зобов'язує онлайн-платформи запровадити гарантії достовірності послуг, що мають виключати наявність ботів та фейкових акаунтів. Соцмережі також повинні імплементувати системи прозорості, за якими можна чітко ідентифікувати автоматизовані акаунти та їх дії, аби їх не плутали зі справжньою людською взаємодією в мережі. Такі вимоги спрямовані на уникнення неправильної інтерпретації та умисного розповсюдження дезінформації серед користувачів.

Як вбачається з вищезазначеного, ЄС поки що не встановлює суттєвих правил щодо використання ботів, передаючи ці повноваження на розсуд окремої компанії або онлайн-платформи, з огляду на особливості використання цифрових інструментів в окремих державах-членах. З одного боку, така практика є зрозумілою, адже частота використання ботів в окремих соцмережах є різною, що і зумовлює суворість правил в одному випадку та повну відсутність регулювання – в іншому. З іншого боку, відсутність навіть базових керівних принципів та орієнтирів може негативно вплинути на подальше прийняття законодавства на національному рівні держав-членів ЄС.

[35] Вулі Самуель С., Ховард Філіп Н. "Комп'ютерна пропаганда: політичні партії, політики та політичні маніпуляції у соціальних мережах" (2018) (витяг).
URL: https://canvas.stanford.edu/files/5717559/download?download_frd=1

[36] Посилений Кодекс ЄС щодо протидії дезінформації від 16 червня 2022 року, Твердження 14.1.

[37] Рекомендації CM/Rec(2022)12 Комітету міністрів державам-членам щодо виборчої комунікації та висвітлення виборчих кампаній у ЗМІ від 6 квітня 2022 року.

Таким чином, сьогодні боротьбу з ботами ведуть переважно онлайн-платформи. Серед них найбільш активними у виявленні та видаленні неавтентичного контенту залишаються Facebook, Google та Twitter.[38]

Останні намагаються зменшити негативний вплив ботів, надаючи інформацію про боротьбу з ними у своїх щоквартальних звітах. Останній звіт Meta акцентував увагу на кібершпигунстві, а також російських ботах-тролях, що візуально створювали онлайн-підтримку збройного вторгнення Росії на територію України.[39] Своєю чергою, у Рекомендованих принципах регулювання або законодавства для боротьби з операціями впливу, Facebook наголошує на тому, що держави мають сконцентруватися на підвищенні рівня прозорості політичної реклами, підтримці цифрової грамотності та технічних досліджень координованої поведінки.[40] Відповідні звіти соцмереж, що містять тенденції та розслідування негативної маніпулятивної поведінки, можуть стати у нагоді при написанні законопроєктів про регулювання практики застосування ботів на національному рівні.

Діпфейки у виборчому процесі

Задля просування власних думок, підриву репутації конкурентів та завоювання прихильності виборців, політичні актори часто вдаються до поширення діпфейків. Діпфейки – це техніка синтезу зображень на основі штучного інтелекту, яка передбачає створення підробленого, але дуже реалістичного відеоконтенту, у якому неправильно відображаються слова чи дії політиків та знаменитостей.[41] Фактично йдеться про створення картинки, де відомі люди нібито висловлюються на певну тему, коли насправді такого висловлювання не існує.

Варто зауважити: як форма синтетичних медіа діпфейки мають неабиякі переваги, оскільки застосовуються у різноманітних сферах життя. Зокрема, йдеться про відображення історичних подій в освітній сфері, інсталяцію картин та творів у мистецькій сфері, реконструкцію місця подій у сфері криміналістики.

Втім, такі необмежені цифрові можливості створюють численні випадки зловживань у виборчій сфері. Яскравим прикладом цього слугують кібератаки з Російської Федерації у перші дні війни проти України. Тоді російські агенти опублікували хоч і невдалий, проте діпфейк президента України Володимира Зеленського, який нібито закликав своїх громадян скласти зброю та здатися.[42] Крім того, на практиці часто трапляються випадки діпфейків політичних діячів з присвоєнням непритаманних їм висловлювань та наративів. У таких відео здебільшого зустрічаються заклики до насильства, висловлення радикальних та суперечливих політичних позицій або ж лобіювання інтересів, спрямованих на розпалювання ворожнечі. Такі маніпуляції підривають репутацію політичних акторів, навмисне створюючи їм негативний образ. Таким чином, окреслена практика демонструє чимале поле для зловживань у виборчій сфері.

У технічному плані, при створенні діпфейків застосовують два поширені підходи.[43] За першого підходу, використовуються так звані генеративні змагальні мережі (Generative Adversarial Networks) – алгоритми машинного навчання, що можуть аналізувати набір зображень і створювати нові зі схожим рівнем якості. За допомогою другого підходу, так званий автокодувальник (Autoencoders)

[38] Ханлон Бредлі “Довгий шлях: аналіз зусиль Facebook, Twitter і Google у боротьбі з іноземним втручанням” / Альянс за забезпечення демократії (2018). URL:https://securingdemocracy.gmfus.org/a-long-way-to-go-analyzing-facebook-twitter-and-googles-efforts-to-combat-foreign-interference/

[39] Німмо Бен, Аграновіч Девід та інші. “Щоквартальний звіт про загрозу суперництва”. Meta, 2022. URL:https://about.fb.com/wp-content/uploads/2022/08/Quarterly-Adversarial-Threat-Report-Q2-2022.pdf

[40] Гліхер Натаніель. “Рекомендовані принципи регулювання або законодавства для боротьби з операціями впливу”. Meta, 8 жовтня 2020 року. URL:https://about.fb.com/news/2020/10/recommended-principles-for-regulation-or-legislation-to-combat-influence-operations/

[41] Боротьба з діпфейками в європейській політиці / Європейська парламентська дослідницька служба (2021). URL:https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf

[42] Вейкфілд Джейн. “Діпфейки президентів, які використовувалися у російсько-українській війні”. BBC News, 18 березня 2022. URL: https://www.bbc.com/news/technology-60780142

[43] Боротьба з діпфейками в європейській політиці / Європейська парламентська дослідницька служба (2021).

має змогу "витягнути" інформацію про риси обличчя із зображень та використовувати цю інформацію для створення зображень вже з іншим виразом. При цьому діпфейки можуть набувати різноманітних форм: відео, технології клонування голосу, синтез тексту тощо.

Технологія зміни виразу обличчя на зображеннях відома вже давно, проте особливої популярності вона набула у соціальних мережах, які дозволяють практику використання різних фільтрів та засобів монтування відео. Внаслідок цього створюється враження, що маніпулювання відео та зображеннями тільки заохочується такими гравцями. На це дослідники звернули увагу ще у 2016 році під час чергових президентських виборів у США. Внаслідок експерименту у соцмережах було опубліковано створене алгоритмом аудіо, що імітує голос Дональда Трампа.[44] За результатами експерименту, виборці не лише повірили кожному слову зі штучно створеного запису, а й не змогли відрізнити голос на ньому від достовірного аудіо. Саме тому з'явилися побоювання щодо експлуатації технології діпфейків для впливу на думку виборців. Оскільки використання такої практики все ще залишається неврегульованим, соцмережі з власної ініціативи вживали заходів, щоб запобігти подібним ситуаціям під час виборів у США 2020 року. Так, перед виборами Facebook заявив, що буде моніторити та видаляти відео-діпфейки, аби забезпечити користувачів виключно достовірною інформацією.[45] Twitter запровадив правила, що забороняють користувачам "оманливо ділитися синтетичними або маніпульованими медіа, які можуть завдати шкоди".[46] Своєю чергою, Snapchat та Tiktok ніяк не відреагували на ці заяви, продовжуючи зберігати практику використання діпфейків.[47]

Завдяки технічним заходам соцмереж, наприкінці виборчого періоду великої кількості діпфейків виявлено не було.[48] Водночас альтернативні онлайн-платформи створили майданчик для розміщення контенту, що поширює дезінформацію.[49] Таким чином, поки одні платформи встановлювали обмеження для розміщення певної інформації, інші платформи дозволяли повну маніпуляцію контентом без будь-яких наслідків.

Поширення діпфейків є важливою проблемою з огляду на декілька факторів. По-перше, відсутність правил їх використання у соцмережах створює можливість зловживання такими засобами. По-друге, така неправомірна тактика лише поглиблює проблему дезінформації, оскільки користувачі отримують неправдиві відомості, що можуть вплинути на їх вирішальний вибір на користь того чи іншого кандидата. По-третє, діпфейки порушують право особи на зображення, що є втіленням її права на приватність. Нарешті, використання діпфейків без належного правового регулювання призведе до ще більших маніпуляцій під час майбутніх виборчих кампаній.

Проблема поширення діпфейків вже не раз перебувала на порядку денному експертного середовища. Так, у звіті Європолу та Міжрегіонального науково-дослідного інституту злочинності та правосуддя ООН щодо зловмисного використання та зловживання штучним інтелектом автори вказують на загрозу діпфейків для публічної безпеки у майбутньому та наголошують на необхідності запровадження технічних методів виявлення діпфейків, наприклад, спеціального

---

[44] Браун Раян. "Група проти втручання у вибори робить імітатацію Трампа за допомогою штучного інтелекту, щоб попередити про «діпфейки»". CNBC, 7 грудня 2018. URL:https://www.cnbc.com/2018/12/07/deepfake-ai-trump-impersonator-highlights-election-fake-news-threat.html

[45] Тогох Ізабель. "Facebook бореться з діпфейками, проте лазівки для дезінформації залишаються". Forbes, 7 січня 2020.
URL:https://www.forbes.com/sites/isabeltogoh/2020/01/07/facebook-is-cracking-down-on-deepfakes-but-loopholes-for-disinformation-remain/?sh=2948c29c139d

[46] "Правила побудови на публіці: наш підхід до синтетичних та маніпулятивних ЗМІ". Twitter, 4 лютого 2020.
URL:https://blog.twitter.com/en_us/topics/company/2020/new-approach-to-synthetic-and-manipulated-media

[47] Нунз Майкл. "Snapchat та TikTok використовують відеотехнологію діпфейк, навіть якщо Facebook її уникає". Forbes, 8 січня 2020.
URL:https://www.forbes.com/sites/mnunez/2020/01/08/snapchat-and-tiktok-embrace-deepfake-video-technology-even-as-facebook-shuns-it/?sh=29a70f9e42c0

[48] Гроссман Геррі. "Можливо, діпфейки не перевернули вибори в США 2020 року, але їх день настане". Venture Beat, 1 листопада 2020.
URL:https://venturebeat.com/business/deepfakes-may-not-have-upended-the-2020-u-s-election-but-their-day-is-coming/

[49] Менесес Джоао Паоло "Діпфейки та вибори в США 2020: що (не) відбулося" / CECS (2021.
URL: https://arxiv.org/pdf/2101.09092.pdf

маркування.[50] Альтернативним способом боротьби може бути також застосування блокчейну для верифікації джерела медіа, аби розрізнити надійні медіа та сумнівні канали.

Схожі вимоги щодо маркування (а саме позначення діпфейків як "неоригінальні") висувалися і у Звіті Європейського парламенту щодо штучного інтелекту.[51] Особлива увага була присвячена використанню діпфейків у виборчих цілях. Згідно зі звітом, технології діпфейків можуть використовуватися для шантажу, створення неправдивих новин або для підриву суспільної довіри та впливу на громадський дискурс. Оскільки така практика може дестабілізувати країни, поширювати дезінформацію та впливати на виборчі процеси, з'явилася потреба у її законодавчому регулюванні.

Слід зауважити , що у Європейському Союзі наразі відсутні чіткі регулятивні норми, що застосовуються виключно до діпфейків. З-поміж чинного законодавства варто вказати вищезгаданий Посилений Кодекс ЄС щодо протидії дезінформації 2022 року, що встановлює вимоги прозорості для систем штучного інтелекту, які поширюють згенерований маніпулятивний контент. Підписанти зобов'язані забезпечити користувачів такими технічними заходами, які б відразу попереджали про потенційний діпфейк або ж дозволяли самостійно ідентифікувати такий контент.[52]

Приклади таких заходів відображені у Проєкті Закону про боротьбу з поширенням дезінформації через обмеження технології діпфейків, що був представлений Конгресу США у 2021 році.[53] Задля розпізнавання діпфейку Проєкт зобов'язує його авторів встановлювати цифрові водяні знаки ("digital watermarks") та забезпечувати аудіовізуальне розкриття інформації. У першому випадку відповідний рухомий знак повинен містити інформацію про те, що показаний контент є діпфейком. Своєю чергою, аудіовізуальне розкриття означає відображення хоча б одного твердження про контент, що ідентифікується як діпфейк, у нижній частині відео або зображення. Відповідна інформація повинна бути видима протягом усього періоду тривалості відео або аудіо контенту.

У контексті відповідних положень із Посиленим Кодексом тісно перегукується і Проєкт Акту ЄС щодо штучного інтелекту.[54] Попри те, що Проєкт не концентрується на технічних засобах створення діпфейків, а встановлює лише загальні вимоги до прозорості використання таких технологій, документ все ж таки дає змогу знизити рівень зловживання цією практикою. Це зумовлено тим, що діпфейки є втіленням майбутніх інновацій, але одночасно і високоризикованим інструментом омани, оскільки вони уособлюють конкретну людину. Саме тому Проєкт не акцентує увагу на забороні їх використання, а радше забезпечує користувачів можливістю бути належно проінформованим у випадку виявлення маніпулятивного контенту.

Відповідно до його тексту, "зобов'язання щодо прозорості застосовуватимуться до систем, які:

- Взаємодіють з людьми,
- Використовуються для виявлення емоцій або визначення зв'язку з (соціальними) категоріями на основі біометричних даних, або
- Створюють або маніпулюють контентом ("діпфейки")".[55]

[50] "Зловмисне використання та зловживання штучним інтелектом" / Trend Micro Research / Міжрегіональний науково-дослідний інститут (2020).
URL: https://unicri.it/sites/default/files/2020-11/AI%20MLC.pdf

[51] Звіт про штучний інтелект: питання тлумачення та застосування міжнародного права, оскільки ЄС зачіпає сфери цивільного та військового використання та державної влади поза сферою кримінального правосуддя (2020/2013(INI)) від 4 січня 2021 року.
URL: https://www.europarl.europa.eu/doceo/document/A-9-2021-0001_EN.pdf

[52] Там само, Твердження 15(1).

[53] Проєкт Закону про боротьбу з поширенням дезінформації через обмеження технології діпфейків / H.R.2395 / 4 серпня 2021.
URL: https://www.congress.gov/bill/117th-congress/house-bill/2395/text

[54] Проєкт Регламенту Європейського парламенту та Ради щодо встановлення гармонізованих правил щодо штучного інтелекту (Акт про штучний інтелект) та внесення змін до деяких законодавчих актів Союзу від 21 квітня 2021 року.
URL:https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF

[55] Там само, Розділ 5 (5.2.4).

Одна з норм Проєкту передбачає, що, користувачі системи штучного інтелекту, що згенерували діпфейк, повинні розкривати інформацію про те, що створений контент є діпфейком, тобто штучно створеним та маніпулятивним.[56] Внаслідок поверхневого аналізу положення можна припустити, що використання діпфейків може бути правомірним за умови дотримання вимог прозорості. Проте таке буквальне тлумачення піднімає декілька проблемних питань. По-перше, більшість діпфейків поширюються з невідомих акаунтів, тому незрозуміло, як застосовуватимуться правила щодо прозорості у випадку анонімних користувачів та чи виконуватимуть вони вимоги до маркування. По-друге, Проєкт не зобов'язує держави-члени запроваджувати норми про притягнення до відповідальності у разі невиконання вимог, що підриває гарантії дотримання правил. Тому стає очевидним, що належна реалізація норм буде напряму залежати від держав-членів та їх законодавчої імплементації гармонізованих правил на національному рівні.

Звертаючись до практики європейських держав, слід підкреслити, що наразі національних спеціальних законів щодо боротьби з діпфейками не прийнято. Це випливає з того, що маніпулювання відео або зображеннями передбачає поширення неправдивих чи маніпулятивних відомостей, що є складовою дезінформації. Тому можна припустити, що національні закони або кодекси, котрі забороняють дезінформацію, автоматично можуть поширюватися і на діпфейки. Втім, задля забезпечення правової визначеності, слід чітко вказувати, які з типів маніпуляцій потрапляють під законодавче регулювання.

Зловживання політичною рекламою у виборчому процесі

Найбільш поширеною тактикою впливу на громадську думку та маніпулювання нею залишається використання політичної реклами під час виборчих кампаній.

У Європі лише у 2019 році на політичну онлайн-рекламу було витрачено приблизно 100 мільйонів євро.[57] Широке використання цифрових способів поширення агітації та її транскордонний характер призвели до необхідності розробити гармонізовані стандарти онлайн агітації на рівні ЄС, забезпечивши вільний рух реклами та одночасно високі стандарти її прозорості.

Серед відповідних законодавчих ініціатив варто виокремити Директиву ЄС про приватність та електронні комунікації.[58] Стаття 13 Директиви ("Небажана комунікація") наголошує, що використання електронних засобів з метою прямого маркетингу дозволяється виключно за попередньої згоди підписників. До такої комунікації також належать повідомлення політичного змісту, передані політичними партіями та іншими суб'єктами, залученими до політичного процесу. При відправці відповідного електронного листа має вказуватися як особа відправника, так і мета листа (рекламні послуги). Фактично, вищезгадана стаття обмежує надсилання спаму, у якому не зацікавлений користувач. Таким чином, забезпечується як відносна прозорість при розміщенні реклами, так і збереження конфіденційності змісту повідомлення.

Проєкт Регламенту про повагу до приватного життя та захист персональних даних в електронних комунікаціях, що прийде на заміну вищезгаданій Директиві, доповнює статтю щодо небажаної комунікації.[59] Документ наділяє користувачів правом відмовитися від отримання рекламних послуг та встановлює для цього чітку процедуру. Таке право користувача законодавчо перегукується із Загальним регламентом щодо захисту даних, стаття 7(3) якого передбачає, що особа має право

[56] Там само, стаття 52(3).

[57] Прозорість та таргетування політичної реклами. Оцінка впливу (SWD(2021) 355, SWD(2021) 356 (підсумок)), що супроводжує пропозицію Комісії для Регламенту Європейського парламенту та Ради щодо прозорості та таргетування політичної реклами (COM(2021) 731) [2022].
URL:https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/730305/EPRS_BRI(2022)730305_EN.pdf

[58] Директива 2002/58/ЕС Європейського парламенту та ради від 12 липня 2002 року щодо обробки персональних даних та захисту приватності у секторі електронних комунікацій (Директива про приватність та електронні комунікації) [2002], OJ L 201/37.
URL:https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN

[59] Проєкт Регламенту Європейського парламенту та Ради про повагу до приватного життя та захист персональних даних в електронних комунікаціях та скасування Директиви 2002/58/ЕС (Регламент про приватність та електронні комунікації) від 10 січня 2017 року.
URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0010&from=EN

у будь-який момент відкликати свою згоду на обробку персональних даних.[60] Про це особа повідомляється завчасно, ще до моменту надання такої згоди.

У контексті регулювання політичної реклами слід згадати також Проєкт Акту ЄС про цифрові послуги, що містить окрему статтю 24, присвячену вимогам прозорості до реклами, розміщеної в Інтернеті.[61] Згідно із правилами, що пропонуються Проєктом, при публікації реклами користувачі повинні мати змогу ідентифікувати:

1. Що відображена інформація є рекламою;
2. Фізичну або юридичну особу, від імені якої розміщується реклама;
3. Змістовну інформацію про основні параметри, що використовуються для визначення адресата реклами.

Доповнюючи вищезгаданий Проєкт, Європарламентом та Радою ЄС були сформовані чіткіші вимоги, які охоплюють сферу політичної реклами. Наразі такі правила містяться у Проєкті Регламенту щодо прозорості та таргетування політичної реклами, спрямованому на зменшення маніпулятивного впливу та обмеження використання персональних даних виборців.[62] Правила щодо прозорості у Проєкті передбачають, що кожен такий рекламний матеріал має публікуватися з використанням спеціальних технік маркування, які дають змогу ідентифікувати рекламу як політичну. Крім цього, повідомлення повинні містити таку інформацію:

1. Твердження про те, що це політична реклама;
2. Особу замовника політичної реклами та суб'єкта, який повністю контролює замовника;
3. Сповіщення про прозорість, аби зрозуміти ширший контекст політичної реклами та її цілей, або чітка вказівка на те, де цю інформацію можна знайти.[63]

У свою чергу, сповіщення про прозорість має включати в себе інформацію про:

1. Особу замовника та контактні дані;
2. Період, протягом якого планується публікація та розміщення політичної реклами;
3. Загальні витрачені суми чи інші вигоди, отримані частково або в повному обсязі для підготовки, розміщення, просування, публікації та розповсюдження відповідної реклами, та на політичну рекламну кампанію, якщо це доречно, а також джерела витрачених сум;
4. Де доречно, зазначення виборів або референдумів, з якими пов'язана реклама;
5. Де доречно, посилання на онлайн-сховища реклами;
6. Інформацію про те, як використовувати механізми для подання скарг на потенційно протиправну рекламу.[64]

Задля уникнення надмірних обсягів інформації Проєкт наголошує на тому, що сповіщення про прозорість має бути легкодоступним (easily retrieved). Це передбачає чіткість написання та видимість, можливість машинозчитування, а також використання простої мови для зручності користувача. Наприклад, для онлайн-реклами необхідно попередньо опублікувати принаймні банер, котрий вказуватиме на контент відповідної реклами. Крім того, на момент публікації реклами такі сповіщення повинні знаходитися в актуальному стані. Видавці політичної реклами зобов'язані зберігати сповіщення про прозорість разом із іншими модифікаціями протягом п'яти років. Оскільки згадані положення поширюються здебільшого на великі онлайн-платформи, Проєкт закликає держави-члени формувати внутрішні національні співрегулівні кодекси, що можуть застосовуватися до невеликих локальних платформ, які надають рекламні послуги.

---

[60] Регламент Ради ЄС 2016/679 від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних та про вільний рух таких даних, а також про скасування Директиви 95/46/ЕС (Загальний регламент захисту даних) [2016], OJ L 119/1, стаття 7(3).
URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[61] Проєкт Регламенту Європейського парламенту та Ради щодо єдиного ринку цифрових послуг (Акт про цифрові послуги) та внесення змін до Директиви 2000/31/ЕС від 15 грудня 2020 року.

[62] Проєкт Регламенту Європейського парламенту та Ради щодо прозорості та таргетування політичної реклами від 25 листопада 2021 року.

[63] Там само, стаття 7(1).

[64] Там само, стаття 7(2).

Проєкт також накладає зобов'язання щодо ведення звітів на видавців політичної реклами.[65] До останніх належать фізичні/юридичні особи, що транслюють, роблять доступною через інтерфейс або іншим чином доносять до суспільства політичну рекламу за допомогою будь-яких засобів. У відповідному звіті слід зазначати, які послуги надавались у зв'язку з розміщенням політичної реклами, за яку ціну такі послуги було надано, а також хто їх оплачував. Вся вищезазначена інформація зберігатиметься протягом 5 років з моменту публікації реклами.

Проєкт також закликає імплементувати до національного законодавства правила, що запустять механізм скарг користувачів у випадку виявлення протиправної політичної реклами. Такий механізм дозволить якнайшвидше виявити порушника та видалити небажаний контент із відповідного веб-сайту.[66]

Стаття 11 Проєкту також зобов'язує видавців безкоштовно надавати інформацію про політичну рекламу на вимогу зацікавлених осіб. До таких осіб Проєкт відносить перевірених дослідників, членів громадських організацій, політичних акторів, спостерігачів за виборами, а також акредитованих журналістів. Таким чином, Проєкт дозволяє отримувати інформацію лише тим особам, що не мають на меті будь-яких комерційних інтересів. У випадку запиту на інформацію, видавці мають один місяць для надання відповіді.

Для забезпечення виконання правил Проєкт покладає на держави-члени додаткові зобов'язання. По-перше, посилаючись на Проєкт Акту ЄС про цифрові послуги, кожній державі-члену необхідно призначити регулятора серед компетентних органів, який займатиметься моніторингом дотримання обмежувальних заходів.[67] Згідно з Проєктом Акту ЄС про цифрові послуги, такий регулятор виступає Координатором цифрових послуг відповідної держави-члена, що діє незалежно, неупереджено, прозоро та своєчасно.[68] По-друге, Проєкт наголошує на санкціях, які слід розробити на національному рівні державам-членам на випадок порушення вимог щодо прозорості.[69] Вимога щодо встановлення адміністративних або фінансових штрафів тут є доцільною, адже вона забезпечить обов'язковість правил та гарантуватиме неухильне дотримання і виконання міжнародних стандартів.

Наразі Проєкт перебуває на стадії ухвалення. Відповідно до статті 20 Проєкту, Регламент набуває чинності на двадцятий день після його публікації в Офіційному журналі Європейського Союзу. Попередньо він має набути чинності з 1 квітня 2023 року. Цей Регламент є обов'язковим у повному обсязі, а його норми підлягають прямому застосуванню в усіх державах-членах.

Посилаючись на положення Проєкту Регламенту щодо прозорості та таргетування політичної реклами, Посилений Кодекс ЄС щодо протидії дезінформації від 2022 року накладає фактично аналогічні зобов'язання на підписантів у контексті поширення політичної реклами. Підписантам слід розробити чіткі методи маркування, що дадуть змогу розпізнати політичну рекламу, яка була оплачена.[70] Крім того, підписанти повинні брати участь у регулярних дослідженнях для вдосконалення технік маркування. Стосовно вимог прозорості, Кодекс вкотре звертається до Проєкту Регламенту щодо прозорості та таргетування політичної реклами та зобов'язує підписантів відображати поряд із політичною рекламою інформацію про особу замовника, період показу реклами, витрати та зведену інформацію про отримувачів такої реклами.[71] Крім того, користувачам надаватиметься повна інформація, чому вони отримали рекламу політичного змісту. Як вбачається з вищезгаданого, рекомендації Кодексу суттєво перетинаються з вимогами Проєкту, що вказує на узгодженість позицій авторів обох документів. Це також дозволяє говорити про погодження норм Проєкту з більшістю онлайн-платформ, діяльність яких він потенційно регулюватиме.

[65] Там само, стаття 8.
[66] Там само, стаття 9.
[67] Там само, стаття 15(2).
[68] Проєкт Регламенту Європейського парламенту та Ради щодо єдиного ринку цифрових послуг (Акт про цифрові послуги) та внесення змін до Директиви 2000/31/ЕС від 15 грудня 2020 року, стаття 38-39.
[69] Там само, стаття 16.
[70] Посилений Кодекс ЄС щодо протидії дезінформації від 16 червня 2022 року, Твердження 6.1.
[71] Посилений Кодекс ЄС щодо протидії дезінформації від 16 червня 2022 року, Твердження 8.1.

Схожі вимоги до розміщення політичної реклами містяться і в Рекомендації CM/Rec(2022)12 Комітету міністрів державам-членам щодо виборчої комунікації та висвітлення виборчих кампаній у ЗМІ.[72] Рекомендація застосовується винятково до онлайн-платформ, що є "домінуючими, враховуючи їх охоплення, масштаб і вплив" (на кшталт Google, Facebook). Вимоги прозорості, відображені у Рекомендації, вимагають повідомляти найменування та адреси фізичних або юридичних осіб, відповідальних за виробництво або оплату вироблених матеріалів .[73] Цікавим є положення, що накладає на онлайн-платформи обов'язок створювати архіви, котрі містять перелік всіх публікацій політичної реклами, що були поширені цими платформами. Такий архів повинен бути легкодоступним та знаходитися у відкритому доступі для публіки. Рекомендація також зобов'язує держави-члени передбачити механізми притягнення до відповідальності на національному рівні у випадку недотримання правил.

У контексті імплементації міжнародних стандартів у національне законодавство можна розглянути приклад Кодексу поведінки Нідерландів щодо прозорості політичної онлайн-реклами – першого подібного кодексу поведінки у Європейському Союзі.[74] Напередодні парламентських виборів 2021 року 11 із 13 парламентських партій та онлайн-платформи (Facebook, Google, Snapchat, TikTok) взяли на себе відповідні зобов'язання щодо дотримання вимог прозорості політичної реклами.[75] Таким чином, Кодекс зобов'язує дотримуватися вимог як політичних акторів, так і онлайн-платформи. Його положення наголошують на прозорості реклами, що виключає її фінансування з боку третіх осіб, а також на потребі уникати надмірного мікротаргетингу та психологічного профілювання. Своєю чергою онлайн-платформи, відповідно до положень Кодексу, зобов'язуються надавати деталізовану інформацію про рекламодавця та власне рекламу.

Для підвищення прозорості вимагається реєстрація та верифікація політичних акторів, що поширюють політичну рекламу. Така реєстрація необхідна не лише для швидкої ідентифікації видавців, але й для виявлення сумнівних рекламодавців, відсутніх у реєстрі, оскільки Кодекс забороняє поширення політичної реклами з-поза меж ЄС. Крім цього, забороняється поширювати неправдиві відомості та мову ворожнечі, а у випадку її виявлення онлайн-платформи уповноважені негайно її видалити. Кодекс є рекомендаційним документом із керівними принципами, які вказують на потребу дотримуватися певних правил розміщення політичної реклами. Водночас такий документ є орієнтиром для зменшення зловживання політичною рекламою та захисту виборців під час виборчих кампаній.

Положення щодо прозорості на законодавчому рівні містяться і у законодавстві Франції, як-от Законі Франції про боротьбу з маніпулюванням інформацією.[76] Протягом виборчих кампаній на медіа (в тому числі онлайн-медіа) покладається обов'язок надавати аудиторії чітку та прозору інформацію про особу, що замовила опублікований політичний контент, а також розмір винагороди за публікацію.[77] За порушення цих правил закон встановлює санкції у вигляді ув'язнення до одного року або штрафу на суму 75 тисяч євро.[78]

[72] Рекомендації CM/Rec(2022)12 Комітету міністрів державам-членам щодо виборчої комунікації та висвітлення виборчих кампаній у ЗМІ від 6 квітня 2022 року.
[73] Там само, Твердження 2(2.1).
[74] Кодекс поведінки Нідерландів щодо прозорості політичної онлайн-реклами (2022). URL:https://www.idea.int/sites/default/files/news/news-pdfs/Dutch-Code-of-Conduct-transparency-online-political-advertisements-EN.pdf
[75] "Перший національний Кодекс поведінки щодо політичної онлайн-реклами у Європейському Союзі, підписаний нідерландськими політичними партіями та глобальними онлайн-платформами". International IDEA, 9 лютого 2021. URL:https://www.idea.int/news-media/news/first-national-code-conduct-online-political-advertising-european-union-signed-dutch
[76] Закон Франції про боротьбу з маніпулюванням інформацією № 2018-1202 від 22 грудня 2018 року.
[77] Там само, стаття 1(6).
[78] Там само, стаття 1(3).

Крім того, вимоги до прозорості передбачені у Виборчому кодексі Франції.[79] Стаття 163-1 кодексу містить широкий перелік інформації, яку повинні надавати онлайн-платформи користувачам протягом трьох місяців перед виборами, виключаючи:

- Інформацію про фізичну особу або назву компанії, зареєстрований офіс та корпоративну мету юридичної особи та особи, від імені якої, де доречно, вона має право діяти, яка сплачує винагороду платформі в обмін на просування інформаційного контенту, пов'язаного з дебатами загального інтересу;

- Інформацію про використання персональних даних користувача у контексті просування інформаційного контенту, що стосується питань загального інтересу;

- Суму винагороди, отриману в обмін на просування такого інформаційного контенту, якщо сума перевищує встановлений поріг.

Вся вищезгадана інформація зібрана у єдиному реєстрі, що регулярно оновлюється та знаходиться у відкритому доступі для громадськості. Такі деталізовані вимоги кодексу спонукали платформи на кшталт Twitter заборонити будь-яку політичну рекламу у Франції.[80]

Цікаво, що за законодавством Німеччини, "забороняється реклама політичного, ідеологічного чи релігійного характеру". Так, німецький Міждержавний договір про радіомовлення, що регулює аудіовізуальні медіа та радіо (включно з тими, що транслюються через Інтернет), загалом забороняє поширення реклами політичного змісту, що відрізняється від звичайного контенту в позавиборчий період.[81] Прикметно, що вищезгадані правила не поширюються на платформи Facebook та Youtube. Таким чином, стає зрозумілим, чому під час виборчих кампаній німецькі політичні актори поступово переходять до неврегульованих соціальних мереж. Відповідно до бібліотеки оголошень Facebook, під час федеральних парламентських виборів сім основних німецьких партій разом витратили трохи менше 1,5 мільйона євро на рекламу зі своїх офіційних сторінок Facebook.[82]

Мікротаргетинг у виборчому процесі

Мікротаргетинг полягає у використанні персональних даних, стратегічно спрямованому на адресування індивідуальних персоналізованих повідомлень виборцям, яких можна переконати чи мобілізувати. Зазвичай при використанні цієї техніки ігноруються інші виборці, яких не так легко переконати голосувати за обраного кандидата.[83] Техніка націлювання контенту на обране коло осіб зазвичай включає в себе три кроки:

1. Збір особистих даних;
2. Використання цих даних для визначення груп людей, які, ймовірно, сприйнятливі до певного повідомлення;
3. Надсилання індивідуалізованих онлайн-повідомлень.[84]

---

79 Виборчий кодекс Франції. URL: https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006070239/

80 "Twitter блокує уряд Франції власним законом про фейкові новини". BBC News, 3 квітня 2019. URL: https://www.bbc.com/news/world-europe-47800418

81 Міждержавний договір про радіомовлення та телемедіа від 1 травня 2019. URL:https://www.die-medienanstalten.de/fileadmin/user_upload/Rechtsgrundlagen/Gesetze_Staatsvertraege/RStV_22_english_version_clean.pdf

82 Холройд Метью. "Вибори у Німеччині: хто витратив найбільше на рекламу у Facebook?". Euronews, 1 жовтня 2021. URL:https://www.euronews.com/my-europe/2021/09/25/german-election-who-has-spent-the-most-on-facebook-advertising

83 Проект Регламенту Європейського парламенту та Ради щодо прозорості та таргетування політичної реклами від 25 листопада 2021 року.

84 Доббер Т., Фатайг О. та інші "Регулювання онлайн-політичного мікротаргетингу в Європі" / Огляд політики в Інтернеті, 8(4) (2019). URL: https://policyreview.info/articles/analysis/regulation-online-political-micro-targeting-europe

Очевидно, що можливість використання мікротаргетингу напряму залежить від онлайн-платформ, що збирають та зберігають велику кількість персональних даних та дозволяють націлювати інформацію на визначені категорії користувачів. Основними з них є Facebook та Google. Завдяки своїй простій у використанні інфраструктурі, Facebook дозволяє легко використовувати цю практику.[85]

Згадані платформи зберігають величезну кількість персональних даних і пропонують політичним гравцям засоби для охоплення певних груп без необхідності збирати додаткові дані. Проблема такого збереження даних унаочнилася у 2018 році через скандал з Facebook та Cambridge Analytica, пов'язаний з виборами у США 2016 року. Приватна англійська компанія Cambridge Analytica сприяла політичним діячам, зокрема Дональду Трампу, у поширенні матеріалів передвиборної агітації. Компанія збирала приватні дані користувачів, створивши систему, яка профілювала окремих виборців у США, щоб націлити на них персоналізовану політичну рекламу. Внаслідок таких цифрових операцій Cambridge Analytica зібрала понад 50 мільйонів профілів користувачів Facebook та їх персональних даних.[86]

Системи профайлингу розроблені таким чином, аби на основі зібраних даних про користувача робити висновки про його приватні преференції та уподобання.[87] В подальшому такі профілі та прогнози використовуються для персоналізації політичних повідомлень, наприклад, висвітлення у рекомендованих повідомленнях реклами у соціальних мережах.[88] Припускається, що така реклама надсилається, оскільки користувач має бути зацікавлений у ній, з огляду на його поведінку на тій чи іншій платформі. Таким чином, мікротаргетинг має небезпечний вплив на вибір користувачів, оскільки збір даних при його застосуванні передбачає роботу з чутливими даними.

Про це зазначається також і в Плані дій щодо Європейської демократії.[89] Практика використання таргетування в Інтернеті значно ускладнює притягнення політиків до відповідальності та відкриває нові шляхи для спроб маніпулювати виборцями. Більше того, така практика стала ще більш небезпечною з огляду на поєднання персональних даних та штучного інтелекту. І якщо правила обробки персональних даних загалом врегульовано на рівні ЄС, то таргетування поки що чітко регулюється виключно корпоративними умовами надання послуг від онлайн-платформ.

Фундаментальним документом, що вирішує питання обробки персональних даних (у тому числі чутливих), є Загальний регламент захисту даних.[90] Регламент врегульовує питання профайлингу, який в документі визначається як "будь-яка форма автоматизованої обробки персональних даних, яка полягає у використанні персональних даних для оцінки певних особистих аспектів, що стосуються фізичної особи, особливо для аналізу або прогнозування аспектів стосовно продуктивності цієї фізичної особи на роботі, економічного становища, здоров'я, особистих уподобань, інтересів, надійності, поведінки, розташування або рухів".[91] Щодо обробки даних під час профайлингу Регламент встановлює чіткі вимоги до правомірності обробки даних, включаючи прозорість та цілісність, законну основу, обов'язок регулярного звітування та можливість особи відмовитися від такої обробки. Обробка чутливих даних особи дозволяється виключно за згодою осіб, за винятком певних випадків. Такі винятки повинні бути передбачені законом відповідної

[85] Там само.

[86] Кадвалладр Керол, Грехем-Харрісон Емма. "Виявлено: 50 мільйонів профілів Facebook зібрано для Cambridge Analytica через серйозний витік даних". The Guardian, 17 травня 2018. URL:https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

[87] Міотто Лукас, Чахонг Чен "Маніпуляції, профілювання в реальному часі та їхні помилки" / В кн.: "Філософія онлайн-маніпуляції" (2021). URL:https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3968999

[88] "Практичний приклад: Профілювання та вибори - як політичні кампанії знають наші найглибші секрети". Privacy International, 30 серпня 2017. URL:https://privacyinternational.org/case-study/763/case-study-profiling-and-elections-how-political-campaigns-know-our-deepest-secrets

[89] План дій щодо Європейської демократії. Комунікація Комісії до Європейського парламенту, Європейської ради, Європейського економічного та соціального комітету і комітету регіонів від 3 грудня 2020 року.

[90] Регламент Ради ЄС 2016/679 від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних та про вільний рух таких даних, а також про скасування Директиви 95/46/ЕС (Загальний регламент захисту даних) [2016], OJ L 119/1.

[91] Робоча група з питань захисту осіб щодо обробки персональних даних "Вказівки щодо автоматизованого індивідуального прийняття рішень і профілювання для цілей Регламенту 2016/679" (2017). URL: https://iapp.org/media/pdf/resource_center/W29-auto-decision_profiling_02-2018.pdf

держави-члена ЄС. Відповідно до статті 9 Загального регламенту захисту даних, обробка чутливих даних без згоди особи дозволяється, зокрема (1) якщо такі дані були оприлюднені раніше, (2) при поданні або розгляді юридичних позовів, (3) з метою публічного інтересу у сфері публічного здоров'я тощо.[92]

Прикметно, що профайлинг може створювати чутливі дані на основі логічних висновків із звичайних персональних даних, котрі у сукупності з іншими даними стають спеціальними та потребують особливих вимог до їх обробки. Така взаємодія може виявити дані про стан здоров'я, політичні та релігійні переконання, сексуальну орієнтацію та багато інших. Задля зменшення зловживання техніками профайлингу у випадку чутливих даних Регламент встановлює такі обмеження: обробка даних є сумісною з першочерговою метою, вона є законодавчо закріплена, а особа завчасно проінформована про таку обробку.

Для запобігання маніпуляціям з боку політичних акторів було розроблено вже згаданий Проєкт Регламенту Європейського парламенту та Ради щодо прозорості та таргетування політичної реклами.[93] Однією з його цілей є захист фізичних осіб та їх персональних даних шляхом встановлення правил використання мікротаргетингу в контексті публікації політичної реклами.

Розділ III Проєкту присвячений винятково таргетуванню та поширенню політичної реклами. За загальним правилом, забороняються техніки таргетування, що використовують спеціальні категорії персональних даних, окрім випадків, передбачених законом.[94] До таких чутливих даних відносять генетичні, біометричні дані, дані, що розкривають расове чи етнічне походження, політичні погляди, релігійні чи філософські переконання тощо.

Проєкт також містить вимогу до забезпечення прозорості при таргетуванні окремих користувачів. Так, контролери даних[95] зобов'язані розробити внутрішні політики, які чітко пояснюватимуть методи використання техніки таргетування та ампліфікації контенту. Така політика має залишатися незмінною протягом п'яти років. Крім того, вони повинні вести записи про механізми, методи та параметри таргетування, а також вказувати джерело використаних персональних даних. Остання вимога зобов'язує контролерів даних надавати додаткову інформацію, що може бути необхідна для розуміння користувачем технік таргетування або інших аналітичних технік. Факт використання мікротаргетингу обов'язково відображається у відповідному сповіщенні про прозорість. Як і у випадку з політичною рекламою, таке сповіщення повинне містити інформацію про особу замовника та його контактні дані, а також кошти, витрачені на мікротаргетинг. Вся надана інформація має надаватися у легкодоступному форматі, бути машинозчитувальною, чітко видимою і написаною простою мовою.

Правила використання технік мікротаргетингу передбачені і в Рекомендації CM/Rec(2022)12 Комітету міністрів державам-членам щодо виборчої комунікації та висвітлення виборчих кампаній у ЗМІ. Згідно з вимогами прозорості, онлайн-платформи повинні надавати інформацію про фінансування таргетингу, а також детальну демографічну інформацію, яка використовується для поширення реклами серед цільових груп. Користувачі повинні розуміти, чому вони таргетуються, а також мати можливість відмовитися від отримання політичної реклами. Рекомендація також закликає держави-члени розробити національний механізм для уникнення зловживання техніками таргетування, а політичних акторів – створювати власні кодекси поведінки з гарантіями від зловживань мікротаргентингом у їх кампаніях.

---

92 Регламент Ради ЄС 2016/679 від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних та про вільний рух таких даних, а також про скасування Директиви 95/46/ЕС (Загальний регламент захисту даних) [2016], OJ L 119/1.

93 Проєкт Регламенту Європейського парламенту та Ради щодо прозорості та таргетування політичної реклами від 25 листопада 2021 року.

94 Там само, стаття 12(1).

95 Прим. Контролер даних – фізична або юридична особа, державний орган, агентство чи інший орган, який самостійно чи спільно з іншими визначає цілі та засоби обробки персональних даних.

Зловживання алгоритмами онлайн-платформ у виборчому процесі

Алгоритмічні системи являють собою програми, які, часто використовуючи техніки математичної оптимізації, виконують одне або кілька завдань, як-от збір, об'єднання, очищення, сортування, класифікація та визначення даних, а також вибір, пріоритезація, вироблення рекомендацій та прийняття рішень.[96] Найчастіше застосування алгоритмів можна побачити у віртуальному просторі, особливо в об'єкті, який потребує автоматизації, обчислення чи аналізу для процесів, які мають бажаний результат для творця. Зазвичай програми, створені алгоритмами, практично неможливо відрізнити від продуктів, створених людиною.

Вирізняють різні категорії автоматизованого прийняття рішень алгоритмами, зокрема, пріоритезацію та фільтрування.[97] На основі останніх алгоритми включають або виключають інформацію відповідно до персоніфікованих інтересів або преференцій користувача. Таким чином, фільтрування зводиться до надмірного просування "бажаного" контенту та цензурування "нерелевантної" інформації.

Оперуючи шляхом відслідковування закономірностей у базах даних, алгоритми допомагають покращити якість послуг шляхом надання нових рішень для якнайшвидшого виконання завдань. При цьому саме завдяки алгоритмам продовжується збір персональних даних користувачів, які використовуються для прийняття рішень, адаптації рекомендацій або формування середовища. Проте негативний вплив алгоритмів стає особливо помітним у випадку категорій осіб, чиї дані не збираються або не враховуються при першочерговій обробці даних. Це автоматично ставить певну особу, групу або категорію населення у нерівне положення, адже обробці підлягає лише певна кількість персональних даних. Якщо ж алгоритмічна система має навіть ймовірну можливість негативно вплинути на права людини, вона потребує правового регулювання.

Посилений Кодекс ЄС щодо протидії дезінформації від 2022 року згадує про алгоритми у контексті систем штучного інтелекту, що генерують та поширюють маніпулятивний контент. Для дотримання вимог прозорості підписанти зобов'язані встановити власну внутрішню політику для гарантування того, що "алгоритми, які використовуються для виявлення, модерації та санкціонування неприпустимої поведінки та вмісту їхніх послуг, заслуговують на довіру, поважають права кінцевих користувачів і не є забороненими маніпулятивними методами".[98]

Правила прозорості передбачені також і Проєктом Акту ЄС про цифрові послуги.[99] Стаття 12 Проєкту зобов'язує постачальників проміжних послуг в умовах їх надання передбачати інформацію про цифрові інструменти, які використовуються для модерації контенту, включаючи алгоритмічне прийняття рішень.

Серед законодавчих документів слів згадати також і Проєкт Акту ЄС щодо штучного інтелекту, що врегульовує, зокрема, і алгоритми, які використовують онлайн-платформи. Стаття 5 Проєкту містить перелік заборонених практик штучного інтелекту .[100] Серед них варто виокремити використання підсвідомих методів (subliminal techniques) для спотворення поведінки людини та експлуатацію вразливих груп населення (наприклад, дітей або недієздатних осіб) у спосіб, що завдає їм фізичної або психологічної шкоди. Деякі дослідники вважають, що заборонені практики можуть також включати алгоритми рекламного таргетингу та рекомендації контенту

[96] Рекомендації CM/Rec(2020)1 Комітету міністрів державам-членам про вплив алгоритмічних систем на права людини від 8 квітня 2020 року.
[97] Рітчі Оак Джей "Алгоритми платформи та їх вплив на громадську та політичну арену" (2015). URL:https://www.researchgate.net/publication/304380890_Platform_Algorithms_and_Their_Effect_on_Civic_and_Political_Arenas
[98] Посилений Кодекс ЄС про протидію дезінформації від 16 червня 2022 року, Твердження 15.2.
[99] Проєкт Регламенту Європейського парламенту та Ради щодо єдиного ринку цифрових послуг (Акт про цифрові послуги) та внесення змін до Директиви 2000/31/ЕС від 15 грудня 2020 року.
[100] Проєкт Регламенту Європейського парламенту та Ради про встановлення гармонізованих правил щодо штучного інтелекту (Акт про штучний інтелект) та внесення змін до деяких законодавчих актів Союзу від 21 квітня 2021 року.

користувачам.[101] Згідно з вимогами прозорості, системи штучного інтелекту високого ризику повинні бути спроектовані та розроблені таким чином, аби користувач міг інтерпретувати вихідні дані системи та використовувати їх.[102] При цьому такі системи повинні супроводжуватися інструкціями для їх використання, викладенимиі у стислій, повній, чіткій та зрозумілій формі. Прикметно, що Проєкт не відносить до систем з високим ризиком алгоритми, які використовуються у соціальних мережах, для пошуку, в онлайн-торгівлі, у магазинах додатків, мобільних додатках або мобільних операційних системах.

Водночас, документи Ради Європи встановлюють детальніші умови використання алгоритмів. Серед них слід згадати Декларацію Комітету міністрів про маніпулятивні можливості алгоритмічних процесів.[103] Документ наголошує на негативному впливі алгоритмів внаслідок використання техніки прийняття рішень ("decision-making code"). Так, підсвідомі та персоналізовані рівні алгоритмічного переконання можуть чинити значний вплив на когнітивну автономію фізичних осіб та їх право формувати думку та приймати незалежні рішення. Саме тому Декларація акцентує увагу на збереженні можливості осіб формувати думки та приймати рішення незалежно від автоматизованих систем. Документ закликає держави-члени запровадити жорсткішу законодавчу політику, яка чітко визначатиме межі використання алгоритмічних систем. З огляду на їх технічний розвиток, заохочується також проведення дискусійних панелей, де експерти та представники громадянського суспільства отримають змогу висловити свою думку з приводу використання неправомірних практик.

Своєю чергою Рекомендація CM/Rec(2022)12 Комітету міністрів державам-членам щодо виборчої комунікації та висвітлення виборчих кампаній у ЗМІ передбачає вимоги прозорості до використання алгоритмів. Так, алгоритми, які використовуються державними та приватними акторами для класифікації та відображення політичної реклами та матеріалів виборчої комунікації, а також ті, що використовуються в практиках модерації контенту, мають бути прозорими та верифікованими, особливо щодо потенційної упередженості та неточності використовуваних систем. Документ також закликає держави-члени створити належну правову базу для регулювання використання алгоритмів, їх моніторингу та аудиту. Своєю чергою онлайн-платформи зобов'язуються надавати регулярні звіти та статистику про алгоритми, які використовуються при публікації політичної реклами.

Усі ці вимоги повинні узгоджуватися з положеннями, відображеними у Рекомендації CM/Rec(2020)1 Комітету міністрів державам-членам про вплив алгоритмічних систем на права людини. Рекомендація описує ризики порушення прав людини внаслідок надмірного та неправомірного використання алгоритмічних систем. Оскільки такі системи можна зустріти майже у кожній сфері життя (бізнес, комерція, телетрансляції), Рекомендація застосовується також і до виборчого контексту. Посилаючись на принципи постійного перегляду ("review"), демократичної участі, обізнаності та інституційного законодавчого оформлення, Рекомендація зобов'язує попереджати користувачів про обробку та контроль персональних даних (включно з цілями та результатами), які використовуватимуться алгоритмічними системами.

Для підвищення рівня прозорості Рекомендація закликає встановити спеціальні маркування, які дозволять користувачам розрізнити алгоритмічну систему. Задля ефективної ідентифікації алгоритмів, маркування має бути легкодоступним та зрозумілим. Примітно, що Рекомендація зобов'язує держави-члени розробити ефективну систему засобів правового захисту та розв'язання спорів у випадку порушення прав користувачів (як офлайн, так і онлайн). Ця Рекомендація є надійним орієнтиром для держав-членів при розробці національного законодавства, оскільки її людиноцентричний підхід засновується на тому, аби основоположні права людини не були порушені внаслідок використання алгоритмічних систем.

[101] Маккерсі Марк, Пропп Кеннет. "Машини дізнаються, що Брюссель пише правила: новий регламент ЄС щодо штучного інтелекту". Brookings, 4 травня 2021.
URL:https://www.brookings.edu/blog/techtank/2021/05/04/machines-learn-that-brussels-writes-the-rules-the-eus-new-ai-regulation/

[102] Проєкт Регламенту Європейського парламенту та Ради про встановлення гармонізованих правил щодо штучного інтелекту (Акт про штучний інтелект) та внесення змін до деяких законодавчих актів Союзу від 21 квітня 2021 року, стаття 13(1).

[103] Декларація Комітету міністрів про маніпулятивні можливості алгоритмічних процесів від 13 лютого 2019 року.
URL: https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b

Маніпулятивні опитування у виборчому процесі

У виборчих кампаніях часто можна помітити маніпуляції при проведенні опитувань громадської думки ("opinion polls"), які вимірюють та порівнюють політичну конкуренцію. Результати таких опитувань демонструють, які політичні актори мають прихильність серед виборців, та загалом відображають політичні настрої громадськості. Оскільки думка громадськості є одним із факторів, які беруться до уваги при прийнятті рішення про голосування за того чи іншого актора виборцями, що не визначилися або не мають чітко сформованих вподобань, зловмисні гравці можуть маніпулювати статистичними даними для досягнення власних цілей.

Не менш важливу роль у цьому грають медіа (як традиційні, так і онлайн), що висвітлюють результати опитувань. На них покладається обов'язок відображати точну інформацію про кандидатів та виборчий процес, аби уникнути негативного впливу на вибір громадян та забезпечити справедливість виборів. Примітно, що соціологічні опитування мають здебільшого негативний вплив у пострадянських країнах, де маніпуляція думкою часто виражена через приховування замовників опитувань.[104] Яскраві приклади маніпуляції було виявлено при проведенні місцевих виборів в Україні у 2020 році.[105] Так, при висвітленні результатів соцопитування медіа не вказували замовників дослідження, а також даних про час його проведення, територію охоплення, розмір та спосіб формування вибірки, метод, точне формулювання питання та статистичну похибку.

Часто політичні актори залишаються незадоволеними їх місцем у рейтингу під час виборчих кампаній, а тому починають звертатися до так званих псевдосоціологічних служб для оприлюднення більш вигідних результатів.[106] Зазвичай такі фірми виникають виключно в період виборів, проводять опитування, отримують за це кошти та зникають з радарів до наступних виборів. Вони часто публікують результати опитувань на інших платформах та у медіа для підвищення рейтингу політичного діяча на всіх рівнях. Через свою некомпетентність такі служби часто не дотримуються стандартів проведення соціологічного опитування, не вказуючи, зокрема, методу, похибки або території охоплення. Іншою проблемою є маніпуляції при формуванні питань, коли обмежується або певним чином формулюється перелік можливих варіантів відповіді, який натякає на потрібний результат опитування. У підсумку, таке тенденційне формулювання питань має на виході викривлене замірювання громадської думки. Хоча такі сумнівні опитування можна легко ідентифікувати, вони все одно залишаються досить небезпечним онлайн-інструментом для введення публіки в оману.

Крім того, соціологічні опитування можуть бути маніпулятивними з огляду на бажання політичних акторів лобіювати власні інтереси. Так, під час виборчих кампаній багато сайтів проводять опитування користувачів на власних сторінках. Пізніше результати таких опитувань публікуються на інших публічних платформах у якості нейтральної думки, незважаючи на те, що голоси було віддано на користь конкретного політика. Саме тому платформам необхідно публікувати всі вихідні дані проведеного опитування, включаючи його аудиторію та основний зміст.

Для забезпечення надійності соціологічних опитувань мають існувати спеціальні правила висвітлення їх результатів. Вимоги щодо цього можна знайти у Рекомендації №R(99)15 Комітету міністрів державам-членам про заходи щодо висвітлення виборчих кампаній у ЗМІ.[107] Так, "нормативно-правові рамки або системи саморегулювання повинні забезпечити, щоб ЗМІ, поширюючи результати опитувань громадської думки, надавали громадськості достатню інформацію для того, щоб сформувати судження про цінність опитувань.

[104] Бірх Сара "Пострадянська виборча практика у порівняльній перспективі" / Vol. 63, №4 (2011), ст. 707. URL: https://www.jstor.org/stable/27975573

[105] Пристай Денис. "Місцеві вибори-2020. Як маніпулюють рейтингами і соціологічними даними". Суспільне, 27 вересня 2020.
URL:https://suspilne.media/66009-miscevi-vibori-2020-rejtingi-partij-opituvannya-doslidzhennya-j-sposobi-manipulyaciyi/

[106] URL: https://texty.org.ua/d/socio/#about

[107] Рекомендація № R (99) 15 Комітету міністрів до держав-членів про заходи щодо висвітлення виборчих кампаній у засобах масової інформації від 9 вересня 1999 року.
URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805e3c6b

Така інформація може, зокрема:

1. Називати політичну партію або іншу організацію чи особу, яка замовила та оплатила опитування;
2. Визначати організацію, яка проводить опитування, та використану методологію;
3. Вказувати вибірку та похибку опитування;
4. Вказувати дату та/або період проведення опитування".

При цьому Рекомендація дозволяє забороняти публікацію результатів опитувань перед виборами, якщо така заборона є пропорційною та узгоджена зі свободою вираження поглядів.

Своєю чергою, Рекомендація CM/Rec(2022)12 Комітету міністрів державам-членам щодо виборчої комунікації та висвітлення виборчих кампаній у ЗМІ фактично дублює вимоги своєї попередниці, передбачаючи також можливість заборони проведення соціологічних опитувань під час виборчого процесу. Рекомендація надає державам-членам дискрецію у можливості вимагати від онлайн-платформ дотримання правил виборчої тиші або повної заборони опитувань громадської думки під час виборчих періодів, там де це можливо. Крім того, після публікації результатів опитування держави можуть вимагати від медіа та онлайн-платформ надати інформацію щодо опитувань, включаючи дані про фізичних або юридичних осіб, які їх замовили та оплатили.

Україна та використання цифрових технологій у виборчому процесі

Декларуючи свій шлях до цифровізації, Україна протягом останніх років спрямовує свої зусилля на врегулювання сфери цифрових технологій та проблем, котрі виникають внаслідок їхнього свавільного використання. Чинне законодавство у сфері політичної реклами та агітації є застарілим і не враховує роль онлайн-інструментів, а його оновлення затягується через політичні причини та необхідність загального вдосконалення Виборчого кодексу.

Сьогодні українське законодавство містить лише окремі норми, що стосуються використання певних неправомірних практик. Виборчий кодекс врегульовує загальні питання, пов'язані з розміщення політичної реклами. Так, політична реклама має бути відокремлена від інших матеріалів і позначена, а опитування громадської думки, результати яких поширюються в Інтернеті, мають обов'язково публікуватися із вказанням часу проведення, території, яку охоплювало опитування, розміру та способу формування соціологічної вибірки опитаних, методу опитування, точного формулювання питань, можливої статистичної похибки, замовників опитування.

Втім, такі правила не є достатніми, фактично консервуючи "дике поле" у сфері обмеження шкідливого впливу на виборців зі сторони зловмисних акторів в Інтернеті. Онлайн-медіа та онлайн-платформи фактично не підпадають під дію вимог Кодексу, що створює широкий простір для маніпуляцій та зловживань. При цьому, статистика витрат політичних партій та їх представників під час останніх виборів вказує, що сумарні видатки на політичну рекламу у Facebook та Instagram у 2020 році склали 174 тисячі доларів США.[108] Частково цю проблему покликаний вирішити Проєкт Закону про медіа, що наразі перебуває на розгляді Верховної Ради України та був прийнятий у першому читанні 30 серпня 2022 року.[109] Цей Проєкт вперше встановлює вимоги до онлайн-медіа щодо розміщення передвиборної агітації та закріплює принципи кооперації між національними регуляторами та онлайн-платформами у цьому питанні.

В Україні також відсутнє спеціальне законодавство, яке б регулювало інші практики, згадані у звіті, як-от використання мікротаргетингу, діпфейків або ботів. Водночас законодавче регулювання цієї сфери набуває неабиякого значення, адже маніпулювання думкоювиборців створює серйозні загрози для безпеки держави, особливо в умовах війни проти України та відродження імперських амбіцій Російської Федерації. Спроби застосувати наявні загальні механізми до таких явищ можуть призводити до суперечливих наслідків. До прикладу, у вересні 2022 року СБУ виявила дві ботоферми, що поширювали контент для виправдання збройної агресії проти України

[108] Патрікєєва Наталія. "Витрати політиків на рекламу у Facebook: партії вкладають найбільше". ЧЕСНО, 15 вересня 2020. URL: https://www.chesno.org/post/4207/

[109] Проєкт Закону про медіа №2693-д від 2 липня 2020 року. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/3115

та розхитування суспільно-політичної ситуації в країні. Зловмисників було звинувачено за ст. 361 КК (“Несанкціоноване втручання в роботу інформаційних (автоматизованих) електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж”). Відсутність предмету злочину (координованої неавтентичної поведінки) і, як наслідок, його об’єктивної сторони ставить серйозні питання щодо правомірності притягнення до відповідальності за цією статтею. А отже, наявні прогалини у законодавстві мають бути заповнені.

Роль цифрових технологій у майбутньому лише зростатиме. Саме тому вже сьогодні слід впроваджувати відповідні законодавчі зміни, аби захистити демократичні процеси і не дати їх спотворити. Важливо спиратися при цьому на стандарти, розроблені Європейським Союзом, адже гармонізація нашого законодавства є невід’ємною частиною євроінтеграційного курсу, закріпленого у Конституції України та підтвердженого наданням Україні статусу кандидата на вступ до ЄС.

Загальні висновки та рекомендації

Україна сьогодні перебуває на фронті однієї з найбільших воєн на європейському континенті після завершення Другої світової війни. Здавалося б, це мало ослабити здатність нашої держави приймати законодавчі рішення, які системно заповнюватимуть прогалини у її законодавстві. Тим більше, актуальність питання виборів є досить сумнівною, оскільки їх проведення під час дії правового режиму воєнного стану неможливе.

Втім, ми вважаємо, що цей час є вікном можливостей. Зокрема, щоб підготуватися до іншої частини війни, яка, незалежно від перебігу подій на фізичному полі, відбуватиметься в онлайн-просторі. Для цього варто встановити ефективні механізми, що убезпечили б демократію від руйнування зсередини внаслідок шкідливих інформаційних впливів на українських співгромадян за допомогою цифрових технологій.

Сьогодні використання онлайн-інструментів для фасилітації демократичних процесів є маловрегульованим, що дає зловмисним гравцям занадто широкі можливості використовувати для власних потреб технології, які негативно впливають на свободу прийняття поінформованих рішень.

З огляду на останні тенденції розвитку законодавства Європейського Союзу, м'якого права в рамках Ради Європи та інших міжнародних організацій, адаптовувати законодавство до майбутніх викликів необхідно вже сьогодні. У контексті змін до українського законодавства Лабораторія цифрової безпеки рекомендує:

1. Врегулювати питання розміщення передвиборної агітації в онлайн-медіа та за допомогою операторів банерної реклами, впровадивши прозорі правила її маркування та запровадивши дієві механізми притягнення до відповідальності за їх порушення, що враховуватимуть вимоги необхідності та пропорційності;

2. До закінчення дискусій про встановлення юрисдикції над діями онлайн-платформ на національному рівні, в тому числі через прийняття на рівні ЄС Акту про цифрові послуги, запровадити механізми співпраці з онлайн-платформами для впровадження вимог до прозорості політичної реклами, сповіщень про її замовників та забезпечення доступу громадськості до бібліотек такої реклами, а також прозорості алгоритмів модерації контенту;

3. Після прийняття Акту ЄС про цифрові послуги імплементувати його у національне законодавство України з урахуванням вимог щодо запобігання шкідливим впливам на політичні та демократичні процеси, і створенням незалежного та ефективного механізму нагляду за впровадженням його положень;

4. При імплементації до національного законодавства вимог Загального регламенту захисту персональних даних (GDPR) запровадити заборону на використання мікротаргетингу при поширенні політичної реклами та агітації;

5. Встановити обмеження на використання діпфейків у рамках виборчого та референдумного процесів, чіткіше врегулювавши можливість їх використання поза межами цих часових проміжків;

6. Запровадити додаткові запобіжники для обмеження маніпулятивних опитувань громадської думки, зокрема, шляхом чіткої ідентифікації вихідних даних та репрезентації аудиторії, думки якої такі опитування висвітлюють;

7. Закріпити обмеження на використання ботів для просування дезінформаційних кампаній та встановити відповідальність за їх використання задля впливу на суспільну думку у сфері виборів та референдумів.

ДОДАТОК

Документи ЄС та Ради Європи
щодо ролі цифрових технологій у виборчому процесі

1. Посилений Кодекс ЄС щодо протидії дезінформації від 16 червня 2022 року / The Strengthened Code of Practice on Disinformation 2022
2. Декларація про майбутнє Інтернету від 28 квітня 2022 року / Declaration for the Future of Internet
3. Рекомендації CM/Rec(2022)12 Комітету міністрів державам-членам щодо виборчої комунікації та висвітлення виборчих кампаній у ЗМІ від 6 квітня 2022 року / Recommendation CM/Rec(2022)12 of the Committee of Ministers to member States on electoral communication and media coverage of election campaigns
4. Прозорість та таргетування політичної реклами. Оцінка впливу (SWD(2021) 355, SWD(2021) 356 (підсумок)), що супроводжує пропозицію Комісії для Регламенту Європейського парламенту та ради щодо прозорості та таргетування політичної реклами (COM(2021) 731) [2022] / Transparency and targeting of political advertising. Impact assessment (SWD(2021) 355, SWD(2021) 356 (summary)) accompanying a Commission proposal for a Regulation of the European Parliament and of the Council on the transparency and targeting of political advertising (COM(2021) 731)
5. Проект Регламенту Європейського парламенту та ради щодо прозорості та таргетування політичної реклами від 25 листопада 2021 року / Proposal for a Regulation of the European parliament and of the Council on the transparency and targeting of political advertising
6. Вказівки Європейської комісії щодо посилення Кодексу практики щодо дезінформації 26 травня 2021 року / European Commission Guidance on Strengthening the Code of Practice on Disinformation
7. Проект Регламенту Європейського парламенту та ради щодо встановлення гармонізованих правил щодо штучного інтелекту (Акт про штучний інтелект) та внесення змін до деяких законодавчих актів Союзу від 21 квітня 2021 року / Proposal for a Regulation of the European parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts
8. Звіт про штучний інтелект: питання тлумачення та застосування міжнародного права, оскільки ЄС зачіпає сфери цивільного та військового використання та державної влади поза сферою кримінального правосуддя (2020/2013(INI)) від 4 січня 2021 року / Report on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice (2020/2013(INI))
9. Проект Регламенту Європейського парламенту та ради щодо єдиного ринку цифрових послуг (Акт про цифрові послуги) та внесення змін до Директиви 2000/31/ЕС від 15 грудня 2020 року / Proposal for a Regulation of the European parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC
10. План дій щодо Європейської демократії. Комунікація Комісії до Європейського парламенту, Європейської ради, Європейського економічного та соціального комітету і комітету регіонів від 3 грудня 2020 року / Communication from the Commission to the European parliament, the Council, the European economic and social Committee and the Committee of the regions. On the European democracy action plan
11. Оцінка Кодексу практики щодо дезінформації – досягнення та сфери для подальшого вдосконалення. Робочий документ Комісії від 10 вересня 2020 року / Commission staff working document. Assessment of the Code of Practice on Disinformation - Achievements and areas for further improvement
12. Рекомендації CM/Rec(2020)1 Комітету міністрів державам-членам про вплив алгоритмічних систем на права людини від 8 квітня 2020 року / Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems

13. Звіт про виконання Плану дій проти дезінформації. Спільна комунікація до Європейського парламенту, Європейської ради, Європейського економічного та соціального комітету і комітету регіонів від 14 червня 2019 року / Joint communication to the European parliament, the European council, the Council, the European economic and social Committee and the Committee of the regions. Report on the implementation of the Action Plan Against Disinformation
14. Декларація Комітету Міністрів про маніпулятивні можливості алгоритмічних процесів від 13 лютого 2019 року / Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes
15. План дій проти Дезінформації. Спільна комунікація до Європейського парламенту, Європейської ради, Європейського економічного та соціального комітету і комітету регіонів від 5 грудня 2018 року / Joint communication to the European parliament, the European council, the Council, the European economic and social Committee and the Committee of the regions. Action Plan against Disinformation
16. Кодекс ЄС щодо протидії дезінформації від 26 вересня 2018 року / EU Code of Practice on Disinformation
17. Стан Союзу 2018: Європейська комісія пропонує заходи для забезпечення вільних і чесних виборів до Європейського Союзу. Прес-реліз Європейської комісії від 12 вересня 2018 року / Press release. State of the Union 2018: European Commission proposes measures for securing free and fair European elections
18. Боротьба з дезінформацією в Інтернеті: європейський підхід. Комунікація Комісії до Європейського парламенту, ради, Європейського економічного та соціального комітету і комітету регіонів від 26 квітня 2018 року / Communication from the Commission to the European parliament, the Council, the European economic and social Committee and the Committee of the regions. Tackling online disinformation: a European Approach
19. Боротьба з дезінформацією в Інтернеті: експертна група виступає за більшу прозорість між онлайн-платформами. Прес-реліз Європейської комісії від 12 березня 2018 року / Press release. Tackling disinformation online: Expert Group advocates for more transparency among online platforms
20. Проект Регламенту Європейського парламенту та ради щодо поваги до приватного життя та захисту персональних даних в електронних комунікаціях та скасування Директиви 2002/58/ЕС (Регламент про приватність та електронні комунікації) від 10 січня 2017 року / Proposal for a Regulation of the European parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)
21. Регламент ради ЄС 2016/679 від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних та про вільний рух таких даних, а також про скасування Директиви 95/46/ЕС (Загальний регламент захисту даних) [2016], OJ L 119/1 / Regulation (EU) 2016/679 of the European parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
22. Директива 2002/58/ЕС Європейського парламенту та ради від 12 липня 2002 року щодо обробки персональних даних та захисту приватності в секторі електронних комунікацій (Директива про приватність та електронні комунікації) [2002], OJ L 201/37 / Directive 2002/58/EC of the European parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
23. Рекомендація № R(99) 15 Комітету міністрів до держав-членів про заходи щодо висвітлення виборчих кампаній у засобах масової інформації від 9 вересня 1999 року / Recommendation No. R(99) 15 of the Committee of Ministers to member States on measures concerning media coverage of election campaigns