ДЕЗІНФОРМАЦІЯ ТА ВИБОРЧІ КАМПАНІЇ

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Дезінформація та виборчі кампанії

Ів-Марі Дубле

Генеральний директорат із питань демократії
Демократичне врядування
Управління з виборчого сприяння

Рада Європи

За висловлені в цій роботі міркування відповідальність несе виключно автор, і такі міркування не обов'язково відображають офіційну політику Ради Європи.

Обкладинка та дизайн:
Департамент із питань виготовлення документів та публікацій (SPDP), Рада Європи

Фото на обкладинці: © Depositphotos

Видавництво Ради Європи
F-67075, Strasbourg Cedex
(Страсбург, Франція)
book.coe.int

Видання французькою мовою:
Yves-Marie Doublet
Désinformation et campagnes électorales
ISBN 978-92-871-8910-3

Видання англійською мовою:
Yves-Marie Doublet
Disinformation and electoral campaigns
ISBN 978-92-871-8911-0

Неофіційний переклад та видання цієї публікації українською мовою здійснено за підтримки проєкту Ради Європи «Підтримка прозорості, інклюзивності та чесності виборчої практики в Україні»

Зміст

Вступ

1. Кембриджський словник тлумачить фейкові новини так: «схожі на новини фальшиві історії, які поширюють в інтернеті або за допомогою інших засобів масової інформації та які зазвичай створено для впливу на політичні погляди або задля жарту».

2. Із літа 2016 року під фейковими новинами розуміють навмисне вірусне поширення фальшивих новин в інтернеті та соціальних мережах[1]. Це можуть бути сфабриковані, маніпулятивні матеріали, матеріали від «самозванців» (фальшивих сайтів/сторінок, схожих на відомі оригінали), матеріали, що вводять в оману, фальшивий контекст або канал зв'язку, сатира та пародія. Відповідно це поняття вживають у різних значеннях. The Guardian була першою газетою, яка згадала маленьке містечко Велес у Македонії, звідки походить таке явище. На політичних сайтах цього міста вдавалися до так званого «клікбейту» — засобу, який застосовують, аби заохотити відвідувачів перейти за посиланням на певну вебсторінку, — для того щоб заробляти гроші від «трампоманії» (Trumpmania) під час американської виборчої кампанії 2016 року. Підлітки цього містечка керували понад 100 сайтами з фейковими новинами. Розслідування, проведене 3 листопада 2016 року американським сайтом Buzzfeed, за кілька днів до президентських виборів у США, пояснює успіх цього феномена: «Найкращий спосіб здійняти галас — ділитися політичними публікаціями у Фейсбуку із сенсаційним та часто недостовірним контентом, який може потішити прихильників Трампа»[2].

3. Така специфіка роботи передбачає потребу в розмежуванні помилкової інформації, дезінформації та пропаганди, які точно описала американська дослідниця Рене Діреста, керівник відділу політики організації «Дані для демократії»[3]. Зокрема, помилкова інформація пов'язана з неналежною або недостовірною інформацією, яку подають журналісти без будь-якого злого умислу. А дезінформація — це навмисна спроба змусити людей повірити в ті речі, які є неточними. До дезінформації належить сфабрикована, змішана з фактами та реальними подіями інформація, яка суттєво відрізняється від будь-яких схожих на новини даних, а також це автоматизовані облікові записи, які використовують для функціонування мереж прихильників фейкових новин, зрежисовані відео чи цільова реклама[4]. Таку техніку використовує одна група, щоб таргетувати іншу групу (здійснити на неї вплив, скеровуючи її у потрібному напрямку) та ввести в оману читачів.

4. У цій ієрархії різних способів комунікації під пропагандою розуміють інформацію визначеного спрямування, яку поширює уряд, певні групи чи окремі люди. У листопаді 2017 року британська прем'єр-міністерка заявила, що насаджування фейкових новин — це спосіб «озброєння інформації»[5]. Усі ці різні канали часто об'єднуються під прапором фейкових новин, але засоби та наміри відрізняються від одного типу інформації до іншого. Із соціальної точки зору фейкові новини сприяють формуванню спільнот людей, які мають доступ до однакових джерел, поділяють ту саму ідеологію та ті самі теорії змови[6].

5. Фейкові новини можуть набувати декількох форм: вони можуть складатися з тверджень, висловлення думок без будь-яких доказів, або з використання мови ненависті до соціальних груп чи меншин. Навіть якщо ініціатива, яка стоїть за такою маніпуляцією громадської думки, має приватний ха-

---

[1] Фейкові новини — визначення та правовий статус // Fake News — Definition und Rechtslage, Wissenschaftlicher Dienste, Deutscher Bundestag, 2017.

[2] Правдива історія про фейкові новини // L'histoire vraie des fake news, L'Opinion, 1315, 7 серпня 2018 року.

[3] Як у наш час зрозуміти, що є правдою? // How do we know what's true anymore? Ютуб, 13 квітня 2018 року.

[4] Багатовимірний підхід до дезінформації // A multi-dimensional approach to disinformation, Звіт Незалежної експертної групи високого рівня з питань фейкових новин та дезінформації в інтернеті, Європейська комісія, 12 березня 2018 року.

[5] Бучан Л. Тереза Мей попереджає Росію про втручання у вибори та закликає захистити Велику Британію // Buchan L. Theresa May warns Russia over election meddling and vows to protect the UK, The Independent, 13 листопада 2017 року.

[6] Жіжек С. Фейкові новини, куди не кинь оком // Zizek S. Fake News, Wohin das Auge reicht, Neue Zürcher Zeitung, 6 серпня 2018 року.

рактер, деякі уряди намагаються контролювати соціальні медіа для формування громадської думки та протидії опозиції і критиці.

6. За останні кілька років ця практика, яка заважає громадянам приймати обґрунтовані рішення, набирає обертів. Уплив цього феномена особливо значний через надзвичайну швидкість його поширення, а також через те, що пошук авторів таких кампаній та цифрових матеріалів дуже складний.

7. Зростання обсягів фейкових новин обґрунтовують кілька чинників.

Уплив соціальних медіа — 2016 року активних користувачів мережі Фейсбук було 2 мільярди на місяць, а користувачів Твіттера — 400 мільйонів осіб. Щомісяця близько 1,8 мільярда користувачів заходять на відеохостинг Ютуб. У своєму звіті Digital News Report 2018 Інститут із вивчення журналістики Reuters вважає Фейсбук найважливішою мережею для пошуку, читання, перегляду та обміну новинами, навіть з урахуванням того, що користування Фейсбуком упало з 42% 2016 року до 36% 2018-го. У США 62% дорослих отримують новини із соціальних медіа[7]. Для кожної вікової групи до 45 років новини в інтернеті мають важливіше значення, ніж телевізійні новини.

Способи та їхня швидкість — Фейсбук створив цільову парадигму, що дозволяє політичним партіям під час виборчих кампаній мати доступ до понад 162 мільйонів користувачів у США та індивідуально таргетувати їх відповідно до їхнього віку, статі, виборчого округу й інтересів[8]. Зокрема, наголошено, що цифрові медіа використовують алгоритмічні процеси для таргетування як клієнтів, так і виборців. Облікові записи ботів використовують для впливу на політичний дискурс. Через них роблять твіти та ретвіти з лайками й фоловерами, аби охопити широку аудиторію, але такі лайки та фоловери часто є штучними. Навіть більше, недавнє дослідження Массачусетського технологічного інституту показало, що фальшиві новини поширюються швидше, ніж реальні. Згідно з цим дослідженням у фальшивих новин на 70% більше шансів на ретвіт, ніж у правдивих історій, а правдивим історіям потрібно приблизно в шість разів більше часу порівняно з фальшивими новинами, аби бути побаченими 1 500 особами[9].

Витрати — Це стало дешевшим і базується на короткотерміновій стратегії, що не має на меті створення репутації якості. Для фінансування пропаганди в соціальних мережах потрібно всього 40 000 євро; 5 000 євро — достатня сума, аби «купити» ініціативу щодо мови ненависті, а за 2 600 євро ви можете придбати 300 000 фоловерів у Твіттері[10]. Фальшиву та шкідливу інформацію створюють для отримання прибутку. Отже, упродовж декількох років між цифровими компаніями та медіабізнесом укладався «шлюб», і політичні кампанії поєднували профілі виборців із комерційною інформацією від інформаційних брокерів. Як наслідок — зросло значення політичного маркетингу, який спирається на дані. Усе це може мати значний вплив на суспільство, чесні вибори та демократію.

8. Така тенденція викликає низку запитань. Чи фейкові новини настільки відрізняються від фальшивої інформації, яку використовували в минулому, наприклад, обидві супердержави під час холодної війни? Чи змінюють соціальні медіа ті практики, до яких традиційно вдавалися під час виборчих кампаній? Чи дійсно вплинули фейкові новини на результат виборів? Чи варто розглядати такі практики як неминучі побічні наслідки технологічного зрушення, особливо через те, що їх важко врегулювати? Чи варто покладатися на саморегулювальний підхід, реагуючи на таке явище, або це потребує все ж прийняття жорстких правил — особливо якщо саморегулювальний підхід виявляється неефективним, зокрема, коли такі практики застосовують за межами території, де відбуваються вибори? Чи відповідає такий регуляторний підхід принципу свободи вираження поглядів? Які правові інструменти було запроваджено в різних державах-членах Ради Європи або в інших країнах для протидії фейковим новинам? Які уроки з цього досвіду можна зробити? Як гарантовано захист приватного

---

[7] Алькотт Х., Генцков М. Соціальні медіа та фальшиві новини на виборах 2016 року // Allcott H., Gentzkow M. Social Media and Fake News in the 2016 Election, Journal of Economic Perspectives, т. 31, № 2, 2017, с. 211–236.

[8] Честер Дж. Роль цифрового маркетингу в політичних кампаніях // Chester J. The role of digital marketing in political campaigns, Огляд інтернет-політики, Центр цифрової демократії, Вашингтон, 31 грудня 2017 року.

[9] http://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308.

[10] www.assemblee-nationale.fr/15/pdf/rapports/r0990.pdf.

життя громадян? Чи потрібно вживати юридичних заходів на міжнародному рівні з огляду на численні випадки дестабілізації виборчих кампаній, що фіксуються останнім часом у різних країнах? Окрім можливого використання нормативно-правової бази, як ще можна підвищити поінформованість громадськості щодо автентичності інформації та необхідності перевірки фактів на додаток до заохочення до більш ретельного редакційного аналізу в ЗМІ?

9. Мета цього звіту — відповісти на ці запитання та надати пропозиції щодо формування відповідної нормативно-правової бази на рівні Ради Європи.

1. Загальний огляд ситуації

10. Випуск фейкових новин можна розглядати як із технічної, так і з політичної точки зору.

1.1. Технічні дані

11. Щоб забезпечити обізнаність щодо важливості технічних питань у цьому контексті, ми повинні пригадати різні методи, які можна використовувати в соціальних медіа.

12. Дослідження показують, що більше людей дізнаються про новини завдяки алгоритмам (пошуковим, соціальним тощо)[11], ніж завдяки виданням, і ці алгоритми надають більшості користувачів доступ до значно більшої кількості онлайн-ресурсів. Алгоритми — не нейтральні засоби. Їх розробили з максимальною точністю саме для здійснення вибірки, сортування, класифікації, ранжування, фільтрування, таргетування та здійснення запитів на доступну інформацію або екстрені новини. Вони є способом організації інформації у великих масштабах шляхом посилення певних її аспектів. Обчислювальні алгоритми застосовують машинне навчання для того, щоб генерувати результати. Алгоритми машинного навчання використовують як «узагальнювачі», надаючи дані, на основі яких обчислювальні алгоритми зможуть навчатися. Алгоритм самостійно приймає рішення щодо операцій, які необхідно здійснити для виконання конкретного завдання. Така техніка дає можливість виконати набагато складніші завдання порівняно зі звичайним алгоритмом. Ендрю Ин зі Стенфордського університету визначає машинне навчання як «науку про те, як змусити комп'ютери діяти без явного програмування». Таке навчання охоплює планування, аналіз, розроблення та впровадження методів, які дають змогу комп'ютеру здійснювати операції систематичним шляхом та виконувати складні завдання.

Нині розроблено реальну бізнес-модель, яка базується на монетизованому зборі даних та на нагляді за індивідуальною поведінкою в інтернеті[12]. Саманта Бредшоу з Оксфордського інтернет-інституту розповіла Комітету з цифрових технологій, культури, ЗМІ та спорту Палати громад про силу Фейсбука у маніпулюванні емоціями людей шляхом показування для них різних типів історій: «Якщо б ви показали їм більше негативних історій, вони відчули б ще більше негативу. Якби показали їм позитивні історії, вони відчули б більше позитиву»[13]. Варто пригадати, що за версією Оксфордського словника словом 2016 року стало «post-truth» («постправдивий»), прикметник, що стосується обставин або позначає їх, за яких об'єктивні факти не мають такого впливу на формування громадської думки, як апелювання до емоцій та особистих переконань. Використання аналітики даних, заснованої на психологічному профілі аудиторії, лягло, наприклад, в основу роботи компанії Cambridge Analytica, яка з'явилася 2012 року з уже створеної консультаційної групи SCL, що працювала над «представленням факту, підкріпленого емоцією».

13. Колишній генеральний директор Cambridge Analytica дав свідчення перед згаданим вище комітетом:

> Для того щоб виборці отримували «правильний» тип повідомлень, Cambridge Analytica потребувала інформації про виборців, наприклад, про те, які товари вони купували, які ЗМІ читали, на яких автомобілях їздили. The Guardian після розслідувань, що тривали близько року, написала: «[Cambridge Analytica]... платила дослідникам із Кембриджського університету, аби зібрати детальні психологічні профілі американського електорату, використовуючи величезний пул американських користувачів Фейсбука, які здебільшого про це не здогадувалися, сформований за допомогою онлайн-опитування[14].

---

[11] Ньюмен Н. Загальний зміст та ключові висновки // Newman N. Executive Summary and Key Findings, Reuters Institute Digital News Report 2017.

[12] Як людям зберегти ініціативу? Етичні питання, порушені алгоритмами та штучним інтелектом // How can humans keep the upper hand? The ethical matters raised by algorithms and artificial intelligence, Національна комісія з питань інформаційних технологій і прав людини, грудень 2017 року. Доступно за посиланням: www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf.

[13] https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf.

[14] Там само.

Щоб скеровувати виборців, упливаючи на них, та надсилати їм відповідні повідомлення, організатори кампаній використовують пристосовані до конкретних груп населення інструменти мікронацілювання (мікротаргетування). Для опису мікронацілювання також вдаються до терміна «темна реклама» («dark ads»).

14. Експерти використовують вираз «політична ехокамера» як метафору для онлайн-кліків, що призводять до появи політичної «бульбашки», у яку люди можуть потрапити під час користування онлайн-сервісами. Далі наведено приклад того, як алгоритмічні канали стимулюють упередженість.

> Якщо ви читаєте новини з ліберальних джерел або навіть просто маєте здебільшого ліберальних друзів, Фейсбук запропонує вам ще більше новин ліберального характеру. Те саме відбувається і з консерваторами, навіть із найбільш маргінальними членами політичного спектру. Коротко кажучи, це посилене алгоритмами підтверджувальне упередження означає: що більше ви читаєте інформацію, із якою погоджуєтеся, то частіше Фейсбук показуватиме вам ще більше інформації, із якою ви погоджуєтеся... Що більше ви чуєте аналогічні точки зору з одних і тих самих джерел, то більше це підкріплює ваші ідеї, жодного разу не ставлячи їх під сумнів[15].

15. Але дані та алгоритми «непрозорі у тому сенсі, що реципієнт результату алгоритму не має конкретного уявлення, як і чому ввідні дані (інформація, яку отримав алгоритм) призвели до певної категоризації. Навіть більше, самі ввідні дані можуть бути абсолютно невідомими або відомими лише часткове»[16]. Stirista, фірма, яка спеціалізується на цифровому маркетингу, пропонує схоже моделювання для виявлення людей, які є потенційними прихильниками й виборцями. Компанія стверджує, що для 155 мільйонів виборців нею було визначено «адреси електронної пошти, файли cookie та імена у соцмережах», а також «культурні вподобання, релігію, інтереси, політичні погляди та сотні інших деталей для створення насичених інформацією, докладних профілів виборців»[17]. Якщо чиєсь політичне переконання не завжди формується завдяки алгоритмам, алгоритми можна використати для визначення профілю виборців. Це стало частиною бізнес-моделі, оскільки це — спосіб заробітку грошей.

16. Непрозорість алгоритмів порушує два питання: чи результат є наслідком волі розробника платформи? І чи користувач може відстежити цей результат? Деякі небажані впливи алгоритмів було створено навмисно, але вони невідомі користувачам. У таких випадках непрозорість описують як навмисну стратегію приховування та маніпулювання споживачами або виборцями. Програмісти, органи державної влади, громадські організації та журналісти мають перевіряти ці алгоритми та їхні приховані цілі. В інших випадках оператори можуть не планувати таких впливів, і користувачі виявлятимуть ці впливи або ж не виявлятимуть їх[18].

17. «Бот» — ще один майстерний механізм впливу на виборців. Це автоматизована комп'ютерна програма, яка імітує поведінку людини в соціальних медіа через публікації, проставляння «лайків» та спілкування з реальними людьми[19]. Один німецький експерт наголошує: «Соціальні боти — це фейкові облікові записи в соціальних мережах, які прикидаються реальними людьми»[20]. Людина, яка керує лише одним ботом, може впливати на мільйон людей. Наприклад, боти можуть поляризувати громадську думку завдяки мові ворожнечі. Під час цього самого слухання перед Комітетом Бундестагу з питань цифрової політики експерт поставив ботів у один ряд із методами, пов'язаними з «низькоякісною високочастотною маніпуляцією». Вони відрізняються від певних фейкових новин, які асоціюють із «високоякісною низькочастотною маніпуляцією»[21]. За оцінками постачальника хмарних

---

[15] https://lifehacker.com/how-sites-like-google-and-facebook-put-you-in-political-1787659102.

[16] Бюррелл Дж. Як «думає» машина: розуміння непрозорості в алгоритмах машинного навчання // Burrell J. How the machine 'thinks': Understanding opacity in machine learning algorithms, Big Data and Society, січень 2016 року, с. 1–12.

[17] Честер Дж., наведено вище.

[18] Кардон Д. Можливості алгоритмів // Cardon D. Le pouvoir des algorithmes, Pouvoirs, La Datacratie, 164, 2018.

[19] Цифрова агітація: підвищення прозорості для виборців // Digital campaigning: Increasing transparency for voters, Виборча комісія, червень 2018 року.

[20] Гегеліч С. Опитувальник Комітету з питань цифрової політики // Hegelich S. Ausschuss Digitale Agenda Fragenkatalog, Deutscher Bundestag Auschussdrucksache 18 (24) 125.

[21] Фейкові новини, соціальні боти, хакерство та спроби спільного маніпулювання демократичними процесами прийняття рішень у Мережі // Fake News, Social Bots, Hacks und Co-Manipulationsversuch demokratischer Willensbildungsprozesse im Netz, Протокол 81 засідання, 25 січня 2017 року, Бундестаг ФРН.

послуг Imperva Incapsula, 2016 року діяльність ботів становила 51,2% всього вебтрафіку. Тоді як чимало з них мають комерційні наміри, боти-зловмисники лишаються неідентифікованими та можуть бути використані для хакерства, спаму або крадіжки контенту[22].

18. Відповідно до виборчого законодавства Великої Британії учасники кампанії можуть купувати ботів і платити людям за поширення своїх агітаційних повідомлень. Проте, якщо виборці не можуть цього помітити, то таку ситуацію вважають уведенням в оману[23].

19. «Троль» — це реальна людина, яка проводить час у інтернеті та соціальних медіа, публікуючи повідомлення та коментарі, що стимулюють суперечки і чвари, або ж недоречні повідомлення та коментарі, аби роздратувати чи розгнівити інших людей[24].

20. Гештеги — короткі коди, які вставляють у повідомлення для можливості відстеження цих повідомлень, — також використовують під час виборчих кампаній. Популярні гештеги містять «актуальні теми», які надають доступ до «розмов». Гештеги використовують боти. Поширювані гештеги відображають думку дуже незначної кількості людей, які мають велику кількість облікових записів. Створюється враження, що вони представляють думку великої кількості людей. Прості короткі коди змушують людей повірити в те, що погляд виражає широко поширену думку[25].

21. 2011 року витрати кампаній на цифрову рекламу становили 0,3% від загальних витрат на рекламу у Великій Британії. 2017 року ці витрати зросли до 42,8% від загальних витрат на рекламу[26].

1.2. Політичні дані

22. Соціальні медіа були високо оцінені за забезпечення доступності демократичної інформації та заохочення до онлайн-спілкування, що робить політичну інформацію доступнішою та допомагає виборцям зробити більш поінформований вибір. У рішенні від 10 березня 2009 року у справі «*Компанія "Таймс Ньюспейперс Лтд." проти Сполученого Королівства*» (Times Newspaper Ltd v. the United Kingdom) Європейський суд з прав людини зазначив:

> «З огляду на свою доступність та здатність зберігати й передавати величезну кількість інформації інтернет відіграє важливу роль у покращенні доступу громадськості до новин та полегшенні поширення інформації загалом»[27].

Але соціальні медіа можуть використовуватися на шкоду та здатні впливати на політичні переконання.

23. Для того щоб виявити вплив мереж фейкових облікових записів та ботів на голоси виборців, було досліджено виборчі кампанії у США, референдум у Великій Британії 2016 року щодо членства у ЄС, вибори президента Франції, загальнонаціональні вибори у Великій Британії та Німеччині 2017 року та президентські вибори у Чехії 2018 року.

24. Під час президентських виборів у США 2008 та 2012 років агітаційні групи Барака Обами мали у своєму розпорядженні безліч наборів даних практично щодо всіх виборців. Загальновизнано, що фейкові новини могли посприяти перемозі Дональда Трампа на президентських виборах у США 2016 року. На соціальні медіа припадало 13,8% джерел новин про вибори під час виборчого процесу 2016 року в США. Фейкові новини поширювалися задля сприяння перемозі Дональда Трампа та явно були орієнтовані йому на користь. База даних, зібрана завдяки проведеному дослідженню, налічує 115 фейкових історій на користь Трампа, якими ділилися у Фейсбуку загалом 30 мільйонів разів, та 41 фейкову історію на користь Клінтон, якими ділилися загалом 7,6 мільйона разів[28]. Серед цих фейкових історій було і повідомлення про те, що Папа Римський підтримує кандидатуру Дональда Трампа.

---

[22] Свобода у Мережі 2017: «Маніпуляція соціальними медіа для підриву демократії» // Freedom on the Net 2017: «Manipulating social media to undermine democracy».

[23] *Цифрова агітація: підвищення прозорості для виборців,* наведено вище.

[24] Там само.

[25] *Правдива історія про фейкові новини,* наведено вище.

[26] *Цифрова агітація: підвищення прозорості для виборців,* наведено вище.

[27] Пункт 27 рішення.

[28] Алькотт Х., Генцков М., наведено вище, с. 211–236.

Загалом агітаційна кампанія у Фейсбуку мала вирішальне значення для перемоги Трампа. Президентська кампанія Трампа витратила більшу частину свого бюджету на цифрову рекламу у Фейсбуку. Було надіслано 5,9 мільйона повідомлень цільовим виборцям, тоді як Гілларі Клінтон надіслала лише 66 000 повідомлень[29]. Можна вважати, що у «хитких» штатах, де різниця між прихильністю до кандидатів була незначною, такі таргетовані повідомлення мали вирішальний вплив на результат президентських виборів у США.

25. У згаданому вище проміжному звіті Комітету з цифрових технологій, культури, ЗМІ та спорту Палати громад щодо питань дезінформації і фейкових новин, який було опубліковано 29 липня 2018 року, зазначено: «Під час президентських виборів росіяни стоять за понад 3 000 рекламними оголошеннями у Фейсбуку та Інстаграмі, що просували 120 сторінок у Фейсбуку, під час кампанії, яка охопила 126 мільйонів американців»[30]. На слуханнях у квітні 2018 року перед Конгресом США CEO Facebook Марк Цукерберг пояснив, що російські облікові записи здебільшого використовували рекламу для впливу на погляди щодо певних питань, а не для просування конкретних кандидатів чи політичних повідомлень.

26. Щодо британського референдуму 2016 року, на якому стояло питання про членство у ЄС, спільний дослідницький проєкт Університету Свонсі та Каліфорнійського університету в Берклі нарахував 156 252 російські облікові записи з твітами про Брекзіт і встановив, що вони опублікували понад 45 000 повідомлень щодо Брекзіту за останні 48 годин кампанії[31]. За даними комунікаційної агенції 89up, Russia Today (RT) та Sputnik опублікували в період з 1 січня до 23 червня 2016 року 261 статтю про референдум щодо ЄС, висловлюючи антиєвропейські погляди. У звіті також було показано, що RT та Sputnik досягли більшого охоплення в Твіттері у контексті антиєвропейських виступів, аніж кампанії «Vote Leave» або «Leave» («Проголосуй за вихід» або «Виходьмо»)[32].

27. У контексті виборів президента Франції 2017 року дослідження виявило незвичні схеми використання облікових записів, які припускали можливість існування чорного ринку багаторазових ботів, що використовувалися з метою політичної дезінформації[33]. На основі бази, що становила 17 мільйонів зібраних постів, виявили, що користувачі, які «зливали інформацію» на Макрона, були не французькими користувачами з різноманітними політичними поглядами, а здебільшого іноземцями, що мали інтерес до ультраправих тем та альтернативних ЗМІ.

28. Торкаючись питання загальнонаціональних виборів у Великій Британії 2017 року, в звіті Інтернет-інституту Оксфордського університету щодо проєкту про комп'ютерну пропаганду встановлено, що обсяг «низькосортних макулатурних новин», визначених як «оманлива, брехлива або некоректна інформація, яка дуже схожа на дійсну новину про політику, економіку та культуру», становив 11,4% поширюваного контенту[34].

29. Якщо спостерігати за впливом фейкових новин на загальні вибори в Німеччині 2017 року, можна зазначити, що закордонні фейкові новини мали обмежений вплив. Більшість фейкових новин поширювалися ультраправими силами. Соціальні медіа не були постійно в пріоритеті; використовували також традиційні засоби масової інформації. Увагу фейкових новин було зосереджено здебільшого на двох темах: біженці та злочинність. Обмежену роль соціальних медіа серед інформаційних каналів у Німеччині, якщо порівнювати зі США, можна пояснити незначним впливом фейкових новин. Найвагоміша фейкова новина стосувалася очікуваної бійки 1000 мігрантів у невеликому містечку в Баден-Вюртемберзі. Цю новину поширили 500 000 осіб[35].

---

[29] *Правдива історія про фейкові новини*, наведено вище.

[30] https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36302.htm.

[31] Брекзіт Путіна? Вплив кремлівських медіа та ботів під час референдуму у Великій Британії 2016 року // Putin's Brexit? The influence of Kremlin media and bots during the 2016 UK EU referendum, 89up, лютий 2018 року.

[32] Російські облікові записи у Твіттері агітували за Брекзіт перед референдумом щодо ЄС // Russian Twitter accounts promoted Brexit ahead of EU referendum, Reuters, 15 листопада 2017 року.

[33] Феррара Е. Дезінформація та соціальний бот, операції напередодні виборів президента Франції 2017 року // Ferrara E. Disinformation and social bot, operations in the run-up to the 2017 French Presidential Election, *First Monday,* 22 (8) 2017 року.

[34] www.niemanlab.org/2017/06/brits-and-europeans-seem-to-be-better-than-americans-at-not-sharing-fake-news/.

[35] Сендерлауб А., Майер М., Дітер-Рюль В. Факти замість фейків // Sängerlaub A., Meier M., Dieter-Rühl W. Fakten statt Fakes, Stiftung Neue Verantwortung, березень 2018 року.

30. Докази, які було отримано з результатів дослідження численних популярних статей на сторінках Фейсбука, також підкреслюють роль іноземного впливу та дезінформації під час останніх президентських виборів у Чехії 2018 року[36].

31. Деякі спостерігачі вважають, що на поширення дезінформації потрібно поглянути в ширшому контексті. Ця практика існувала завжди, оскільки вона є невід'ємною частиною політичної дискусії. Канцлер Отто фон Бісмарк говорив, що люди ніколи не брешуть так, як після полювання, під час війни або перед виборами. Майже для кожної епохи існують виразні історичні приклади політичної брехні. Такі приклади можна навести щодо Румунії V століття, Франції XVII століття та Німеччини XIX століття, а також у всьому світі в XX столітті[37].

1.3. Інтенсифікація процесу

32. Навіть якщо вплив дезінформації в різних країнах неоднаковий, швидке поширення цього явища, його технічна розвиненість у контексті швидкості, масштабів та екстратериторіальності, його безпечне сприйняття суспільством і порівняно невеликі обсяги фінансових затрат — усе це уособлює великі зміни та загрози не лише для виборчого процесу, а й для наших демократій загалом. Консалтингова та дослідницька група Gartner вважає, що до 2020 року штучний інтелект як інструмент дезінформації перевершуватиме штучний інтелект, який використовують для виявлення такої дезінформації[38].

33. Багато води спливло з часу прийняття резолюції Європейського парламенту «Стратегічні комунікації ЄС як протидія пропаганді третіх сторін» 2016 року[39].

34. Це питання стосується все більшої і більшої кількості країн. У звіті за 2017 рік проєкт «Freedom on the Net» представив комплексне дослідження свободи інтернету в 65 країнах, які охоплюють 87% світових користувачів інтернету. Було вказано на поширеність політичних ботів у 20 країнах, існування практики фейкових новин довкола виборів у 16 країнах та використання зламаних облікових записів у 10 країнах. У 20 країнах, де набули поширення політичні боти, характерні моделі онлайн-активності вказують на координоване використання ботів для впливу на політичний дискурс[40].

35. Мабуть, зрозуміло, що зазначені вище випадки впливу соціальних медіа на виборчі кампанії в західних демократіях не поодинокі. Докази формально організованих маніпулятивних кампаній у соціальних медіа у 48 країнах (порівняно з 28 країнами минулого року) представлено Оксфордським університетом у дослідницькому проєкті щодо комп'ютерної пропаганди[41]. У кожній країні є щонайменше одна політична партія чи державна установа, яка використовує соціальні медіа для маніпуляції громадською думкою на національному рівні. Невеликі країни з менш освіченими виборцями можуть бути більш уразливими до недостовірних новин та дезінформації, ніж великі країни з більш освіченими виборцями і якісною журналістикою.

36. Цифрові операції з дезінформації впливають на більшу кількість виборців порівняно з традиційними способами. Ми можемо очікувати зростання ваги такої практики порівняно з традиційною, оскільки цифрові методи дають змогу охопити ширшу аудиторію. Прихильники політиків сприяють зміцненню такої тенденції. У доцифрову епоху політичні активісти зі схожими поглядами витратили

---

[36] www.europeanvalues.net/wp-content/uploads/2018/02/The-role-of-the-Kremlin%E2%80%99s-influence-and-disinformation-in-the-CECH-presidential-elections.pdf.

[37] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digi-tal-culture-media-and-sport-committee/fake-news/written/85595.html. Також Уїґ Ф.-Б. Дезінформація: зброя брехні, боротьби та хаосу в інформаційному суспільстві // Huyghe F.-B. Désinformation: armes du faux, lutte et haos dans la société de l'information, Sécurité globale, № 6, 2016, с. 64.

[38] Gartner. Gartner оприлюднив основні прогнози для IT-організацій та користувачів у 2018 році, та не тільки // Gartner. Gartner Reveals Top Predictions for IT Organizations and Users in 2018 and Beyond, прес-реліз, 3 жовтня 2017 року.

[39] 23 листопада 2016 року (2016/2030 (INI)): параграф 52: «[Європейський парламент] підкреслює, що особливу увагу варто приділяти новим технологіям — включно з цифровим мовленням, мобільним зв'язком, онлайн-медіа та соціальними мережами, зокрема тими, що мають регіональний характер, — що полегшує поширення інформації про…».

[40] Свобода у Мережі 2017: «Маніпуляція соціальними медіа для підриву демократії, 2018» // Freedom on the Net 2017: «Manipulating social media to undermine democracy, 2018», Freedom House.

[41] http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf.

б набагато більше часу, намагаючись охопити виборців — адже мали б ходити від одних дверей до інших, аби зібрати інформацію та переконати людей проголосувати.

37. Способи, розроблені інформаційними брокерами для розуміння психологічного профілю виборців, як бачимо, значно інвазивніші, ніж у минулому, завдяки алгоритмам та пошуковим системам.

38. Здавалося б, алгоритми посилюють схильність особи до сприйняття лише тих об'єктів, людей, думок і культур, які відповідають її інтересам. Один із висновків звіту Французького управління з питань захисту даних у грудні 2017 року про етичні питання, які постали у зв'язку з використанням алгоритмів та штучного інтелекту, полягав у тому, що персоналізація інформації може призвести до надзвичайної фрагментації публічного простору й зникнення мінімального «набору» основної інформації, який поділяють люди. Це спричиняє атомізацію політичної спільноти.

39. Також виникає питання про право на приватне життя. У таких країнах, як США, з огляду на Першу поправку, яка гарантує свободу слова, використання політичних даних не захищене. У зв'язку з цим європейські країни на відміну від США розробили загальні правила конфіденційності, які можна використати для активізації зусиль із протидії дезінформації.

40. Цифрові технології змінюються дуже швидкими темпами й продовжують розвиватися. Шкода від нинішніх фейкових новин блякне порівняно зі шкодою, яка може йти від «глибинних фейків». Це стосується імітації мови та образів за допомогою штучного інтелекту з метою створення альтернативних реалій — показу того, як хтось говорить чи робить те, що він/вона ніколи не говорили чи не робили. Найпростіша форма глибинних фейків — надання комп'ютеру відповідних указівок, а також завантаження зображень та голосових записів певної особи, щоб навчити його імітувати голос цієї особи[42].

41. Для того, щоб спростувати чутки, які поширюються в Твіттері, необхідно від 12 до 14 годин[43]. Отже, вплив недостовірних новин напередодні дня голосування може мати руйнівне значення.

42. Релятивізм у наших суспільствах набирає обертів. Це означає, що істинність та хибність, правильне і неправильне, стандарти міркування та процедури обґрунтування розглядають як продукти різних угод/домовленостей і структур оцінювання. Їхні повноваження обмежуються контекстом, який дає їм імпульс для розвитку[44]. Цю думку окреслив філософ Славой Жижек, щоб пояснити розвиток явища фейкових новин у зв'язку з постмодерністською деконструкцією, оскільки люди можуть не розуміти різниці між реальними та фальшивими новинами[45]. Коли журналістка Леслі Шталь взяла інтерв'ю у президента Трампа — це було перше телевізійне інтерв'ю з Трампом після його перемоги на виборах 2016 року. Він підкреслив, що критикує пресу, аби «принизити» та «дискредитувати» журналістів, щоб ніхто не повірив негативним історіям про нього[46]. Ця навмисна стратегія на тлі недовіри до журналістів формує атмосферу, яка підігріває у людей страх та упередження для того, щоб вплинути на їхню поведінку й сприяти дестабілізації виборців, які втрачають точку опори.

43. Збільшення використання цифрових інструментів у політичній агітації має серйозний фінансовий вплив, що необхідно брати до уваги. Усі держави-члени Ради Європи запровадили регулювання політичного фінансування відповідно до Рекомендації Rec(2003)4 про загальні правила щодо протидії корупції у фінансуванні політичних партій та виборчих кампаній. Ці правила містять положення про межі витрат, прозорість ресурсів, моніторинг та санкції. Таку нормативно-правову базу впроваджують поетапно завдяки імпульсу GRECO (Група держав проти корупції).

У більшості країн-членів Ради Європи чинні правові норми щодо фінансування кампаній не потребують подання інформації щодо використання цифрових матеріалів, і, якщо закордонні пожертви на користь політичних партій чи кандидатів заборонені, жодні правила прямо не забороняють витрати за кордоном.

---

[42] https:// whatis.techtarget.com/ definition/deepfake.

[43] Звіт № 677 (2017–2018) Катрін Морен-Десаї, Комісія з питань культури, освіти та комунікацій Сенату Франції // Rapport n° 677 (2017–2018) de Mme Catherine Morin-Desailly, La commission de la culture, de l'éducation et de la communication du Sénat français),18 липня 2018 року (французькою мовою).

[44] https://plato.stanford.edu/entries/relativism/.

[45] Жижек С., наведено вище.

[46] www.cnbc.com/2018/05/22/trump-told-lesley-stahl-he-bashes-press-to-discredit-negative-stories.html.

У Великій Британії під час кампанії, присвяченій референдуму щодо членства в ЄС, «Vote Leave» («Проголосуй за вихід», основна організація, що реалізовувала кампанію за вихід Великобританії з ЄС), яка широко використовувала цифрові агітації, зазнала критики через фінансування таких цифрових інструментів. Дозволений ліміт витрат під час кампанії, присвяченій референдуму, становив 7 мільйонів фунтів стерлінгів. Вважається, що Арон Бенкс, якого позиціонують як людину, близьку до груп, що обстоюють російські інтереси, пожертвував 8,4 мільйона фунтів стерлінгів на кампанію за вихід з ЄС, що стало найбільшою політичною пожертвою в британській політиці. Джерело цих грошей лишається незрозумілим. Мета пожертв від прихованих джерел[47] — вплинути на виборчу кампанію, водночас цифрові виборчі кампанії, проведені з-за кордону з метою впливу на виборців, послаблюють правила політичного фінансування, засновані на прозорості, й навіть можуть зробити їх неефективними/недійсними.

1.4. Можливі відповіді

44. Із точки зору законодавства ЄС правовий статус постачальника інтернет-послуг має бути конкретним. Для докладного розуміння обов'язків постачальника послуг необхідно звернути увагу на статтю 14 директиви 2000/31[48]. Відповідно до тлумачення вказане правило застосовується до постачальника інтернет-послуг за умови, коли сам постачальник не відіграє активної ролі у процесі, тобто він не знає про дані, які зберігаються, або ж не контролює їх. Якщо постачальник не відігравав активну роль у процесі, він не може нести відповідальність за дані, які він зберігав на вимогу рекламодавця, хіба тільки він, дізнавшись про неправочинний характер даних або діяльності самого рекламодавця, оперативно не видалив ці дані або не заблокував до них доступ[49]. Отже, хостинг-провайдер, як наприклад Фейсбук, має видалити незаконне повідомлення лише у разі, коли йому про нього відомо. У документі від 28 вересня 2017 року щодо боротьби з незаконним контентом в інтернеті з метою посилення відповідальності щодо роботи онлайн-платформ Європейський Союз окреслив європейський підхід, поєднавши необхідність швидкого та ефективного вилучення незаконного вмісту, профілактики та кримінального переслідування злочинів для захисту права на вільне спілкування в інтернеті[50]. 1 березня 2018 року Європейська комісія видала рекомендацію щодо заходів для ефективної протидії незаконному онлайн-контенту, яку буде розглянуто в п. 97[51].

45. У контексті протидії практиці поширення фальшивої інформації можливі два варіанти: перший заснований на саморегулюванні, другий — на законодавчому регулюванні.

1.4.1. Саморегулювання

46. Спеціалісти-практики виступають за саморегулювання: Фейсбук та Твіттер заявили про внутрішні ініціативи, пов'язані з наданням громадськості більшої кількості інструментів та інформації, щоб мати змогу визначати, які організації чи приватні особи фінансують політичну рекламу і хто є їхньою запланованою цільовою аудиторією.

---

[47] Параграф 191 Проміжного звіту: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf.

[48] «1. Якщо надаються інформаційні послуги, до яких входить зберігання інформації, що надається одержувачем послуг, держави-члени забезпечують звільнення постачальника послуг від відповідальності за інформацію, яка була збережена за запитом одержувача послуг, при умові, що:

а) постачальник послуг не знає про незаконну діяльність чи інформацію, яка стосується позовів про відшкодування збитків, не обізнаний із фактами чи обставинами, з яких випливає незаконна діяльність чи інформація; або

б) постачальник за умов обізнаності вдається до швидких дій із метою усунення можливості доступу чи відключення доступу до інформації.

2. Пункт 1 не застосовується, якщо одержувач послуг діє під егідою чи під контролем постачальника».

[49] Рішення Європейського суду (Великої палати) від 23 березня 2010 року, *Google France SARL та Google Inc. проти Louis Vuitton Malletier SA* (C-236/08), *Google France SARL проти Viaticum SA та Luteciel SARL* (C-237/08) та *Google France SARL проти Centre national de recherche en relations humaines (CNRRH) SARL та інших* (C-238/08).

[50] https://ec.europa.eu/digital-single-market/en/news/communication-tackling-illegal-content-online-towards-enhanced-responsibility-online-platforms.

[51] https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online.

47. У січні 2018 року Європейська комісія створила Експертну групу високого рівня (HLEG) для консультування щодо політичних ініціатив, пов'язаних із протидією фейковим новинам та дезінформації, яку поширюють в інтернеті. Основним результатом роботи HLEG був звіт, розроблений із метою перегляду найкращих практик у світлі фундаментальних принципів та відповідних реакцій, які випливають із цих принципів[52]. Щоб надати уявлення про зміст звіту, його охарактеризували так: «Добра порція етики, крихта відповідальності»[53].

48. Багатовимірний підхід, рекомендований HLEG, ґрунтується на низці взаємопов'язаних та взаємопідсилювальних реакцій. Ці реакції тримаються на п'яти стовпах, що слугують:

1. підвищенню прозорості онлайн-новин, що передбачає адекватний та сумісний із конфіденційністю обмін даними про системи, які забезпечують циркуляцію інформації в інтернеті;
2. сприянню медійній та інформаційній грамотності для протидії дезінформації і допомоги користувачам у орієнтуванні в середовищі цифрових медіа;
3. розробленню інструментів для розширення можливостей користувачів і журналістів протидіяти дезінформації та сприяти позитивній взаємодії з інформаційними технологіями, що швидко еволюціонують;
4. захисту різноманітності та сталості екосистеми європейських новинних медіа;
5. сприянню постійним дослідженням впливу дезінформації в Європі, спрямованим на оцінювання відповідних заходів, що вживаються різними учасниками процесу для того, щоб регулярно адаптувати/коригувати ці заходи та способи реагування.

49. В очікуванні майбутніх виборів у ЄС, що відбудуться у травні 2019 року*, Європейський Союз висловив стурбованість щодо можливого ризику поширення дезінформації напередодні дня голосування. У зв'язку з цим 26 квітня 2018 року ЄС запропонував до використання Кодекс практики щодо протидії дезінформації для Європейського Союзу. Комісія мала оцінити його застосування шляхом проведення широких консультацій із зацікавленими сторонами та на основі ключових показників ефективності, що ґрунтувалися на цілях документа. Якщо результати виявляться незадовільними, комісія може розглянути подальші заходи, зокрема регуляторні. Комісія підтримала б створення незалежної європейської мережі фактчекерів із метою визначення загальних методів їхньої роботи, обміну найкращими практиками, досягнення максимально широкого охоплення в усіх країнах ЄС та участі в спільних перевірках фактів та пов'язаній із ними діяльності. Це сприяло б підзвітності та відповідальності онлайн, а також використанню нових технологій для боротьби з дезінформацією в довгостроковій перспективі. Комісія звертає увагу на необхідність посилення стійкості суспільства до дезінформації. Про досягнуті успіхи комісія мала відзвітувати до грудня 2018 року.

50. Якщо говорити про ці ініціативи, на увагу заслуговують дві пропозиції: діяльність онлайн-платформ та фактчекінг (перевірка фактів).

51. Щодо діяльності онлайн-платформ HLEG нагадує, що рекламні мережі, функціонування яких забезпечують самі платформи або інші сторони, відіграють важливу роль у їхній стратегії, яка ставить перед собою три цілі:

- рекламні мережі відмовляються розміщувати рекламу на сайтах, які було визначено поширювачами дезінформації; це безпосередньо зменшує дохід постачальників дезінформації;
- постачальники реклами усувають рекламу з джерел дезінформації і з метою забезпечення прозорості чітко визначають політичну рекламу як спонсорований контент;

---

[52] https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation.

[53] Бенсамун А. Європейська стратегія щодо штучного інтелекту: все ще про етику // Bensamoun A. Stratégie européenne sur l'intelligence artificielle: toujours à la mode éthique, Recueil Dalloz, 2018, № 19, с. 1022.

* Тут і далі наведену інформацію зазначено на момент виходу друком оригінального видання. — *Прим. перекладача*.

- рекламні мережі розподіляють доходи між сайтами та партнерами лише після підтвердження того, що останні працюють у межах відповідних умов та положень.

52. 2018 року мережа Фейсбук інвестувала в рекламу в усьому світі, підкресливши, що «з фейковими обліковими записами їй не по дорозі». Але у згаданому вище звіті Комітету Палати громад зазначено про повторення серйозних збоїв у роботі компанії, які призвели до маніпулювання даними та відповідно до поширення дезінформації й помилкової інформації[54]. Перед комітетами з правових питань та культури Сенату Франції один із керівників Google France наполягав на тому, що Гугл упроваджує чимало ініціатив для протидії дезінформації в інтернеті, як-от видалення реклами, яку використовують для поширення фейкових новин, упровадження принципу «слідкуй за грошима» для боротьби з дезінформацією, коригування посилань в алгоритмах, що пов'язані з певними подіями[55].

Як Фейсбук, так і Твіттер пообіцяли створити архіви політичної реклами, які будуть доступними для громадськості[56]. На проміжних виборах у США восени 2018 року Фейсбук, Гугл і Твіттер заявили, що перевірять, чи базувалися самі кампанії у США, та оприлюднять бази даних політичної реклами, за публікацію якої їм заплатили[57]. На своїй платформі мережа Фейсбук видалила 32 облікові записи та сторінки, які стосувалися проміжних виборів 2018 року до Конгресу США[58]. Компанія також створила мережі фальшивих облікових записів та подій. Ці мережі використовувалися для виявлення та нейтралізації «поганих гравців». Було також заблоковано 652 сторінки, які було створено в Ірані й які поширювали проіранські повідомлення[59].

53. Варто посилити фактчекінг наративів, використовуючи інструменти інтернет-фактчекінгу (скажімо, Snopes.com). Наприклад, директор Pagella Politica[60], італійської незалежної організації з перевірки фактів, наголошує на особливостях своєї роботи: «Після того як ми знаходимо новинну статтю, яка вочевидь є фальшивою, ми пишемо фактчекінговий матеріал, розміщуємо його в спеціальному розділі нашого сайту і надаємо посилання на нього мережі Фейсбук»[61]. Тут також необхідно звернути увагу на Кодекс принципів Міжнародної мережі з перевірки фактів (IFCN). Німецький дослідницький центр штучного інтелекту (Deutsche Forschungszentrum für künstliche Intelligenz GmbH-DFKI), наприклад, розробив застосунок для виявлення фейкових зображень, які використовують для поширення фальшивої інформації, проте які початково були опубліковані в інших контекстах[62].

Водночас ми повинні пам'ятати, що в інтернеті щодня циркулюють сотні мільйонів інформаційних повідомлень. Фактчекери можуть упоратися лише з невеликою частиною такої інформації. Потужності опрацювання інформації фактчекерами явно не відповідають очевидній потребі, навіть якщо фактчекери не просто працюють на такого оператора, як Фейсбук, а пропонують перевірку фактів на онлайн-платформах. Очевидно, що існує значний дисбаланс між тими, хто контролює алгоритми та дані, та самими суб'єктами даних. Існує також дисбаланс між людськими ресурсами, які продукують та поширюють дезінформацію, і кількістю людей, які її виявляють. Наприклад, у вересні 2015 року в рамках Європейської служби зовнішніх справ було створено оперативну робочу групу зі стратегічних комунікацій (East StratCom Task Force)[63]. Вона покладається на волонтерів, які спеціалізуються на зборі дезінформаційних повідомлень, але людських ресурсів суттєво не вистачає. У звіті Атлантичної ради, підготованому в березні 2018 року, рекомендовано, щоб ЄС вимагав від усіх держав-членів відряджати національного експерта для посилення роботи цієї оперативної групи[64].

---

[54] Пункт 133: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf.

[55] Звіт № 677 (2017–2018) Катрін Морен-Дасаї, наведено вище.

[56] Честер Дж., наведено вище.

[57] Цифрова агітація: підвищення прозорості для виборців, наведено вище.

[58] Фейсбук розкриває нові підроблені акаунти // «Facebook» deckt neue gefälschte Konten auf, *Neue Zürcher Zeitung*, 2 серпня 2018 року.

[59] Фейкові новини: американські технічні оркестри дають свою відповідь // Fake News: la tech américaine orchestre sa réplique, *Les Échos,* 23 серпня 2018 року.

[60] https://pagellapolitica.it.

[61] www.theatlantic.com/international/archive/2018/02/europe-fake-news/551972/.

[62] Бюлетень DFKI 40, 2017.

[63] https://euvsdisinfo.eu/news.

[64] www.atlanticcouncil.org/publications/reports/democrat-defense-against-disinformation.

54. З огляду на це можемо дійти висновку, що саморегулювання не є повноцінним рішенням.

1.4.2. Нормативно-правове регулювання

55. Нормативно-правове регулювання не в змозі, з юридичної точки зору, ставити під сумнів свободу надання послуг та свободу вираження поглядів.

1.4.2.1. Свобода надання послуг

56. Із точки зору норм ЄС обмеження можуть застосовуватися в загальних інтересах, для забезпечення свободи надання послуг у контексті захисту споживачів[65].

1.4.2.2. Свобода вираження поглядів

57. Деякі країни ухвалили законопроєкти, які дають змогу урядам відкривати кримінальні провадження щодо осіб, яких підозрюють у поширенні «фальшивої» інформації в інтернеті. Так було в Малайзії у квітні 2018 року і в Білорусі в червні того самого року[66]. Але основи концепції свободи вираження поглядів роблять можливість застосування цензури в Європі нереальною. Такі пропозиції одразу ж пов'язували б із посиланням на «Міністерство інформації» або «Міністерство правди»[67]. Цей аргумент, зокрема, висунули під час парламентської дискусії проти законопроєкту членів Народної партії (Partido Popular) у Нижній палаті Іспанії 17 липня 2018 року. Палата відхилила законопроєкт, спрямований на вдосконалення моніторингових можливостей спецслужб із метою протидії дезінформації.

58. У Європі право людини на свободу вираження поглядів закріплене в статті 10 Європейської конвенції з прав людини[68] та в статті 11 Хартії основних прав Європейського Союзу[69]. У справі «Хендісайд проти Сполученого Королівства» (Handyside v. the United Kingdom) від 7 грудня 1976 року Європейський суд з прав людини зауважив, що поняття щодо свободи вираження поглядів застосовують до «інформації» чи «ідей» не лише тоді, коли їх сприймають сприятливо або вважають нешкідливими, а й коли такі «інформація» чи «ідеї» ображають, шокують чи шкодять державі або будь-якій групі населення. Така особливість лежить у межах цінності плюралізму, толерантності та широкого розуміння, без яких не існує демократичного суспільства. Це означає, окрім іншого, і те, що кожна «формальність», «умова», «обмеження» або «покарання», накладені у цій сфері, мають бути пропорційними законній поставленій меті. В іншому рішенні[70] суд у Страсбурзі визначив, що у виборчих кампаніях поширення новини має відбуватися навіть тоді, коли ця новина може бути визнана фальшивою. Стаття 10 Конвенції не забороняє обговорення або поширення отриманої інформації, навіть якщо є значні підозри щодо неправдивості такої інформації. В іншому разі це позбавить людей права висловлювати свої погляди та думки щодо заяв, які звучать у засобах масової інформації, і відповідно необґрунтовано обмежить право на свободу вираження поглядів, викладене в статті 10 Конвенції.

59. Суд дбає про те, щоб не підтримувати жодних заходів, які можуть призвести до зловживань, наприклад, щодо постанов/рішень про блокування сайтів; блокування доступу до хостів та сайтів третіх

---

[65] *Комісія проти Франції // Commission v. France*, 22 жовтня 1998 року, C-184/96.

[66] Удар Лукашенка по журналістиці // Lukaschenkos Schlag gegen den Journalismus, Neue Zürcher Zeitung, 10 серпня 2018 року.

[67] Ройтер М. Думка комітету щодо питань цифрового порядку денного // Reuter M. Stellungsnahme Auschuss Digitale Agenda, Deutscher Bundestag, Netzpolitik.org.

[68] «Кожен має право на свободу вираження поглядів. Це право передбачає свободу дотримуватися своїх поглядів, одержувати і передавати інформацію та ідеї без втручання органів державної влади і незалежно від кордонів. Ця стаття не перешкоджає державам вимагати ліцензування діяльності радіомовних, телевізійних або кінематографічних підприємств.

Здійснення цих свобод, оскільки воно пов'язане з обов'язками і відповідальністю, може підлягати таким формальностям, умовам, обмеженням або санкціям, що встановлені законом і є необхідними в демократичному суспільстві в інтересах національної безпеки, територіальної цілісності або громадської безпеки, для запобігання заворушенням чи злочинам, для охорони здоров'я чи моралі, для захисту репутації чи прав інших осіб, для запобігання розголошенню конфіденційної інформації або для підтримання авторитету і безсторонності суду».

[69] «Кожен має право на свободу вираження поглядів. Це право передбачає свободу на вираження думок, отримання й передання інформації та ідей без втручання державних органів і незалежно від кордонів».

[70] *Салов проти України // Salov v. Ukraine,* 6 вересня 2005 року, 655118/01.

сторін на додаток до сайтів, щодо яких ведуться судові процеси, робить чимало інформації недоступною, тим самим обмежуючи права користувачів інтернету. Таке втручання не було передбачуваним і, як зазначено щодо однієї зі справ, не забезпечило заявникові достатній рівень захисту, на який він мав право в демократичному суспільстві з огляду на верховенство права[71]. Блокування доступу користувача до Ютуба без законних підстав порушує право на отримання та передавання інформації[72].

60. Держави-члени Ради Європи мають позитивне зобов'язання забезпечувати ефективність свободи вираження поглядів: вони мають створити сприятливе середовище для участі в громадських обговореннях усіх зацікавлених осіб, надаючи їм змогу висловлювати власні думки та ідеї без остраху. Держава повинна не просто утримуватися від будь-якого втручання у свободу вираження поглядів особи — вона має «позитивне зобов'язання» захищати його/її право на свободу вираження поглядів від нападів, зокрема й із боку приватних осіб[73].

61. Наявність фактів можна продемонструвати, тоді як правдивість оцінних суджень не залежить від доказів. Вимогу довести правдивість оцінного судження виконати неможливо, до того ж вона порушує саму свободу поглядів, яка є основоположною частиною права, що захищається статтею 10[74].

62. Окрім практики суду, варто звернути увагу на стандарти, прийняті Радою Європи: Рекомендація CM/Rec(2016)5 Комітету Міністрів державам-членам щодо свободи інтернету (13 квітня 2016 року), яка закликає держави-члени сформувати сприятливе середовище для свободи інтернету, *зокрема*, включно із упровадженням програм медійної та цифрової грамотності. Необхідно нагадати, що поняття «мова ворожнечі» було визначено Комітетом Міністрів 1997 року. Рада Європи ухвалила Конвенцію про кіберзлочинність у Будапешті 23 листопада 2001 року, і можна припустити, що кібератаку може бути визначено як форму дезінформації. Донедавна кіберзагрози вважали такими, що мають фізичні чи економічні наслідки, але зараз дезінформацію можна вважати такою загрозою, яка потенційно здатна завдати шкоди демократичному процесу.

63. Для всебічного огляду міжнародних стандартів у цій галузі спеціальні доповідачі Організації Об'єднаних Націй, Організації з безпеки та співробітництва в Європі, Організації американських держав (ОАД) та Африканської комісії з прав людини і народів (АКПЛН)[75] підготували Спільну декларацію 2017 року про свободу вираження думки, «фейкові новини», дезінформацію та пропаганду, вказавши на стурбованість міжнародних організацій щодо дезінформації в інтернеті. У декларації підкреслено позитивне зобов'язання держав сформувати сприятливе середовище для свободи вираження думки та визначено широкі стандарти публічної політики для досягнення цієї мети[76].

64. Отже, існує велика потреба та значний попит на регуляторні постанови, які виходитимуть за межі простого режиму саморегулювання. Але для формування пропозицій щодо нормативно-правової бази, яка стосуватиметься дезінформації, спочатку необхідно скласти перелік чинних правил щодо цих питань у державах-членах, а також у інших країнах.

1.4.2.3. Приклади нормативно-правових рамок

Франція

65. Правила, що регулюють захист персональних даних, обмежують те, наскільки програмне забезпечення, спрямоване (таргетоване) на окремих осіб, може розвиватися на практиці, адже згода — це необхідна умова такого збору даних. Французька правова система розрізняє регулярні та епізодич-

---

[71] *Ахмет Їлдірим проти Туреччини // Ahmet Yildirim v. Turkey,* 18 грудня 2012 року, 3111/10.

[72] *Ченгіз та інші проти Туреччини // Cengiz and Others v. Turkey,* 1 грудня 2015 року, 48226/10 та 14027/11.

[73] *Дінк проти Туреччини // Dink v. Turkey,* 14 вересня 2010 року, 2668/07, 6102/08, 30079/08, 7072/09 та 7124/09.

[74] *Єрусалим проти Австрії // Jerusalem v. Austria,* 27 травня 2001 року, 26958/95.

[75] Їх призначають ООН, ОБСЄ, ОАД та АКПЛН для сприяння міжнародному співробітництву й розроблення стандартів щодо свободи вираження поглядів, свободи медіа та ЗМІ.

[76] Пункт 3 Спільної декларації: «a. Держави пов'язані позитивним зобов'язанням сприяти формуванню умов, необхідних для вільних, незалежних і плюралістичних засобів комунікації, включно з плюралізмом ЗМІ, і які слугують ключем для розв'язання проблеми дезінформації та пропаганди. b. Державам варто створити чітку нормативно-правову базу, що регулює діяльність мовників, із наданням наглядовому органу захисту від політичного або комерційного втручання або тиску та можливості розвитку вільного, незалежного й плюралістичного мовного сектора».

ні політичні контакти, ініційовані політичними партіями й кандидатами. У разі регулярних контактів люди повинні бути поінформованими про опрацювання даних (їх характер, мету опрацювання та умови, за яких можна висловити відмову від такого опрацювання). Для епізодичного контакту потрібна згода особи на опрацювання даних[77]. Ці правила схожі на стандарти ЄС.

66. Фейкові новини вже врегульовані статтею закону від 29 липня 1881 року, яку спершу застосовували до преси. Вона стосується новин, які можна вважати такими, що можуть потенційно завдати шкоди громадському порядку[78]. Потрібні три умови: новини, які публікують, дублюють чи поширюють, є фальшивими; їхня публікація може завдавати шкоди громадському порядку; автор діяв недобросовісно, зі злим наміром. Факти мають бути точними та деталізованими. Судовий процес може бути ініційовано прокурором. Якщо громадський порядок не зазнав шкоди, немає правових підстав для вчинення будь-яких правових дій. На практиці дуже мало прикладів справ, які передають до суду. Поширення фальшивих новин карається штрафом у розмірі 45 000 євро. Застосування цих правил було поширено 2004 року на онлайн-інформацію.

67. Стаття 411–10 Кримінального кодексу стосується основних інтересів нації.

> Надання цивільним чи військовим органам влади Франції фальшивої інформації, яка може ввести їх в оману та завдати шкоди основним інтересам нації, аби задовольнити інтереси іноземного підприємства чи організації або підприємства чи організації, які перебувають під іноземним контролем, карається позбавлення волі терміном на сім років та штрафом у розмірі 100 000 євро.

68. Поширення фальшивих новин із метою впливу на голоси або спонукання виборців до утримання від голосування карається одним роком позбавлення волі та штрафом у розмірі 15 000 євро (стаття L.97 Виборчого кодексу).

69. Поширення фальшивих новин може вплинути на законність голосування та призвести до визнання виборів недійсними. Це сталося одного разу, коли було оприлюднено інформацію, що один із кандидатів зняв свою кандидатуру на користь іншого кандидата. Державна рада у ролі судді з виборчих питань вирішила, що це може вплинути на справедливість результатів виборів, що призвело до скасування виборів[79].

70. 2018 року після виявлення підозрілих фейкових новин щодо Емманюеля Макрона під час президентської виборчої кампанії 2017 року членами парламенту було представлено законопроєкт, спрямований на запобігання фейковим новинам під час виборчих кампаній, якщо дію вчиняють із території держави-члена ЄС. Законопроєкт критикували і преса, й адвокати. Після першого читання в Національній асамблеї Сенат відхилив його, постановивши, що законопроєкт не в змозі вирішити питання, пов'язане з дезінформацією, що він суперечить свободі вираження поглядів під час виборчих кампаній, а також побоюючись, що цим процесом можуть зловживати у політичних цілях. Однак законопроєкт знову стоїть на порядку денному Національної асамблеї, яка має сказати своє остаточне слово.

71. Законопроєкт спрямований на виявлення та припинення навмисних звинувачень, пов'язаних із фальшивою чи оманливою інформацією, опублікованою на онлайн-платформі протягом трьох місяців перед виборами.

72. На платформи поширюється зобов'язання щодо прозорості. Вони повинні надавати чітку, правдиву та прозору інформацію щодо себе або будь-якої третьої сторони, яка спонсорує контент. Вони також повинні оприлюднювати суму, яку вони отримали за спонсорування контенту.

73. Прокурор, будь-яка особа, яка має юридичний інтерес для судового розгляду справи за нагальної потреби, партії чи кандидати можуть подати скаргу на інформацію, яка вірогідно є фальшивою або неправдоподібною і яку навмисно, штучно та широко поширюють онлайн. Це поняття штучного та широкого поширення ключове для фальшивої інформації. Суддя зобов'язаний розглядати такі спра-

---

[77] www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux.

[78] Овре П. Фальшиві новини // Auvret P. Fausses nouvelles, Jurisclasseur Communication, Fascicule 3210.

[79] Державна рада, Франція, 14 квітня 1999 року, 196924. Jurisdata 1999-050242.

ви упродовж 48 годин, а також має право заблокувати публікацію та змусити платформу припинити її просування.

74. На технічних посередників, які є особами, що пропонують доступ до послуг зв'язку, покладатиметься зобов'язання щодо посиленого співробітництва. Отже, вони повинні будуть оперативно видаляти будь-який незаконний контент, про який їм було повідомлено, та мають запровадити легкодоступний і видимий механізм для того, щоб люди могли повідомляти їм про будь-які фейкові новини.

75. Вища рада з аудіовізуальних засобів Франції (CSA), французький регуляторний орган із питань телерадіомовлення, має право відмовити у підписанні конвенції з іноземною країною, якщо діяльність такої країни може серйозно зашкодити життю нації шляхом поширення фейкових новин або порушення принципу плюралізму ЗМІ.

Німеччина

76. Право на свободу вираження думок закріплене у пункті 1 статті 5 Основного закону, що охоплює свободу вираження поглядів та свободу поширення інформації[80]. Судове переслідування, розпочате турецьким головою держави Реджепом Тайїпом Ердоганом проти німецького журналіста, який здійснював на нього напади, було відхилено. Прокурор вважав, що таке діяння не можна розглядати як правопорушення[81].

77. Згідно з німецьким кримінальним законодавством варто розрізняти заяви щодо конкретних осіб та загальні заяви. Поширення загальних фальшивих новин без будь-яких посилань на конкретних осіб або груп осіб не підлягає кримінальному покаранню. За образи та наклеп можна отримати покарання в тому разі, якщо було принижено або дискредитовано конкретних осіб. У рішенні від 22 червня 2018 року Конституційний суд відхилив скаргу щодо обвинувального вироку за розпалювання ворожнечі та насильства щодо певних груп населення шляхом запереченням злочинів, скоєних за час правління нацистської влади, зокрема, заперечення вбивств, скоєних у концентраційному таборі «Аушвіц-Біркенау». Поширення фактичних заяв, які явно не відповідають дійсності та є свідомо неправдивими, не сприяє процесу формування думки. Отже, це не підпадає під свободу вираження поглядів[82]. За образи накладають штраф або ж карають позбавленням волі на два роки. Ті самі санкції застосовують до навмисних образ щодо окремих осіб. Заяви на видалення новин чітко не регламентують, але судова влада їх реєструє.

78. Будь-яка особа, яка пропонує платформу для новин, коментарів, блогів та інтернет-форумів — відповідно до законодавства ЄС (параграф 44) — вважається «хост-провайдером» на підставі пункту 10 закону про телемедіа (*Telemediengesetz*), і вона не уповноважена активно контролювати зміст повідомлень на відповідність вимогам закону та кримінального законодавства. Якщо «хост-провайдер» знає про такі повідомлення чи контент, він зобов'язаний негайно їх видалити.

79. Із 1 жовтня 2017 року набрав чинності закон про посилення законної відповідальності соцмереж (*Netzwerkdurchsetzungsgesetz*[83] — NetzDG). Цей нормативний акт, який прозвали «Законом про Фейсбук», безпосередньо спрямований на соціальні шерингові платформи, які дозволяють міжособистісну комунікацію, і має на меті боротьбу з мовою ворожнечі та поширенням злочинного контенту (наприклад, антиконституційного контенту, контенту, пов'язаного з тероризмом, дитячою порнографією, а також контенту, що принижує гідність)[84]. Провайдери соціальних мереж, які отримують понад 100 скарг на рік щодо незаконного контенту, зобов'язані готувати щопівроку звіти німецькою мовою про розгляд скарг на незаконний контент на своїх платформах і публікувати ці звіти у Федеральному віснику

---

[80] BVerfGE 54, 208 57, Генріх Бьоль, 3 червня 1980 року.

[81] Брауер Й. Розслідування проти Яна Бьомерманна за образу органів та представників зарубіжних країн тощо. Примітка щодо правової оцінки // Brauer J. Ermittlungsverfahren gegen Jan Böhmermann wegen Beleidigung von Organen und Vertretern ausländischen Staaten usw. Vermerk zur rechtlichen Bewertung, Generalstaatsanwalt, Кобленц, 13 жовтня 2016 року.

[82] Федеральний конституційний суд зміцнює свободу слова // 1 BvR 673/18, Bundesverfassungsgericht stärkt Meinungsfreiheit, Frankfurter Allgemeine Zeitung, 4 серпня 2018 року.

[83] www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2.

[84] www.technologylawdispatch.com/2017/10/social-mobile-analytics-cloud-smac/germanys-new-hate-speech-act-in-force-what-social-network-providers-need-to-do-now.

(*Federal Gazette*) та на власному сайті не пізніше одного місяця після закінчення звітного півріччя. Звіти, опубліковані на власному сайті, мають бути легко впізнаваними, доступними та постійно наявними.

80. Звіт повинен:

- містити загальні спостереження, що окреслюють зусилля, яких докладає провайдер соціальної мережі для усунення діяльності, що підлягає кримінальному покаранню, на платформі;
- подавати опис механізмів подання скарг на незаконний контент та критерії, які застосовують під час вирішення питання про видалення чи блокування незаконного контенту;
- вказувати кількість вхідних скарг на незаконний контент у звітному періоді з розбивкою щодо адресатів — контролюючих органів чи користувачів, а також щодо причин скарг;
- визначати організацію, кадрові ресурси, рівень спеціальної та лінгвістичної експертизи в підрозділах, відповідальних за опрацювання скарг, а також навчання та підтримку осіб, які відповідають за опрацювання скарг;
- зазначати про членство в галузевих асоціаціях із указуванням того, чи мають ці галузеві асоціації відповідну службу з питань роботи зі скаргами;
- вказувати кількість скарг, щодо яких було проведено консультацію із зовнішнім органом під час процесу прийняття рішення;
- вказувати кількість скарг у звітному періоді, які призвели до видалення чи блокування сумнівного контенту з розбивкою щодо адресатів — контролюючих органів чи користувачів.

81. На підставі закону NetzDG платформи, розміщені поза межами Німеччини, «мають негайно призначити особу, уповноважену за послуги у Федеративній Республіці Німеччині, і вказати це на своїй платформі так, щоб цю інформацію було легко побачити та вона була легко доступною». Контент підлягає видаленню або блокуванню упродовж 24 годин, якщо він явно незаконний. Інший незаконний контент підлягає видаленню або блокуванню «негайно», тобто протягом семи днів із моменту, коли щодо контенту було проведено «оцінювання». Водночас це не поширюється на скарги, подані іншими способами, аніж ті, що існують у рамках процедури роботи зі скаргами. Цілком імовірно, що процедури геоблокування було б недостатньо.

82. За порушення правових норм може накладатися штраф у розмірі до 5 мільйонів євро для фізичних осіб і до 50 мільйонів — для провайдера платформи. За порушення правових норм можна отримати покарання, навіть якщо це порушення було скоєно не в межах Федеративної Республіки Німеччини.

83. Деякі юристи вважають цей закон несумісним із принципом свободи вираження поглядів. Навіть *Wissenschaftlicher Dienst* (Дослідницька служба Німецької асамблеї (Бундестагу) з підтримки політичної діяльності членів у парламенті та на виборчих округах, яка надає спеціалізовану інформацію, пропонує аналітичні міркування та висновки експертів) висловила стурбованість щодо відповідності цього акта Основному закону у таких моментах: дуже короткі періоди, упродовж яких має бути оцінено сумісність повідомлень зі свободою вираження поглядів; законність мети нормативного акта (боротьба проти отруєння настроїв в країні, *Vergiftung der Stimmung im Land*); неоднозначні положення нормативного акта про вимогу або її відсутність щодо деталізації фактів; пропорційність штрафів щодо свободи вираження поглядів; відповідність цього нормативного акта закону в плані конфіденційності. Для роз'яснення цих моментів потрібно звернутися до судової практики Конституційного суду Німеччини, Суду Європейського Союзу та Європейського суду з прав людини.

Велика Британія

84. Британська виборча комісія закликала підвищити рівень прозорості для виборців у контексті практики цифрових виборчих кампаній. Вона надала рекомендації щодо відповідальності цифрових кампаній, витрат на них, прозорості платежів за проведення цифрових кампаній та контролю за виконанням цих правил[85].

---

[85] *Цифрова агітація: підвищення прозорості для виборців,* наведено вище.

Сполучені Штати Америки

85. Закон про чесну рекламу, представлений у жовтні 2017 року перед Конгресом США, впроваджує правила розкриття інформації та відмови від відповідальності (застереження) щодо політичної реклами в інтернеті. Технологічним компаніям потрібно зберігати копії передвиборчих рекламних оголошень та забезпечувати їхню доступність для громадськості. Реклама також повинна містити застереження, схожі до тих, які передбачено телевізійною або друкованою політичною рекламою, де виборцям надають інформацію про те, хто заплатив за рекламу, скільки та на кого цю рекламу було спрямовано (таргетовано). Також має бути надана інформація про дату та час публікації першого рекламного повідомлення[86]. Твіттер пообіцяв підтримати двопартійний законопроєкт, який внесли сенатори-демократи Емі Клобучар (штат Міннесота), Марк Ворнер (штат Вірджинія) та колишній сенатор-республіканець Джон Маккейн (штат Аризона).

86. Зрозуміло, що чимало країн усвідомлюють небезпеку маніпулювання громадською думкою під час виборчих кампаній і докладають комплексних зусиль щодо впровадження нових норм для протидії дезінформації. Однак лишається чимало перешкод для розроблення ефективних правил, які відповідали б конституційним та міжнародним стандартам, що робить це завдання ще складнішим[87].

87. Подальші рекомендації можуть стати корисними для дискусій щодо можливих міжнародних стандартів усередині Ради Європи. Ці стандарти — поєднання саморегулювання та офіційного регулювання, адже питання торкається посилення конфіденційності, прозорості, стримування, чутливості моніторингу/контролю, етики, освіти та належних практик, що використовуються платформами.

---

[86] www.warner.senate.gov/public/index.cfm/the-honest-ads-act.

[87] Саме тому Державна рада Франції надала свою правову оцінку щодо законопроєкту, який стосується фейкових новин.

2. Рекомендації

88. Для того щоб бути готовою до вищевказаних юридичних та технічних викликів, Рада Європи може розглянути такі питання.

2.1. Визначення термінів

89. Замість терміна «фейкові новини» варто використовувати «дезінформація» або «фальшива інформація».

90. HLEG вважає, що термін «фейкові новини» «неадекватний для того, щоб охопити комплексність проблеми дезінформації, до якої залучено контент, що насправді є не повністю «фейковим», а сфабрикованою інформацією, змішаною з фактами та реальними подіями, що виходять за рамки всього того, що нагадує поняття «новини»[88]. Ця сама робоча група вважає, що термін «фейкові новини» не лише неадекватний, а й оманливий, оскільки його привласнюють деякі політики та їхні прихильники й використовують для того, щоб спростовувати висвітлення, яке вважають неприйнятним та неприємним. Тому термін став зброєю, із якою потужні суб'єкти можуть втручатися в обіг інформації, атакувати та дискредитувати незалежні новинні ЗМІ.

91. У французькому законі поняття «фальшива інформація» ширше за поняття «фейкові новини», адже воно не передбачає будь-яке попереднє поширення інформації, яка, можливо, посилалася на точні та детальні факти. Утім, аби уникнути втягнення органів державної влади у правовий розгляд щодо захисту свободи інформації, варто встановити, що у поширенні такої фальшивої інформації є лихий намір.

92. У цьому контексті потрібно пам'ятати про практику Європейського суду з прав людини:

> Існування фактів можна продемонструвати, тоді як правдивість оцінних суджень не можна довести; вимогу довести правдивість оцінного судження неможливо виконати, і ця вимога порушує сам принцип свободи вираження поглядів, що є основоположною частиною права, яке захищається статтею 10 [Європейської конвенції про права людини][89].

2.2. Прозорість

93. Питання прозорості має бути сфокусоване на операторах та фінансуванні їхньої діяльності.

94. Вимоги щодо прозорості вже застосовують у сфері комунікацій. У статті 6 директиви 2000/31/ЄС Європейського Парламенту та Ради від 8 червня 2000 року про деякі правові аспекти інформаційних послуг, зокрема електронної комерції, на внутрішньому ринку (Директива про електронну комерцію) зазначено, що держави-члени мають забезпечувати відповідність комерційних повідомлень, які є частиною або самі становлять інформаційні послуги, принаймні таким умовам:

a. комерційне повідомлення має бути чітко ідентифіковане як таке;

b. фізична чи юридична особа, від імені якої надсилається комерційне повідомлення, має чітко ідентифікуватися.

95. Можна також згадати Регламент Європейського Парламенту і Ради (910/2014) від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку. Він пропонує передбачуване регуляторне середовище для транскордонного онлайн-використання, розпізнавання та посилення електронної ідентифікації, автентифікації та довірчих послуг, на які можна покладатися, для того, щоб сприяти розвитку і добровільному використанню систем безпечної ідентифікації постачальників інформації на основі найвищих стандартів безпеки та конфіденційності, включно з можливим використанням перевірених псевдонімів.

---

[86] Багатовимірний підхід до дезінформації, наведено вище, с. 10.

[87] *Моріс проти Франції // Morice v. France,* 23 квітня 2015 року, 293969/10.

96. У статті 5 директиви 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Європейського Союзу визначено способи ідентифікації операторів основних послуг.

97. Рекомендація Європейської комісії від 1 березня 2018 року щодо заходів для ефективної боротьби з незаконним контентом в інтернеті[90] підвищує прозорість та точність механізмів сповіщень і дій:

> (16) Постачальників хостингових послуг потрібно заохочувати до публікації чітких, зрозумілих та достатньо детальних обґрунтувань своєї політики щодо вилучення чи блокування доступу до контенту, який вони зберігають, зокрема контенту, який вважається незаконним.
>
> (17) Постачальників хостингових послуг потрібно заохочувати регулярно публікувати, бажано щонайменше щороку, звіти про свою діяльність, пов'язану з видаленням та блокуванням контенту, який вважається незаконним. Ці звіти мають містити, зокрема, інформацію про обсяг та тип видаленого контенту, кількість отриманих сповіщень щодо незаконного контенту та зустрічних сповіщень від тих, хто опублікував відповідний контент, а також час, необхідний для вжиття заходів.

Отже, існує загальна тенденція до підвищення прозорості для постачальників послуг у ЄС.

98. Американці та французи працюють над законодавством, а Британська виборча комісія наголошує на необхідності визначення того, хто стоїть за цими онлайн-платформами. Для того щоб задовольнити цю потребу, Британська виборча комісія пропонує, щоб цифровий матеріал, який використовують для виборчих кампаній, містив вихідні дані. Ця вимога буде корисною для забезпечення дотримання політичними партіями, кандидатами та третіми особами граничних норм витрат, адже джерела політичної реклами різноманітні та складні для ідентифікації. Щоб посилити прозорість, Британська виборча комісія рекомендує «зобов'язати учасників кампаній надавати рахунки від постачальників із докладними відомостями щодо деталей кампаній».

99. Чи удосконалиться нормативно-правове регулювання завдяки маркуванню на соціомедійних платформах? «Репортери без кордонів», одна з провідних неурядових організацій у сфері захисту та просування свободи інформації, хоче створити репозитарій за європейськими стандартами ISO щодо прозорості 3MI, етики та незалежності. Якщо така система робить джерела зрозумілими, це може виявитися контрпродуктивним. «Білі списки» статей чи джерел новин, засновані на рейтингах користувачів або незалежних установ, часто стають «довіреними» для погоджених урядом новин. Це може створити враження, ніби надійними є лише соціальні медіа з відповідним маркуванням. У своєму повідомленні про дезінформацію від 26 квітня 2018 року[91] інституції ЄС рекомендували запровадження показників достовірності для джерел контенту, які б засновувалися на об'єктивних критеріях та затверджувалися б асоціаціями новинних медіа. Але хто був би уповноваженим надавати таке маркування, і що відбулося б, якщо платформа з маркуванням поширила б фальшиві новини?

100. У законі про чесну рекламу в США наголошено, що прозорість фінансування політичної реклами — ключовий чинник для забезпечення виконання інших законів про фінансування агітаційних кампаній, включно із забороною фінансування кампаній іноземними громадянами. Закон передбачає поширення поточних вимог щодо доступу громадськості до даних про продажі політичної реклами, що наразі застосовуються до телерадіомовлення і кабельних та супутникових провайдерів, також і на цифрові платформи. Такий підхід підвищує прозорість і відповідальність за платну політичну рекламу, оскільки потребує, щоб цифрові платформи з 50 мільйонами або більше унікальних щомісячних відвідувачів упродовж більшості місяців за попередні 12 місяців вели облік усіх запитів рекламодавців, чиї сукупні запити на спеціальну політичну рекламу на платформі протягом попередніх 12 місяців перевищили 500 доларів США.

101. Із цією самою метою Британська виборча комісія пропонує учасникам кампаній повідомляти, скільки вони витратили на створення та надсилання таргетованих повідомлень виборцям за допомогою цифрових каналів.

---

[90] https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online.

[91] Європейська комісія, Брюссель. 26.04.2018 COM (2018) 236 final.

2.3. Тривалість виборчих кампаній

102. Обмеження щодо реклами, лімітоване періодом виборчих кампаній, не порушило б свободи надання послуг та свободи вираження поглядів відповідно до стандартів Європейського Союзу, особливо з огляду на те, що йдеться про загальний громадянський інтерес.

103. Щоб охопити діяльність із проведення цифрових кампаній, виборчий період має бути точно визначений законом і не повинен бути занадто коротким. Є країни, де цей період дуже короткий (Азербайджан, Греція, Литва, Північна Македонія). У такому контексті партії та кандидати не зобов'язані фіксувати доходи та витрати до цього періоду, навіть якщо вони пов'язані з виборчою кампанією. Отже, доречність коротких періодів передвиборчої кампанії необхідно переглянути та подовжити їх, щоб уникнути ризиків, пов'язаних із нечесною конкуренцією та проведенням масштабних цифрових кампаній до початку офіційної виборчої кампанії.

104. Наприклад, за півроку до загальнодержавних виборів (до Національної асамблеї) у Франції заборонено будь-яку рекламу про досягнення або про управлінські успіхи у виборчому окрузі, де мають відбутися вибори (стаття L.52–1 Виборчого кодексу). Таке правило, з меншими часовими обмеженнями, можна застосовувати для регулювання або заборони будь-якого поширення дезінформації у великих та штучних масштабах.

2.4. Витрати на цифрові виборчі кампанії

105. Витрати на цифрові кампанії варто розглядати як частину виборчих витрат, за відсутності інших нормативних положень щодо цього питання, і вони мають бути внесені до допустимого обсягу витрат партії, кандидата та, якщо це необхідно, до витрат третіх сторін.

106. Чи варто забороняти фінансування цифрових кампаній з інших країн? Чи буде це суперечити праву на свободу вираження поглядів?

107. У різних державах-членах Ради Європи є депутати, які представляють виборців за кордоном — громадян держав-членів, які проживають за кордоном, але беруть участь у виборах в країні, громадянами якої вони є, а також у європейських виборах. Європейські громадяни можуть голосувати на місцевих виборах у тій європейській країні, де вони проживають. Але проблема дезінформації може стосуватися їх так само, як і будь-якого виборця.

108. Чи є відмінність між забороною на закордонні виборчі витрати та забороною закордонних пожертв, що регламентовано в деяких державах-членах Ради Європи (наприклад, у Франції, Німеччині за певних умов, Латвії Молдові, Румунії, Туреччині та Україні)? Чому закордонні пожертви мають бути заборонені, а закордонні виборчі витрати — дозволені? Якими були б наслідки заборони на закордонні пожертви за одночасного дозволу на закордонні виборчі витрати? Закордонні виборчі витрати на цифрові послуги можуть бути розглянуті як пожертви в негрошовій формі з боку третіх сторін. Окрім того, обмеження щодо граничного обсягу виборчих витрат застосовують не скрізь. Отже, якщо це питання не буде врегульовано, це може бути шляхом допуску нерівних можливостей між політичними партіями та кандидатами, а також обходу допустимого обсягу виборчих витрат там, де такий обсяг встановлено.

109. Питання свободи вираження поглядів не було висунуто на розгляд, коли законодавчі органи у різних державах-членах вирішували заборонити пожертви від іноземних компаній. Оскільки іноземні компанії не беруть участі в голосуванні, заборона будь-яких витрат на кампанію, джерелом яких виступає іноземна компанія, може відповідати принципу свободи вираження поглядів.

110. Що стосується права неурядових організацій на трансляцію політичної реклами на радіо та телебаченні, то Європейський суд з прав людини мав збалансувати право НУО-заявника ділитися інформацією та ідеями загального інтересу, які громадськість має право отримувати, з бажанням органів влади захистити демократичну дискусію та процес від викривлення його потужними фінансовими групами, що мають кращий доступ до впливових ЗМІ. Суд визнав, що такі групи можуть отримати конкурентні переваги у сфері платної реклами і відповідно обмежити право на вільні та плюраліс-

тичні дебати, головним гарантом яких є держава[92]. Як результат, для підтримки вільної та плюралістичної дискусії має бути врахований ризик дисбалансу між політичними силами, що змагаються. Той самий ризик, який раніше суд мав оцінювати щодо традиційних засобів трансляції, зараз потрібно застосувати щодо соціальних медіа, які сьогодні набагато більш поширені, ніж раніше. Деякі кандидати та політичні партії можуть з вигодою використовувати потужні й анонімні онлайн-платформи, тоді як інші можуть взагалі не отримувати допомоги від соціальних платформ. Отже, нерегульоване втручання соціальних медіа у виборчі кампанії несе небезпеку створення несправедливих виборчих кампаній.

2.5. Обробка персональних даних відповідно до Європейського загального регламенту про захист даних (GDPR) та захист громадян

111. США та Європейський Союз мають різні підходи до конфіденційності. Перша поправка в США дозволяє використовувати політичні дані як захищену форму вираження.

112. У Європейському Союзі Загальний регламент про захист даних (GDPR) застосовується з 25 травня 2018 року, і до 6 травня 2018 року всі держави-члени мали ввести його до власного національного законодавства. У ньому зазначено, що захист фізичних осіб у контексті опрацювання персональних даних є основоположним правом. Пункт 1 статті 8 Хартії основних прав Європейського Союзу та пункт 1 статті 16 Договору про функціонування Європейського Союзу (TFEU) передбачають, що кожен має право на захист персональних даних.

113. Згідно з GDPR обробка персональних даних призначена для служіння людству. Право на захист персональних даних — не абсолютне право; воно повинне розглядатися в зв'язку з його функцією в суспільстві та бути збалансованим з іншими фундаментальними правами згідно з принципом пропорційності. У цьому Регламенті дотримано всі фундаментальні права та свободи і принципи, визнані у Хартії, як це передбачено в договорах Європейського Союзу, зокрема щодо поваги до приватного та сімейного життя, житла та спілкування, захисту персональних даних, свободи думки, совісті та віросповідання, свободи вияву поглядів та свободи інформації, свободи підприємництва, права на дієвий засіб правового захисту та справедливий суд, а також — культурного, релігійного та мовного різноманіття.

114. GDPR не застосовують до питань захисту фундаментальних прав і свобод або вільного потоку персональних даних, пов'язаних із діяльністю поза межами законодавства Європейського Союзу, наприклад, діяльністю щодо національної безпеки. Можна вважати, що виборчі питання підпадають під суверенітет кожної держави-члена і підпадають під принцип субсидіарності. Але політичні партії можуть збирати персональні дані про політичні переконання населення. Дозвіл на опрацювання таких даних можна надавати для цілей суспільного інтересу за умови впровадження відповідних заходів безпеки.

115. У березні 2018 року Європейська рада заявила, що: «соціальні мережі та цифрові платформи мають гарантувати прозору практику й повний захист конфіденційності та персональних даних громадян»[93]. Незважаючи на сферу застосування GDPR, деякі його положення можуть послужити Раді Європи для розроблення правової бази для протидії дезінформації, адже цілі GDPR і цілі можливої правової бази Ради Європи певною мірою однакові. Визначення, вимога щодо згоди суб'єкта даних та прозорість опрацювання можуть представляти певний інтерес для Ради Європи, аби гарантувати доброчесність виборчих кампаній та виборів.

116. Щодо виборів до Європарламенту 2019 року Європейський Союз шукає можливості накладати штрафи на європейські політичні партії, які зловживають використанням персональних даних виборців для впливу на результати виборів. Розмір санкцій може сягнути 5% від річного бюджету політичної партії, який фінансується із загального бюджету Європейського Союзу та з пожертв і внесків. Про

---

[92] Енімал Дефендерз Інтернешнл проти Сполученого Королівства // Animal Defenders International v. the United Kingdom, 22 квітня 2013 року, 48876/08. Ів-Марі Дубле. Заборона рекламних виборчих кампаній на телебаченні та радіо не суперечить статті 10 Європейської конвенції з прав людини // Yves-Marie Doublet. L'interdiction des campagnes politiques publicitaires à la télévision et à la radio n'est pas contraire à l'article 10 de la CEDH, Revue trimestrielle des droits de l'homme, 2014, 98, с. 483.

[93] www.consilium.europa.eu/en/press/press-releases/2018/03/23/european-council-conclusions-22-march-2018/.

цей проєкт сповістила газета *Financial Times* 26 серпня 2018 року. Його передбачено схвалити урядами країн ЄС та парламентом ЄС, а також існує необхідність внесення змін до регламенту 1141/2014 від 22 жовтня 2014 р. щодо статуту та фінансування європейських політичних партій і політичних фондів, який діє з 1 січня 2017 року[94]. Пункт 4 (a) статті 27 про санкції передбачає, що в разі неможливості визначення кількості порушень санкція становитиме 5% річного бюджету відповідної європейської політичної партії чи європейського політичного фонду. Сфера застосування цієї норми обмежується європейськими політичними партіями. Її метою є забезпечення достовірності змісту повідомлень.

2.5.1. Визначення

117. Визначення щодо персональних даних та їх обробки, надані у GDPR, можуть бути корисними під час розгляду питання дозволеного використання даних із метою визначення профілів виборців.

118. Визначення персональних даних у GDPR є ширшим, ніж було у попередньому законодавстві ЄС, і містить онлайн-ідентифікатори, такі як IP-адреса. «Персональні дані» — це будь-яка інформація, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати («суб'єкт даних»). Ідентифікована фізична особа — це така особа, яку прямо чи опосередковано можна ідентифікувати, зокрема, за такими ідентифікаторами, як ім'я, ідентифікаційний номер, дані про місцеперебування, онлайн-ідентифікатор, або ж її можна ідентифікувати за одним чи декількома чинниками, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи. «Опрацювання» означає (для цілей GDPR) здійснення будь-якої операції або низки операцій із персональними даними чи наборами персональних даних із використанням автоматизованих засобів або без них, серед операцій — такі як збирання, реєстрація, організація, структурування, зберігання, адаптація чи зміна, пошук, ознайомлення, використання, розкриття через передавання, поширення чи надання іншим способом, упорядкування чи комбінування, обмеження, стирання чи знищення. Особи мають право не бути об'єктом прийняття рішень, заснованих на автоматизованому опрацюванні без будь-якого втручання людини, якщо таке рішення може заподіяти їм шкоду.

119. Алгоритми повинні регулюватися цими правилами, лише якщо вони спираються на персональні дані; якщо ж це не так, то це — з юридичної точки зору біла пляма[95]. Тому таке чутливе питання потребує вирішення.

2.5.2. Прозорість обробки

120. Відповідно до вимог GDPR будь-яка обробка персональних даних має бути законною та справедливою. Фізичні особи повинні бути обізнані про те, що їхні персональні дані збирають, використовують, обговорюють або якось інакше обробляють, а також про те, якою мірою обробляють чи оброблятимуть. Принцип прозорості вимагає, щоб будь-яка інформація та повідомлення щодо обробки таких персональних даних були доступними і зрозумілими, з використанням чітких і простих формулювань.

2.5.3. Вимога щодо отримання згоди окремої людини

121. Для того щоб обробка була законною, персональні дані необхідно обробляти на підставі згоди відповідного суб'єкта даних або на іншій законній підставі, встановленій законом, або у GDPR, або в іншому нормативно-правовому акті Європейського Союзу чи держави-члена, як вказано у GDPR. Такий підхід передбачає необхідність дотримання встановленого законом зобов'язання, яке поширюється на контролера, або необхідність виконання договору, стороною якого є суб'єкт даних, або для вжиття заходів на запит суб'єкта даних до укладення договору. Не може бути ніякого припущення щодо факту надання згоди. Повинна бути можливість відкликати згоду в будь-який момент так само легко, як її було надано.

---

[94] Кох Т. Новий закон європейських політичних партій // Koch T. Das neue Recht der europäischen politischen Parteien, PRUF, MIP 2018, 24. Jahrgang, c. 71.

[95] Віллані С. та ін. Надати значення штучному інтелекту, для національної та європейської стратегії // Villani C. et al. Donner un sens à l'intelligence artificielle, Pour une stratégie nationale et européenne, La Documentation française, Париж, 2018, c.148.

122. Якщо таке регулювання захисту даних не є єдиною відповіддю на проблему, воно є ключовим елементом у розширенні прав і можливостей осіб та у посиленні відповідальності цифрових операторів.

2.6. Основні принципи алгоритмів та штучного інтелекту

123. Статтею 1 GDPR передбачено, що захист фізичних осіб у зв'язку з обробкою персональних даних є основоположним правом. Із цієї причини Французьке управління з питань захисту даних (CNIL) вважає, що штучний інтелект має відштовхуватися від двох основних принципів: справедливості[96] та постійної уваги й пильності. Справедливість стосується платформ і полягає в «добросовісному забезпеченні пошукової оптимізації (SEO) або сервісу ранжування без намагання змінювати їх чи маніпулювати ними в переслідуванні цілей не в інтересах користувачів». Справедливість встановлює зобов'язання щодо контролерів.

Оскільки розроблення алгоритмів спричиняє зменшення індивідуальної пильності, щодо алгоритмів у законодавчій базі, яка стосується дезінформації, варто закріпити принцип постійної уваги та пильності[97].

2.7. Спрощене судочинство за нагальної потреби

124. Судові дії у прискорених судових провадженнях у разі невідкладних справ, які запропоновано в актуальній версії французького законопроєкту, можуть бути чинником стримування. Водночас вони порушують три такі питання.

- Європейський суд з прав людини вважає, що під час виборчих кампаній можливе вживання більш різких слів та використання більш різкого мовлення, ніж зазвичай. Під час виборчих кампаній допускають словесні надмірності[98]. Як наслідок — може постати питання щодо можливості застосування такого втручання.
- З одного боку, у Франції, як і в Німеччині, суддя не має багато часу на винесення рішення щодо того, чи загрожує дезінформація громадському порядку і чи може вона дестабілізувати виборчу кампанію (48 годин і 24 години після отримання скарги). З другого боку, з огляду на швидкість поширення фейкових новин оперативно ухвалене судове рішення надасть можливість кандидатові, щодо якого здійснюються атаки та поширюються фейкові новини, відповісти.
- Якщо Рада Європи обере такий варіант, важливо звернути увагу на пропорційність санкції. Постачальник інтернет-послуг може отримати припис заблокувати своїм клієнтам доступ до сайту, який порушує авторські права. Однак такий припис та забезпечення його виконання мають гарантувати справедливий баланс між відповідними фундаментальними правами. Заходи, які будуть вжиті постачальником інтернет-послуг, мають бути чітко таргетованими в тому сенсі, що вони мають бути спрямовані на усунення порушення авторських або суміжних прав третіми особами, проте не мають впливати на користувачів інтернету, які вдаються до послуг провайдера з метою законного доступу до інформації. Якщо цього не буде дотримано, втручання провайдера у сферу свободи інформації цих користувачів було б невиправданим з огляду на поставлену мету[99].

2.8. Співпраця з різними зацікавленими сторонами

125. Як підкреслює HLEG, варто докласти зусиль для поліпшення інформаційної грамотності та підвищення обізнаності ЗМІ й системи освіти про небезпеку різних цифрових механізмів дезінформації. HLEG закликає до дій для підтримки програм із медіа та грамотності для людей будь-якого віку.

---

[96] Державна рада Франції. Цифрові технології та фундаментальні права // Conseil d'État. Le Numérique et les droits fondamentaux, 2014, с. 273 та 278–281.

[97] www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf, с. 50.

[98] Європейський суд з прав людини, Бразільє проти Франції // Brasilier v. France, 11 квітня 2006 року, заява № 71343/01.

[99] CJEU, UPC Telekabel, 27 березня 2014 року, C-314/12.

126. Зацікавлені сторони — це платформи, фактчекери, журналісти, ЗМІ та дослідницькі організації. Фактчекінг у державах-членах виглядає сьогодні як безсистемна діяльність. Держави-члени повинні брати на себе ініціативи щодо створення платформ із фактчекінгу.

127. HLEG пропонує заохочувати користувачів до контролю над контентом, який їм запропоновано для перегляду, на основі його показників якості. HLEG просить розширити можливості журналістів за допомогою професійних інструментів автоматичної перевірки контенту, навчання, а також проєктів із медіаінновацій.

128. Захист свободи вираження поглядів, вільної преси та плюралізму й підтримка якісної журналістики є основою програми дій HLEG. Довіра до новин неоднакова в усіх країнах. Наприклад, у Фінляндії 62% людей зазначають, що довіряють новинним організаціям та журналістам, тоді як у Греції цей показник становить лише 23%. Лише сім із 21 країни-члена Ради Європи, які було опитано у рамках звіту Reuters за 2017 рік, мають показник довіри до новинних організацій, що перевищує 50%: Фінляндія, Португалія, Польща, Нідерланди, Іспанія, Німеччина та Данія[100]. У цій ситуації новинні організації та журналісти також страждають від втрати довіри до них. Важливо також звернути увагу на форму державної допомоги медіаорганізаціям.

129. Ці кроки необхідно доповнити чіткими імплементаційними рамками. Як можемо побачити, HLEG запропонувала Європейській комісії промотувати загальноєвропейський кодекс практики, у якому відображено ролі та обов'язки різних зацікавлених сторін. Прозорість, особливо фінансова, відповідальність, конфіденційність, належний доступ, забезпечення розмежування між політичною рекламою та іншим контентом, а також співпраця між платформами — ті основні моменти, на яких зосереджено увагу.

130. Ідеться про консенсусний підхід, за якого ключову роль відіграють онлайн-платформи. Але, як показує досвід США, цифрові ринки не можуть бути лише в руках операторів. Більш визначна роль має відводитися органам державної влади.

131. Уваги заслуговують ще чотири питання[101].

- Необхідно, щоб представники громадянського суспільства наглядали за операторами. У цьому контексті можна згадати діяльність організацій Upturn[102], Propublica[103] та Electronic Frontier Foundation[104] у США.
- Популяризація етики в навчанні інженерів, технічних фахівців та менеджерів онлайн-платформ.
- Практика колективних позовів не лише для припинення будь-яких порушень, а й для відшкодування будь-яких збитків, яких може зазнати фізична особа.
- Створення комітету з питань етики цифрових технологій, який зможе поширювати посібники з належних практик, розробляти кодекси поведінки та давати поради урядам.

2.9. Відповідність європейському праву

132. Запропонована нормативно-правова база передбачатиме звільнення постачальників послуг від відповідальності, що закріплено у статті 14 директиви 2000/31ЄС. Але до постачальників послуг ставлять також й інші вимоги: прозорість відповідно до зазначених вище інструментів, які застосовують до онлайн-платформ, та до вказівок, передбачених Рекомендацією Європейської комісії щодо заходів з ефективної протидії незаконному контенту в інтернеті, навіть якщо сфера застосування цієї рекомендації відрізняється від обговорюваного питання. Так само у запропонованій нормативно-правовій базі варто передбачити забезпечення права на захист персональних даних відповідно до вимог GDPR.

---

[100] https://reutersinstitute.politics.ox.ac.uk.

[101] Віллані С. та ін., наведено вище.

[102] upturn.org.

[103] www.propublica.org.

[104] www.eff.org.

Можна вважати, що напрям цього підходу випливає з попередніх ініціатив Європейського Союзу, не ставлячи під сумнів принцип звільнення від відповідальності, який закріплено у статті 14 директиви 2000/31/ЄС.

2.10. Забезпечення виконання

133. Якщо уряди чи неурядові зацікавлені сторони неохоче погоджуватимуться застосовувати такі правила щодо прозорості чи судового контролю, ці правила залишаться лише марнослів'ям. У швидкоплинному цифровому світі кожна сторона має вживати необхідних заходів для встановлення юрисдикції щодо будь-якого правопорушення, пов'язаного з поширенням фальшивої та оманливої інформації. Але як відповідальність за виявлення, розслідування та відкриття кримінальних проваджень щодо таких правопорушень можна покласти на державу, у якій воно було скоєно, якщо така держава лишає за собою право не виконувати свої зобов'язання на практиці?

2.11. Короткий зміст пропозицій

134. Запропоновано три типи положень.

- Норми цифрового законодавства — Відповідно до європейських та конституційних стандартів ці норми будуть зосереджені на постачальниках послуг. Згідно з принципом звільнення від відповідальності, а також з різноманітними положеннями Європейського Союзу про прозорість такі правові положення вимагатимуть від постачальників послуг прозорості щодо їхньої діяльності та захисту персональних даних. Буде створено прискорену судову процедуру для вирішення невідкладних питань.
- Норми виборчого законодавства — Більш тривалі виборчі кампанії, прозорість фінансових ресурсів провайдерів та заборона виборчих витрат на цифрову діяльність, що здійснюється іноземними юридичними чи фізичними особами, можуть бути основою для формування ефективної нормативно-правової бази.
- Належна практика — Інші заходи зосереджуватимуться на фактчекінгу, співпраці з усіма зацікавленими сторонами, етиці, розробці програм підвищення грамотності та саморегулювання постачальників послуг, тобто всього, що підтримує якісну журналістику.

3. Програма дій

135. Програма дій щодо дезінформації та виборчих кампаній може стати належною основою для вирішення завдань, пов'язаних із цим складним питанням.

Упевнені, що вільні та чесні вибори є пріоритетом Ради Європи у питаннях зміцнення демократичного врядування та участі громадян Європи;

Усвідомлюючи, що відновлення довіри до основних інститутів наших демократій є постійною боротьбою, і зусилля, які докладаються, мають бути систематичними для боротьби зі спробами знецінити правду, які підривають основи демократії;

Висловлюючи стурбованість через ризик того, що соціальні медіа можуть бути використані як глобальні системи та як бізнес-моделі, що підривають політичний процес виборчих кампаній, і впевнені в тому, що питання, які порушуються через алгоритми та штучний інтелект, значною мірою під час виборчих кампаній, суттєво впливають на політичний процес;

Беручи до уваги стрімку швидкість технологічного прогресу, а також той факт, що операції із цифрової дезінформації впливають на більшу кількість виборців порівняно з традиційними методами;

Визнаючи обмежену прозорість проведення цифрових кампаній через використання реклами, алгоритмів, ботів й обмежені можливості контролю та відсутність публічної політики в цій галузі;

Беручи до уваги новий Європейський загальний регламент про захист даних, який має на меті забезпечити захист персональних даних та зобов'язати отримувати згоду користувачів на опрацювання їхніх персональних даних, а також який накладає на соціомедійні платформи більш жорсткі правила, ніж у минулому, та враховуючи, що через відсутність регулювання держави-члени Європейського Союзу і Ради Європи не мають ефективних правових засобів для того, щоб захистити себе від цифрових механізмів маніпулювання під час виборчих кампаній, що є парадоксальною ситуацією, адже європейський виборець виявляється менш захищеним, ніж європейський споживач;

Вважаючи, що для вирішення цих питань існують неурядові та урядові рішення, частина з яких засновуються на саморегулюванні, інші ж — на заохоченні та примусових заходах;

Вітаючи недавні заходи та подальшу діяльність Європейського Союзу, спрямовану на боротьбу з дезінформацією з огляду на майбутні вибори до Європейського Парламенту.

Держави-члени Ради Європи повинні у визначений термін затвердити загальну стратегію щодо соціальних медіа та виборчих кампаній, яка б поєднувала законодавчі заходи та саморегулювання. Держави-члени Ради Європи мають:

- погодити спрямування своїх зусиль щодо забезпечення вільної та неупередженої інформації під час виборчих кампаній та щодо регулювання практик дезінформації, а також не використовувати щодо таких практик вираз «фейкові новини», адже це поняття не є належним та адекватним для нормативно-правової бази;
- скласти перелік різних існуючих способів саморегулювання та законодавчого регулювання цифрових кампаній, які зараз використовують держави-члени;
- визначити тривалість виборчих кампаній для того, щоб уникнути ризику проведення масштабних цифрових кампаній перед самими виборчими кампаніями;
- вимагати зазначення вихідних даних цифрових матеріалів для розкриття інформації щодо того, хто стоїть за онлайн-платформами;
- вимагати розкриття інформації щодо витрат на цифрові виборчі кампанії від онлайн-платформ;
- заборонити фінансування цифрових виборчих кампаній іноземними фізичними або юридичними особами;
- дотримуватися вимог GDPR, зобов'язуючи отримувати згоду громадян на використання їхніх персональних даних для цифрових виборчих кампаній, за винятком випадків, коли ці громадя-

ни регулярно контактують із політичною партією або пов'язаним із нею кандидатом і якщо при цьому ці персональні дані не розголошуються без згоди відповідних громадян;

- покладати зобов'язання щодо забезпечення справедливості та постійної уваги й пильності щодо роботи онлайн-платформ й алгоритмів;
- посилити спроможність судів у разі широкого поширення фальшивої інформації блокувати роботу онлайн-платформ, що поширюють фальшиві новини у великих масштабах, у терміновому порядку за допомогою прискорених судових процедур;
- заохочувати ініціативи фактчекінгу через спеціальну мережу, що діятиме на просторах Ради Європи, з метою сприяння зростанню широкомасштабних фактчекінгових операцій;
- навчати та підтримувати користувачів у контексті покращення доступу та використання онлайн-інформації, а також інформувати користувачів у разі, коли контент створюється або поширюється за допомогою ботів чи алгоритмів;
- заохочувати навчання з питань етики для всіх, хто залучений до роботи з цифровими технологіями, які впливають на вибори;
- посилити застосування принципів етики онлайн-бізнес-платформ;
- популяризувати належну практику серед онлайн-платформ, підписуючи з ними угоди, що засновуватимуться на спільно визначених відповідними державними органами й онлайн-платформами нормативних рекомендаціях;
- продовжувати підтримувати високоякісні медіаорганізації та журналістику;
- створити комісії з питань етики у кожній державі-члені та уповноважити їх очолювати процес обговорення етичних, політичних і соціальних питань, які постають у зв'язку з розвитком технологій, особливо щодо виборчих цифрових кампаній;
- забезпечити ефективні, пропорційні та стримувальні санкції у відповідь на порушення відповідних норм щодо цифрових виборчих кампаній;
- створити групу взаємодії між державами-членами для підтримки та сприяння стратегічному співробітництву й обміну інформацією.

Висновки

136. Виборче право — частина суверенітету держав. Воно пов'язане з їхнім історичним минулим та відповідною організацією їхніх інституцій. Це сфера, де немає спільних норм, окрім загальних принципів вільних та чесних виборів, що на практиці покликані захищати вільне вираження поглядів виборців у виборі своїх представників. Але вплив інвазивних цифрових методів у рамках глобалізації створює новий контекст, який потребує міжнародних інструментів для захисту європейських демократій, що зіштовхуються зі спільними загрозами.

137. Рада Європи — найоптимальніший і найбільш легітимний орган у Європі для ініціювання обговорення в цій галузі та просування далі порівняно з Європейською комісією і Спільною декларацією ООН та ОБСЄ 2017 року.

138. Європейський правовий інструмент, який промотуватиме Рада Європи, може надати спільний напрям для всеохопної рамкової програми. Інструмент Ради Європи може забезпечити рівні «правила гри» для кожної держави-члена. Для цього доступна низка різних інструментів.

139. Ми запропонували попередню пропозицію для програми дій. Програму дій щодо протидії корупції було схвалено міжгалузевою групою 1995 року, і цей документ став основою для розробки численних правових інструментів Ради Європи з цих питань: кримінальних і цивільно-правових конвенцій, рекомендацій, резолюцій та звітів. Але незважаючи на те, що розробка програми дій — часовитратний процес, необхідно розглянути варіанти різних доступних заходів разом з аргументами «за» і «проти» кожного з цих можливих рішень.

140. У деяких випадках рекомендації або резолюції передували конвенціям Ради Європи. Так було, зокрема, щодо боротьби з корупцією у приватному секторі або ж щодо боротьби з кіберзлочинністю. Рекомендації встановлюють загальні стандарти та заохочують держави-члени до ініціювання відповідного законодавчого процесу. Це було б найдоцільнішим і найоперативнішим підходом до роботи над цим питанням. Але такий варіант має недолік, дозволяючи державам-членам можливість для різних тлумачень, тоді як для того, щоб бути ефективними, регулятивні норми в цій галузі мають бути однаковими та стандартизованими.

141. Настанови доцільні тоді, коли вже існують сформовані законодавчі рамки на міжнародному рівні або ж на рівні законодавства держав-членів. Настанови надають програмні рекомендації щодо впровадження та доповнення чинних регуляторних норм.

142. У конвенції є перевага, яка полягає в зобов'язальному характері документа. Можна визначити певну кількість ратифікацій для того, щоб ця конвенція набула чинності, не очікуючи її ратифікації кожною державою-членом. Ще два аргументи додають ваги цьому варіанту. Більшість конвенцій Ради Європи передбачають моніторинговий механізм для забезпечення їх дотримання, а також можливість для держав-нечленів приєднатися до цих конвенцій. Підготовка цієї конвенції розпочнеться фактично з нуля, оскільки лише деякі держави-члени ухвалили конкретні правила саме щодо цих питань, які можуть полегшити розробку конвенції, зважаючи на відсутність поточних механізмів. Однак переговори щодо конвенції потребують часу.

143. З огляду на досягнутий консенсус щодо пов'язаних із дезінформацією загроз для виборчого процесу Раді Європи необхідно визначитися щодо найоптимальнішої правової форми для реагування на цю проблему. Якою б не була обрана форма, вона сприятиме зміцненню демократії в Європі та підтримуватиме Раду Європи в її зобов'язанні забезпечувати вільні та чесні вибори, які стали основоположною частиною європейської ідентичності та її конституційних цінностей.

Від літа 2016 року під «фейковими новинами» розуміють навмисне, вірусне поширення неправдивої інформації в інтернеті й у соціальних медіа з наміром, зокрема, дискредитувати політичну партію, заплямувати чиюсь репутацію або поставити під сумнів наукову істину. Ця практика, яка заважає громадянам приймати обґрунтовані рішення, стала дуже поширеною. Її вплив украй серйозний не лише з огляду на те, як швидко поширюються фейкові новини, а й тому, що ідентифікувати авторів таких кампаній та цифрових матеріалів дуже складно.

Мета цього документа — дати відповіді на запитання, пов'язані із цим феноменом, зокрема на ті, які виникають під час виборчих кампаній, і висунути пропозиції щодо формування нормативно-правової бази на європейському рівні.

УКР

www.coe.int

Рада Європи є провідною організацією у сфері прав людини на континенті. Вона налічує 47 держав-членів, серед яких усі держави-члени Європейського Союзу. Кожна держава-член Ради Європи стала учасницею Європейської конвенції з прав людини — угоди, метою якої є захист прав людини, демократії та верховенства права. Дотримання Конвенції в державах-членах контролює Європейський суд з прав людини.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE