В. В. МАСИЧ. РЕГУЛЮВАННЯ ВИКОРИСТАННЯ КОМУНІКАТИВНИХ МОЖЛИВОСТЕЙ ІНТЕРНЕТУ

Розглянуто міжнародні правові механізми протидії використанню можливостей Інтернету у деструктивних цілях, особливості їх застосування в Україні.

Ключові слова: *інформаційно-комунікаційні технології, кібертероризм, свобода слова, мова ненависті.*

Рассмотрены международные правовые механизмы противодействия использованию возможностей Интернета в деструктивных целях, особенности их использования в Украине.

Ключевые слова: *информационно-коммуникационные технологии, кибертерроризм, свобода слова, язык ненависти.*

The international legal mechanisms of counteraction the usage Internet resources with destructive purposes and the peculiarities their implementation in Ukraine are considered.

Key word: *information and communication technologies, cyber terrorism, freedom of speech, hate speech.*

Останнім часом Інтернет все частіше використовується як ефективний інструмент встановлення не лише горизонтальних (соціальних) зв'язків між користувачами, а й вертикальних – між виборцями та політиками, між громадянами та органами виконавчої влади. До безсумнівних переваг такого методу спілкування слід віднести оперативність (швидке розповсюдження інформації про діяльність або бездіяльність відповідних органів) та відносну доступність (для встановлення контакту слід мати комп'ютер, підключений до Інтернет, що не передбачає затрат на спілкування поштовими повідомленнями).

Однак досить часто можливості нових технологій використовуються для реалізації з деструктивних цілей: організації екстремістської діяльності, розпалювання ворожості, дестабілізації суспільства тощо. До переваг Інтернету, які приваблюють екстремістки налаштованих осіб, слід віднести:

– анонімність доступу до більшості ресурсів;

– можливість максимально оперативного доступу до інформації у будь-який час доби з будь-якої точки світу;

– наявність на сайтах широкого потоку проекстремістської інформації;

– широкий вибір аудіовізуальної продукції, яка сприймається краще, ніж друковані методи поширення інформації;

– можливість використання різноманітних звукових ефектів;

– популярність Інтернет серед молоді.

Що стосується тих, хто створює і підтримує подібні сайти, то вони користуються наступними перевагами Інтернету:

– анонімність створення та підтримка сайтів;

– приховування певної інформації шляхом обмеження доступу до неї через введення паролю, жорстких правил реєстрації на сайті;

– створення інформаційних мереж і перехресних посилань на різноманітні споріднені сайти, близькі за ідеологією;

– швидкість перенесення інформації з одного домену на інший. Навіть якщо сайт було виявлено і закрито компетентними органами, його контент можна легко

© *МАСИЧ Вадим Васильович* – аспірант Інституту держави і права ім. В.М. Корецького НАН України

перенести на інший сайт з іншою адресою;

– реєстрація сайту не в країні проживання основної аудиторії. Це ускладнює процес контролю владних органів над змістом і самим фактом існування небажаного сайту, а також утруднює притягнення авторів сайту до адміністративної або кримінальної відповідальності[1].

Основну роль серед європейських країн у боротьбі з екстремістськими сайтами відіграють перш за все Німеччина та Франція, які стали ініціаторами розробки Радою Європи Конвенції по боротьбі з кібертероризмом[2], яка була підписана у Будапешті 23 листопада 2001 року і вступила у силу 1 липня 2004 року. Конвенція є першою міжнародною угодою про злочини, що здійснюються через Інтернет та інші комп'ютерні мережі. Її головне завдання полягає в тому, щоб здійснювати у пріоритетному порядку спільну політику у сфері кримінального права, спрямовану на захист суспільства від комп'ютерних злочинів, в тому числі шляхом прийняття відповідних нормативно-правових актів та зміцнення міжнародного співробітництва. Цю конвенцію Україна ратифікувала 21 грудня 2006 року, а вступив він в силу з 1 квітня 2004 року, а серед країн Ради Європи Конвенцію не підписали і не ратифікували з Азербайджан, Грузія, Монако, Росія.

Конвенція визначає такі види комп'ютерних злочинів, щодо яких кожна держава повинна вжити заходів:

1) злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (протизаконний доступ (ст. 2), неправомірний перехват (ст. 3), вплив на дані (ст. 4), вплив на функціонування системи (ст. 5), протизаконне використання пристроїв (ст. 6),

2) правопорушення, пов'язані із використанням комп'ютерних засобів (підлог з використанням комп'ютерних технологій (ст. 7), шахрайство з використанням комп'ютерних технологій (ст. 8),

3) правопорушення, пов'язані зі змістом даних (дитяча порнографія (ст. 9))

4) правопорушення, пов'язані з порушенням авторського права і суміжних прав (ст. 10).

Згідно положень конвенції, між країнами-учасниками спрощуються процедури видачі, направлення запиту, закладаються основи для взаємної допомоги у зберіганні даних, що зберігаються у комп'ютері на території іншої країни, розкритті даних про потоки інформації, у доступі до електронних даних, у зборі в режимі реального часу змісту даних конкретних повідомлень.

Спершу проти підписання цієї конвенції виступали США, оскільки вважали, що вона суперечить Першій поправці до Конституції США, що декларує свободу слова. Однак згодом, у 2006 році її все таки ратифікували і вона набула чинності з 1 січня 2007 р.

У політичній та законодавчій практиці США розрізняють «екстремізм» та «тероризм». Якщо останній справді сприймається як загроза, то до екстремістської діяльності ставлення більш поблажливе. Слід зазначити, що позиція США щодо інтернетівського екстремізму стала жорсткішою після терактів 11 вересня 2001 р. Через місяць після цих подій Дж. Буш підписав закон, що давав спецслужбам право вторгатися у комп'ютерні мережі та окремі персональні комп'ютери, за наявності найменших підозр щодо причетності їх власників до терористичної діяльності.

Американське законодавство забороняє публікацію низки текстів у мережі Інтернет. До них відносяться тексти, які містять «загрози» і які мають «намір завдати іншому фізичні чи майнові збитки або травмувати іншим чином шляхом здійснення незаконного акту»[3]. Ці погрози, як правило, є різними варіаціями расистських лозунгів. Ними можуть бути електронний лист потенційній жертві

або ж висловлювання на Інтернет-форумі. Однак для того, щоб стати реальною основою для обвинувачення, висловлювання повинно бути «правдивим», тобто повинно сприйматися адресатом як реальна загроза застосування до нього насильства. Крім того, кожна погроза повинна мати свого індивідуального адресата.

Основою для обвинувачення також є агресивні висловлювання. Для виходу з-під захисту Першої поправки до Конституції США суб'єкт агресивних висловлювань повинен висловити їх проти конкретної особи. Якщо автор таких текстів лише говорить про свою ненависть до певної расової, етнічної, релігійної групи, то його неможливо притягнути до відповідальності, навіть якщо його слова травмують (морально чи фізично) окремих представників такої групи. Однак в окремих штатах кримінальне переслідування можливе, якщо агресивні висловлювання мали місце, наприклад, у Пенсільванії, де це заборонено законом.

До екстремістських висловлювань, що караються законом, відносяться і «заклики до неминучого насильства». Судова практика США розрізняє висловлювання, «спрямовані на те, щоб потягнути за собою неминуче насильство, і з високим ступенем ймовірності призводять до такого насильства»[4] та висловлювання, які не тягнуть за собою неминучих дій. До уваги береться також те, чи «заклики» здійснюються у процесі безпосереднього спілкування, тоді покарання може бути накладене, хоча і у такому випадку довести неминучість насильницьких дій досить складно. Якщо ж подібні заклики містяться у тексті поштової розсилки або в Інтернеті, то шанс на кримінальне переслідування за ці дії мінімальний.

Останнім видом екстремістських висловлювань вважаються наклепи. До них відносяться промови та тексти, що не відповідають дійсності, які спрямовані на збурення ненависті до расових, релігійних та етнічних груп. Шансів на кримінальне переслідування схожих висловлювань практично немає. Якщо вони спрямовані проти окремих осіб, то перспектива судового розгляду може стати реальністю, якщо ці особи є державними службовцями, які зможуть довести, що в основі висловлювань проти них лежав «справді злий намір»[5]. В інших випадках такі наклепи не можуть стати основою для звинувачення особи, що їх розповсюдила.

Згодом конвенція була доповнена Додатковим протоколом щодо кримінального покарання за висловлювання расистського та ксенофобського характеру, що поширюються через комп'ютерні системи[6]. Він був відкритий для підписання 28 січня 2003 року і вступив в силу 1 березня 2006 року. Його основна вимога полягає у встановленні країнами-учасницями кримінальної відповідальності за поширення расистських чи ксенофобських матеріалів через комп'ютерні мережі, а також за аналогічні висловлювання та погрози. Ст. 6 Протоколу передбачає встановлення покарання за заперечення, виправдання чи схвалення фактів геноциду чи злочинів проти людяності.

Продовженням міжнародних зусиль щодо боротьби з проявами ненависті стало рішення[7] Ради міністрів Організації з безпеки та співробітництва від 2009 року, яке закликало держави-члени:

1) збирати, зберігати і обнародувати достовірні відомості і досить детальні статистичні дані про злочини на ґрунті ненависті і насильницьких проявах нетерпимості, включаючи кількість випадків, доведених до відома правоохоронних органів, число порушених справ і вироків;

2) приймати у випадку необхідності конкретне і цілеспрямоване законодавство у боротьбі зі злочинами на ґрунті ненависті, що передбачає ефективні заходи

покарання, які б враховували важкість таких злочинів;

3) вживати відповідних заходів для заохочення жертв повідомляти про злочини на ґрунті ненависті, з визнанням того, що приховування відомостей про них перешкоджає державам розробці ефективної політики;

4) запроваджувати або удосконалювати заходи щодо професійної підготовки і створення потенціалу, орієнтовані на посадових осіб правоохоронних, прокурорських і судових структур, що займаються злочинами на ґрунті ненависті.

На практиці реалізувати принцип кримінальної відповідальності за коментарі в Інтернеті вдалося відносно недавно. Судові справи за нетерпимі висловлювання у мережі уже розглядалися у Австралії та США, однак лише недавно у Великій Британії користувач отримав 18 тижнів тюремного ув'язнення за жорстокі коментарі у соціальних мережах[8].

Додатковий протокол до Конвенції по боротьбі з кібертероризмом Україна ратифікувала 21 грудня 2006 року, який вступив в силу з 1 квітня 2007 р. Однак на сьогодні низка країн до нього не приєдналася, це такі члени Ради Європи як: Болгарія, Великобританія, Ісландія, Іспанія, Італія, Словаччина, Туреччина, Угорщина та Чехія.

Слід зазначити, що якщо положення конвенції знайшли своє відображення у Розділі 16 Особливої частини Кримінального кодексу України[9] (визначено відповідальність за несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361), несанкціоновані дії з інформацією, яка обробляється в комп'ютерах, автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362), порушення правил експлуатації комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється (ст. 363)), то положення Додаткового протоколу у вітчизняному законодавстві не прописані. Вітчизняній судовій практиці не відомі випадки покарання за розпалювання ворожнечі в Інтернеті.

Водночас, як свідчать соціологічні дослідження, проблема недотримання принципу толерантності в ході Інтернет-спілкування є досить актуальною для України. так, згідно з результатами дослідження, проведеного Київським міжнародним інститутом соціології в українському сегменті Інтернету нараховується близько 12 млн. користувачів, що агресивно і вороже висловлюються на адресу представників різних політичних сил, національностей[10]. Загалом близько 60% вітчизняних користувачів Інтернету регулярно відвідують суспільно-політичні сайти. З них 86% періодично читають коментарі до статей та новин, третина з яких вступає в Інтернет-дискусії. Що стосується змісту цих дискусій, то 71% містить образи, погрози та прояви агресії. При цьому 9 з 10 користувачів хоча б раз стикалися із подібними проявами. Найчастіше причиною нетерпимої поведінки в ході таких дискусій є конкретні політики (88,7%). Значно менше агресії викликають інші політичні погляди (14,5%), особисті якості людини (6,5%), регіон проживання та національність (по 3,2%) та соціально-економічний статус (1,6%).

Водночас у Росії, яка не приєдналася до конвенції та додаткового протоколу ст. 282 Кримінального кодексу РФ передбачає покарання за «дії, спрямовані на збудження ненависті або ворожості, а також на приниження достоїнства людини або групи особі за ознакою статі, раси, національності, мови, походження, ставлення до релігії, а також приналежності до будь-якої соціальної групи, здійснені публічно або з використанням засобів масової інформації». У вересні 2011 року Рада по Інтернету та новим ЗМІ при Міністерстві зв'язку підготувала проект

щодо створення інформаційної системи, за допомогою якої користувачі зможуть скаржитися на екстремістські коментарі у мережі.

Отже, проблема толерантного спілкування в Інтернет стає все більш актуальною для усіх країн і України зокрема. Ненависть в українському сегменті Інтернет має яскраво виражену політичну забарвленість і різко зростає у періоди політичних протистоянь. Відсутність законодавчих механізмів боротьби з цим явищем сприяє зростанню рівня ненависті серед Інтернет-користувачів та може стати причиною реальних конфліктів, що дестабілізують суспільство.

1. *Туркин С., Ульянова Е.* Зарубежный опыт противодействия экстремистским тенденциям в Интернете // Конституционное право: Восточноевропейское обозрение. – 2003. – № 3. – С. 2-7. **2.** *The Convention* on Cybercrime (ETS 185) [Електронний ресурс]. – Режим доступу: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG **3.** *United States* v. Watts, 394 U. S. 707 (1969); R. A. V. v. St. Paul, 505 U. S. 377 (1992**). 4.** *Brandenburg* v. Ohio. 395 U. S. 444 (1969). **5.** *New York* Times v. Sullivan, 376 U. S. 254 (1964). **6.** Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, CETS № 189 / [Електронний ресурс]. – Режим доступу: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CM=8&DF=&CL=ENG**7.** Combating hate crimes. Decision № 9/09. Organization for Security and Co-operation in Europe, Ministerial Council, 2 December 2009 / [Електронний ресурс]. – Режим доступу: http://www.osce.org/cio/40695. **8.** *Morris S.* Internet troll jailed after mocking deaths of teenagers / [Електронний ресурс]. – Режим доступу: http://www.guardian.co.uk/uk/2011/sep/13/internet-troll-jailed-mocking-teenagers. **9.** *Кримінальний* кодекс України, Закон України від 05.04.2001 № 2341-III // Голос України. – 2001. – 19 червня. – № 107. **10.** *Фельдман О.* Кибер-ненависть по-украински: кого, сколько и за что?... / [Електронний ресурс]. – Режим доступу: http://www.pravda.com.ua/columns/2011/06/21/6314335/.