

3. Левченко О. В. Нормативно-правове регулювання інформаційної безпеки України: стан та шляхи вирішення проблем. *Збірник наукових праць Харківського університету Повітряних сил*. 2014. Випуск 3 (40) С. 130 –135.

4. Рішення РНБО «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» від 28 квітня 2014 року. URL: <https://zakon.rada.gov.ua/go/449/2014>

5. Валушко І. О. Інформаційна безпека України: трансформація законодавства після російського вторгнення. Історико-політичні студії. *Збірник наукових праць*. 2017. № 2 (8). С. 30 – 43.

Латковський Павло Павлович

к.ю.н, доцент кафедри конституційного, адміністративного та фінансового права Чернівецького навчально-наукового юридичного інституту Національного університету «Одеська юридична академія»

ІНФОРМАЦІЙНІ ПРАВА ЛЮДИНИ ПІД ЧАС ВІЙНИ

Цифрові технології підштовхнули наш світ вперед до безпрецедентного інформаційного прогресу. Цифрова ера також принесла з собою нові виклики у захисті прав людини та демократії, а також інформаційної безпеки країни в цілому. Спеціальні інформаційні операції Російської Федерації намагаються посилити внутрішні протиріччя в Україні та в інших демократичних державах. Технології гібридної війни проти України, у тому числі, моделі й механізми інформаційного втручання, швидко адаптуючись до локальних контекстів та регуляторних політик, наносять шкоду інформаційному простору України та Європейського Союзу.

Глобалізація, пандемія COVID-19, повномасштабна війна РФ проти України - все це зумовило посилення ролі соціальних мереж у національному та світовому інформаційному просторі, їх вплив на внутрішню і зовнішню суспільно-політичну ситуацію, стан додержання прав і свобод людини, зокрема щодо забезпечення принципів рівності прав користувачів соціальних

мереж, що фактично дало змогу ототожнити соціальні мережі до основних суб'єктів впливу в інформаційному просторі.

Сьогодні вже можна констатувати факт того, що Україні вдалося гідно відповісти атаці збройних сил агресора як у військовому, так і в інформаційному просторі. Основою стратегії інформаційної безпеки стало перш за все державне регулювання глобальної стратегії інформаційної безпеки – рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки», яка визначила актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію і захист персональних даних та реалізація якої розрахована на період до 2025 року [1].

Впевнено можна сказати, що інформаційне законодавство України в цілому відповідає європейським та світовим стандартам. Стаття 10 Конвенції про захист прав та основних свобод людини проголосила, що кожна людина має право на свободу вираження поглядів. Це право включає свободу дотримуватися своїх поглядів, одержувати і передавати інформацію та ідеї без втручання органів державної влади і незалежно від кордонів [2]. Проте в сучасних реаліях надзвичайно важливим є контроль з боку державних установ за поширенням інформації, яка має на меті загрозу національній та інформаційній безпеці України.

Свобода вираження думок і доступ до правильної та надійної інформації є основою кібернетичної гігієни. Хоча Інтернет значно полегшує способи самовираження та різноманітність доступної інформації, деякі зацікавлені сторони мають право забороняти, видаляти або спотворювати онлайн-контент відповідно до своїх інтересів. Виникає питання: як провести межу між інформацією, яку варто поширити, та інформацією, яку слід заборонити? І хто має на це право?

Сучасний виклик вимагає ретельного балансування, щоб забезпечити ефективне реагування кримінального правосуддя з відповідними гарантіями верховенства права та недоторканістю прав людини.

По-перше, захист наших суспільних прав має центральне значення для становлення демократії. Громадянське суспільство відіграє тут ключову роль - воно має брати активну участь у розробці політики регулювання інформаційних відносин та інших заходів, що стосуються цифрових технологій та онлайн-простору. Журналісти та представники громадянського суспільства повинні мати відкритий і безпечний доступ до інформаційного простору, вільного від стеження та цензури. Держави та міжнародні інформаційні компанії зобов'язані забезпечити такий доступ та переконатися, що ми, як звичайні користувачі, маємо право самостійно та оперативно приймати колективні рішення, особливо коли виникають інформаційні загрози. Звісно реалізація такої системи передбачає високий рівень інформаційної та кібернетичної розвиненості населення, відповідальність щодо розвитку якого має нести саме держава.

Сьогодні в Україні функціонує декілька проєктів, націлені на підвищенні рівня цифрової грамотності та кібергігієни населення, перелік яких наведено нижче:

Національна онлайн-платформа для розвитку цифрової грамотності, створена Міністерством цифрової трансформації України за підтримки проєкту агентства з міжнародного розвитку США (USAID) «Кібербезпека критично важливої інфраструктури України» [3].

Онлайн-курси, розроблені Міністерством цифрової трансформації України за підтримки швейцарсько-української Програми «Електронне урядування задля підзвітності влади та участі громади» (EGAP), що впроваджується Фондом Східна Європа та фінансується Швейцарією [4].

Платформа Zrozumilo [5] та Всеукраїнська онлайн-школа [6], які також активно займаються розвитком інформаційної обізнаності громадян та державних посадовців.

Також необхідно враховувати той факт, що значний внесок в розвиток цифрової освіти громадян вносять органи Кіберполіції, НБУ, Держспецзв'язку, CERT-UA й Комітету Верховної Ради України з цифрової трансформації.

По-друге, право на свободу вираження власних поглядів має зберігатися як онлайн, так і офлайн, і повинно йти рука об руку з боротьбою із дезінформацією в Інтернеті. Хоча соціальні медіа надають унікальні можливості для спілкування та мобілізації громадського суспільства, ми усвідомлюємо недостатню ефективність компаній у реагуванні на дезінформаційні кампанії на поширення вразливої інформації, непрозорість і тривожне домінування такої інформації на ринку, а також неспроможність держави запровадити правила регулювання цього простору.

Вкрай важливо, що будь-які заходи, вжиті державою для регулювання інформаційного мовлення, повинні відповідати трикомпонентному тесту, заснованому на принципах законності, суспільної необхідності та пропорційності.

Україна має досить розвинуту по сучасним міркам ІТ-спільноту та амбітну політичну програму щодо інформаційної грамотності, штучного інтелекту (ШІ) та цифровізації. Це стало основою для співпраці з міжнародними проектами щодо захисту прав людини та їх взаємодії з органами державної влади України. Серед прикладів варто зазначити такі проекти, які вже сьогодні суттєво впливають на групи громадянського суспільства. Серед них:

Центр демократії та верховенства права (CEDEM) – аналітичний центр, який має досвід у сфері свободи слова та верховенства права, штучного інтелекту та цифрових технологій, а також організації діяльності правозахисних груп [7]. Вебінари та заходи цього центру пов'язані із штучним інтелектом та правами людини, такими як свобода зібрань, смарт міста та соціальні мережі. Вони спрямовані на громадські організації, а також на регіональних журналістів та юристів, які працюють у сфері свободи

вираження поглядів, приватності, сучасних технологій і практики Європейського суду з прав людини.

Європейський центр некомерційного права (ECNL), місією якого є створення правових та політичних середовищ, які дозволяють окремим особам, громадським рухам та організаціям здійснювати та захищати свої громадянські права та свободи, а також втілювати в життя трансформаційні ідеї, що відповідають національним та глобальним викликам [8].

Лабораторія цифрової безпеки (DSLUI) - центр допомоги українським журналістам, правозахисникам та громадським активістам вирішувати проблеми у цифровій безпеці, а також сприяти реалізації прав людини в Інтернеті через вплив на державну політику у сфері цифрових прав.

Після початку війни в Україні ECNL надав підтримку CEDEM і Digital Security Lab Ukraine (DSLUI) щодо потенційного впливу розгортання програм на основі штучного інтелекту на цивільне населення під час конфлікту, зокрема використання інструментів розпізнавання обличчя на базі штучного інтелекту під час воєнного стану. У результаті онлайн-дискусії з ECNL, громадськими організаціями та українськими посадовцями представники уряду попросили скласти рекомендації на основі даних, зібраних ECNL і попросили їх провести оцінку впливу на права людини для деяких додатків на основі ШІ, розроблених у державному секторі.

Також можливість використання альтернативних, менш інтрузивних способів перевірки особи та прийняття державними органами стратегій зменшення ризиків, включаючи оцінку впливу на права людини, з точки зору використання сучасних технологій навіть після закінчення воєнного стану та надзвичайної ситуації в Україні (наприклад, щодо безпеки використання додатків у смартфоні та загальної безпеки баз даних, які обслуговуються автоматизованими системами).

Представники уряду України сьогодні активно звертаються до CEDEM та DSLUI з проханням підготувати рекомендації у сфері захисту прав людини в інформаційному та кібернетичному просторі, а також з питань проведення

оцінки впливу на права людини для деяких додатків на основі ШІ, які ці організації розробляють у державному секторі. Вони також попросили поради щодо належного механізму, рекомендованого для подальшого зберігання та видалення даних, коли вони стануть не потрібні.

Той факт, що український уряд відкритий та готовий отримувати поради від міжнародних організацій із захисту прав людини, а також залучати їх досвід до своєї політики інформаційного розвитку, продовжувати співпрацю з усіма міжнародними партнерами та сприяти створенню безпечного громадянського інформаційного простору без цензури та обмежень для кожного - все це є безумовно позитивним фактором, який ще більше наближає Україну до ЄС та її правового регулювання. Проте потрібно пам'ятати, що саме обмежувальні заходи (санкції) та ефективний механізм моніторингу і відповідальності за їх порушення є найефективнішим механізмом відповіді на дезінформаційну активність Російської Федерації як держави-агресора.

Джерела:

1. Про рішення Ради національної безпеки і оборони України. Указ Президента України від 15 жовтня 2021 року № 685/2021 «Про Стратегію інформаційної безпеки». URL: <https://zakon.rada.gov.ua/laws/show/685/2021>
2. Конвенція про захист прав людини і основоположних свобод (з протоколами) (Європейська конвенція з прав людини). № 995_004. URL: https://zakon.rada.gov.ua/laws/show/995_004
3. Національна онлайн-платформа з цифрової грамотності запрацювала в тестовому режимі. Міністерство та Комітет цифрової трансформації України, 21.01.2020. URL: <https://thedigital.gov.ua/news/natsionalna-onlayn-platforma-z-tsifrovoi-gramotnosti-zapratsyuvala-v-testovomu-rezhimi>
4. E-Governance for Accountability and Participation (EGAP). Official web site. URL: <https://egap.in.ua>
5. Платформа Zrozumilo! Партнерський проект Дія Цифрова Освіта - Національна онлайн-платформа для розвитку цифрової грамотності. URL: <https://osvita.diia.gov.ua/partner-projects/zrozumilo>

6. Всеукраїнська онлайн-школа. Партнерський проект Дія Цифрова Освіта - Національна онлайн-платформа для розвитку цифрової грамотності. URL: <https://osvita.diia.gov.ua/partner-projects/vseukrainska-onlajn-skola>
7. Centre for Democracy and Rule of Law. Official web site. URL: <https://cedem.org.ua>
8. The European Center for Not-for-Profit Law Stichting (ECNL). Official web site. URL: <https://ecnl.org>

Марценко Наталія Степанівна

*к.ю.н., доцент кафедри міжнародного права та міграційної політики
юридичного факультету*

Західноукраїнського національного університету

Злепко Юрій Іванович

*здобувач вищої освіти юридичного факультету
Західноукраїнського національного університету*

ПЕРСПЕКТИВИ РОЗШИРЕННЯ КОЛА СУБ'ЄКТІВ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ У ПРАВІ ЄВРОПЕЙСЬКОГО СОЮЗУ ТА УКРАЇНИ

Розвиток суспільства та технологій за останні десятиліття зазнав істотного прискорення та вплинув на різноманітні сфери життя суспільства та держави (зокрема, на створення музичних, літературних, художніх творів, фільмів, ігор, написання журналістських статей та книг, створення музики та зображення тощо). Збільшення кількості випадків, коли окремі об'єкти створюються чи генеруються Штучним Інтелектом (далі - ШІ), спонукають до дискусій та наукових пошуків вирішення питання про те, який режим правової охорони має бути поширено на такі об'єкти. Разом з тим, діяльність спрямована на створення об'єктів інтелектуальної власності, притягує до себе дедалі більше уваги та попиту, тому чітке юридичне визначення суб'єктів та об'єктів права інтелектуальної власності є вкрай необхідним.