Науково-дослідний інститут інформатики і права
Національної академії правових наук України

Апарат Ради національної безпеки і оборони України

Київський науково-дослідний інститут судових експертиз
Міністерства юстиції України

Навчально-науковий центр інформаційного права
та правових питань інформаційних технологій
ФСП Національного технічного університету
України «Київський політехнічний інститут»

«ТЕОРІЯ І ПРАКТИКА ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ ЗА ПРАВОПОРУШЕННЯ В ІНФОРМАЦІЙНІЙ СФЕРІ»

МАТЕРІАЛИ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
08 червня 2016 року

Київ – 2016

УДК 34:004]

ББК 67.404.3я43

Т33 Теорія і практика юридичної відповідальності за правопорушення в інформаційній сфері: Матеріали науково-практичної конференції / 08 червня 2016 р., м. Київ / Упорядн. : В.М. Фурашев, С.Ю. Петряєв. – К.: НДІІП НАПрН України, Апарат РНБО України, КНДІСЕ Мінюсту України, НТУУ «КПІ», 2016. – 200с.

ISBN978-966-622-779-2

Подано матеріали з актуальних питань проблем юридичної відповідальності за правопорушення в інформаційної сфері. Доповіді учасників конференції, що опубліковані у збірнику можуть бути корисними для законодавців, вчених, фахівців та експертів інформаційної сфери, науково-педагогічних працівників, аспірантів, докторантів, студентів вищих навчальних закладів, а також усіх, хто цікавиться сучасними суспільно-правовими проблемами розвитку інформаційного суспільства, а також проблемами захисту прав людини в інформаційному суспільстві.

Організаторами заходу виступили: Навчально-науковий центр інформаційного права та правових питань інформаційних технологій ФСП НТУУ «КПІ», Науково-дослідний інститут інформатики і права НАПрН України, Апарат Ради національної безпеки і оборони України, Київський науково-дослідний інститут судових експертиз Міністерства юстиції України. Участь у конференції взяли провідні експерти і вчені наукових установ і навчальних закладів України, представники зацікавлених державних органів та громадських організацій. Інформаційну підтримку у проведенні заходу надали: журнали «Інформація і право», «Правова інформатика», «Теорія і практика», «Інформація та безпека», Вісник НТУУ «КПІ» «Політологія. Соціологія. Право» та Міжвідомчий науково-методичний збірник «Криминалистика и судебная экспертиза» КНДІСЕ МЮ України.

Матеріали викладено в авторській редакції.

Упорядники: **Фурашев В.М., Петряєв С.Ю.**

Оформлення обкладинки:
Лабораторія технічної естетики та дизайну ФСП НТУУ «КПІ» (designlab.kpi.ua@gmail.com)
Балашов Д.В. (balashov.dim@gmail.com)

Рекомендовано до друку Вченою радою Науково-дослідного інституту інформатики і права Національної академії правових наук України Протокол № 6 від 09.06.2016 р.

Вченою радою факультету соціології і права Національного технічного Університету України «Київський політехнічний інститут» Протокол №11 від 29.06.2016 р.

ISBN978-966-622-779-2

УДК 343.32
321.011 342.3
342.727 303.6
32.019.51

О.Е. Радутний,
доктор філософії (PhD) з юридичних наук, доцент кафедри кримінального права № 1 Національного юридичного університету імені Ярослава Мудрого (м. Харків)
Ідентифікатор ORCID
orcid.org/0000-0002-6521-3977
ResearcherID: E-6683-2015

ЗАХИСТ СУВЕРЕНІТЕТУ В ІНФОРМАЦІЙНІЙ СФЕРІ В МЕРЕЖІ ІНТЕРНЕТ-ПРОСТОРУ

Відповідно до положень ст. 17 Конституції України захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу. Невід'ємною складовою частиною суверенітету України виступає її інформаційний суверенітет, під яким на підставі положень ст. 1 Закону України «Про Національну програму інформатизації» № 74/98-ВР від 04.02.1998 розуміють здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави

Згідно до положень ст.7 Закону України «Про основи національної безпеки України» № 964-IV від 19 червня 2003 року[1] загрозами національним інтересам і національній безпеці України в інформаційній сфері визнано прояви обмеження свободи слова та доступу до публічної інформації, поширення засобами масової інформації культу насильства, жорстокості, порнографії, комп'ютерну злочинність та комп'ютерний тероризм, розголошення інформації, яка становить державну таємницю, або іншої інформації з обмеженим доступом, спрямованої на задоволення потреб і забезпечення захисту національних інтересів суспільства і держави, намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Але не меншу загрозу в собі несуть також: посягання на державний суверенітет України та її територіальну цілісність, територіальні претензії з боку інших держав; спроби втручання у внутрішні справи України з боку інших держав; розвідувально-підривна діяльність іноземних спеціальних служб; загроза посягань з боку окремих груп та осіб на державний суверенітет, територіальну цілісність, економічний, науково-технічний і оборонний потенціал України, права і свободи громадян; зрощення бізнесу і політики, організованої злочинної діяльності; злочинна діяльність проти миру і безпеки людства, насамперед поширення міжнародного тероризму; спроби створення і функціонування незаконних воєнізованих збройних формувань та намагання використати в інтересах певних сил діяльність військових формувань і правоохоронних органів держави; прояви сепаратизму, намагання автономізації за етнічною ознакою окремих регіонів України; можливість втягування України в регіональні збройні конфлікти чи у протистояння з іншими державами тощо.

Зазначені загрози можуть втілитися у реальне життя, в тому числі, і шляхом зловживань чи здійснення правопорушень в інформаційній сфері.

Загрози нас оточують навкруги: поява транспортних засобів створила небезпеку для життя і здоров’я людини, прискорення їх швидкості лише

підсилило її, нові форми виробництва постійно створюють виклики безпечним умовам праці, здобутки в дослідженні ядерної енергії поставили людство на межу катастрофи (адже загрозами національним інтересам і національній безпеці України також визнаються загроза використання з терористичною метою ядерних та інших об'єктів на території України;

можливість незаконного ввезення в країну зброї, боєприпасів, вибухових речовин і засобів масового ураження, радіоактивних і наркотичних засобів;

поширення зброї масового ураження і засобів її доставки) тощо.

Вже стали буденними і тому підсвідомістю відштовхуються на задній план такі загрози, як значне антропогенне і техногенне перевантаження території України, зростання ризиків виникнення надзвичайних ситуацій техногенного та природного характеру; непідтримання в належному технічному стані ядерних об’єктів на території України; небезпека техногенного, у тому числі ядерного та біологічного, тероризму;

нераціональне, виснажливе використання мінерально-сировинних природних ресурсів як невідновлюваних, так і відновлюваних; погіршення екологічного стану водних басейнів, загострення проблеми транскордонних забруднень та зниження якості води; неконтрольоване ввезення в Україну екологічно небезпечних технологій, речовин, матеріалів і трансгенних рослин, збудників хвороб, небезпечних для людей, тварин, рослин і організмів, екологічно необґрунтоване використання генетично змінених рослин, організмів,

речовин та похідних продуктів; посилення впливу шкідливих генетичних ефектів у популяціях живих організмів, зокрема генетично змінених організмів, та біотехнологій; застарілість та недостатня ефективність комплексів з утилізації токсичних і екологічно небезпечних відходів тощо.

У зв’язку з цим не слід як перебільшувати значення негативного впливу прискореного розвитку засобів комунікації та інформаційних технологій, так і зменшувати його значення для окремої людини або всього людства у порівнянні з екологічними, ресурсними (корисні копалини, чиста вода тощо) та іншими загрозами.

На сьогодні Інтернет, як загальнодоступна мережа всесвітньої комунікації, розширив свої межи від поєднання між собою окремих стаціонарних пристроїв до розповсюдження на засоби, які постійно перебувають на зв'язку у будь-якій географічній точці (смартфони, планшети), завдяки чому суб'єкт інформаційних правовідносин постійно перебуває у хвилі інформаційного потоку та все більше залучається у взаємодію з віртуальним соціумом.

За ефективністю впливу Інтернет впевнено і переконливо обігнав телебачення та інші засоби масової комунікації[2].

Користувачі поступово відходять від спостерігання та пасивного споживання інформаційної продукції та перетворюються на активних її фігурантів та творців. Раніше окрема фізична особа мала можливість поширювати певну інформацію лише серед доволі обмеженого кола людей (близькі, родичі, знайомі, колеги тощо), держава або інше соціально-політичне утворення теж було певним чином обмежено своєю територією або традиційними засобами комунікації. Завдяки унікальним можливостям мережі Інтернет з'явилася можливість звертатися до безмежно невизначеного кола співрозмовників, здійснювати вплив на величезну кількість людей.

Принциповою особливістю мережі Інтернет у порівнянні з іншими традиційними засобами комунікації є подолання значних відстаней, включення звичайного користувача-спостерігача до процесу взаємодії (користувачі стають активними виробниками контенту, спостерігач стає частиною експерименту, в якому приймає безпосередню) за рахунок використання ефекту присутності, інтерактивності та вільної навігації, відносної доступності інформації, можливості включення в інтерсуб'єктну реальність[3] великої кількості людей (загальне для всіх багатовимірне інформаційне поле) тощо.

Посилення комунікаційної функції мережі Інтернет призводить до зміни формату масової політичної комунікації, що виникає між суб'єктами

політичних відносин у широкому сенсі слова з метою впливати на свідомість населення і спонукати до певного типу політичної поведінки[4].

Такий стан взаємодії є великим здобутком людства, але й вимагає усвідомлення можливих загроз та негативних побічних ефектів (за своїм соціальним змістом та впливом це схоже на легалізацію зброї для населення, коли старими формами взаємодії користуватися вже не можливо, оскільки треба звикати жити і діяти по-новому у змінених умовах).

Є всі підстави віднести до комунікаційних переваг мережі Інтернет високу швидкість обміну інформацією, свободу слова, відносну доступність певних даних, можливість поширення власної інформації, відносну анонімність, широке географічне проникнення, сприяння реалізації творчого потенціалу, можливість спілкуватися на значній відстані тощо.

Втім, раніше окремій людині значно простіше було забезпечувати приватність свого особистого життя. Сьогодні завдяки спокусі використання наданих можливостей, особа сама добровільно надає доступ для інформації, яка її ідентифікує. Але це може статися також і без участі та відома самої особи, коли її близькі або знайомі поширюють пов’язані з нею дані. Таку інформацію здатні використовувати злочинці, недруги, спеціальні служби держави або іноземних держав тощо.

Вільне спілкування за допомогою віртуальних майданчиків, блогів і мікроблогів, форумів і порталів, які підтримують функцію зворотного зв’язку, виводить комунікативні можливості на якісно новий рівень, але збільшує вразливість і створює сприятливі можливості для зловживань.

Таким зловживаннями можуть бути, перш за все, практично всі кримінальні правопорушення, відповідальність за які передбачена в Особливій частині КК України (за винятком окремих, як, наприклад, зґвалтування або пошкодження чи зруйнування релігійної споруди або культового будинку): доведення до самогубства (ст.120 КК), шахрайство з фінансовими ресурсами (ст.222 КК) та звичайне шахрайство (ст.190 КК), публічні заклики до насильницької зміни чи повалення конституційного ладу

або до захоплення державної влади (ч.2 ст.109 КК), шпигунство (ст. ст. 111, 114 КК), перешкоджання законній діяльності Збройних Сил України та інших військових формувань (ст.114-1 КК), погроза вбивством (ст. 129 КК), розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби (ст. 132 КК) тощо. За вказані дії чи бездіяльність чинним законодавством України вже передбачено кримінальну відповідальність.

Поширення таких форматів повідомлень, які тільки зовні виглядають простими за своєю формою, але насправді спрямовані на донесення основної думки через свідомість та підсвідомість, призвело до появи так званих мотиваторів та демотиваторів – візуальних картин, що поєднані з стислим коментарем або закликом та покликані створити певний настрій чи образ сприйняття. Їх популярність обумовлена зручністю, відносною простотою створення та швидким досягнення мети повідомлення.

Обізнана в сучасних комунікаційних засобах молодь стає зручним об'єктом впливу, як прямого (заклики, рекомендації, залучення до участі у флеш-мобах[5], що у подальшому закріплює стереотип бажаної поведінки), так і опосередкованого (створення моди на певну соціальну позицію, наслідування популярним фігурантам блогосфери, удаване ототожнення якостей адресата з якостями відомих людей, оцінка за асоціативним рядом, нав'язування думки про тотожність інтересів маніпулятора з інтересами аудиторії, удаване розкриття таємної інформації тощо).

В якості логічного наслідку з'ясування реальності кожної з наведених загроз постає спокуса негайного внесення змін у чинне законодавство, а саме – передбачити кримінальну відповідальність за посягання на інформаційний суверенітет України.

До розв'язання цього питання слід підійти вельми обережно з наступних причин. Так, зокрема, місія Європарламенту під керівництвом його екс-голови Пета Кокса у своєму звіті за 2016 рік зазначила, що Верховна Рада України в сфері законодавчої діяльності є «слабкою ланкою»,

перенавантажена великою кількістю законопроектів, які мають доволі низьку якість та являють собою «законодавче сміття» («законодавчий спам», «законодавче цунамі»)[6].

Розглянемо ті можливості ефективного забезпечення суверенітету в інформаційній сфері, які закріплені у чинному законодавстві України.

Перш за все, слід звернути увагу на те, що посягання на відносини з забезпечення суверенітету в інформаційній сфері завжди виявлятиметься не в загальній формі (якій відповідає формула «… посягання на інформаційний суверенітет України …»), але у конкретних проявах поведінки.

Це можуть бути, наприклад, заклики до дій, спрямованих на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади, надання інформаційної допомоги іноземній державі,
збирання з метою передачі або передача відомостей, що становлять державну, банківську, комерційну таємницю, відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової,
контррозвідувальної діяльності, у сфері оборони країни, розголошення державної таємниці тощо. Проте, відповідальність за такі дії вже передбачена ст. ст. 109, 111, 114, 231, 328, 330 КК України.

Крім того, не слід забувати, що Особлива частина КК України містить цілий розділ XVI «Злочини у сфері використання електронно-
обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку».

Формами та способами порушення суверенітету в інформаційній сфері, в тому числі, в мережі Інтернет, також можуть бути і перешкоджання здійсненню виборчого права або права брати участь у референдумі, роботі виборчої комісії або комісії з референдуму чи діяльності офіційного спостерігача (ст. 157 КК України), надання неправдивих відомостей до органу ведення Державного реєстру виборців або фальсифікація виборчих документів, документів референдуму, підсумків голосування або відомостей Державного реєстру виборців (ст. 158 КК України), порушення таємниці

голосування (ст. 159 КК України), порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ст. 163 КК України), перешкоджання законній діяльності професійних спілок, політичних партій, громадських організацій (ст. 170 КК України), посягання на здоров'я людей під приводом проповідування релігійних віровчень чи виконання релігійних обрядів (ст. 181 КК України), приховування або перекручення відомостей про екологічний стан або захворюваність населення (ст. 238 КК України), публічні заклики до вчинення терористичного акту (ст. 258^2 КК України), завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності (ст. 259 КК України), погроза вчинити викрадання або використати радіоактивні матеріали (ст. 266 КК України), заклики до вчинення дій, що загрожують громадському порядку (ст. 295 КК України), ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію (ст. 300 КК України), ввезення, виготовлення, збут і розповсюдження порнографічних предметів (ст. 301 КК України), схиляння до вживання наркотичних засобів, психотропних речовин або їх аналогів (ст. 315 КК України), спонукання неповнолітніх до застосування допінгу (ст. 323 КК України), схиляння неповнолітніх до вживання одурманюючих засобів (ст. 324 КК України), незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації (ст. 359 КК України), умисне пошкодження ліній зв'язку (ст. 360 КК України) тощо.

Таким чином, є всі підстави стверджувати, що чинний закон про кримінальну відповідальність на сьогодні без прогалин описує практично всі конкретні форми злочинної поведінки. Зазначене вказує на відсутність необхідності внесення змін в КК України. Втім, це не виключає можливості реагування на нові виклики (неохоплені форми злочинної поведінки), що вимагатиме відповідних змін у чинному законодавстві.

Ще одну проблему вбачають в тому, що через швидкоплинність та високу щільність інформаційних потоків, а так само – через інформаційну залежність, споживач інформації не завжди може перевірити її за ознаками належності та достовірності.

Відверто кажучи, так було, є і буде завжди. Споживача (в тому числі, користувача мережею Інтернет) не вбережеш заборонами чи встановленням помірковано-дозованого доступу до інформації. Логічним продовженням такої надмірної опіки над громадянином з боку держави було б встановлення заборони на вживання алкогольних напоїв та тютюнопаління, користування гострими предметами побуту, знайомство з новими технологіями, що можуть містити елементи ризику, тощо.

Кожна особистість несе обов'язок сама перед собою, близькими та оточуючими, нащадками та суспільством щодо постійного невтомного саморозвитку, формування властивості критично сприймати та аналізувати будь-яку інформацію тощо. Для цього вона має можливість залучати і користуватися тими критеріями, які вже були сформульовані попередніми поколіннями та окремими видатними представниками людства: відповідність раніше засвоєним знанням, досвіду та законам, в тому числі логіки та здорового глузду, узгодженість з ними; відсутність протиріч; можливість парадоксальності; конкретність (не буває істини взагалі, поза чіткими умовами); як вона, певна інформація, відкликається в серці людини, наодинці з собою в моносуб'єктній реальності.

Література:

1. Відомості Верховної Ради України (ВВР), 2003, № 39, ст.351
2. TNS Web Index [Електроннийресурс]. – Режимдоступу: http://www.tns-global.ru/ services/media/media-audience/internet/information
3. Щодо моносуб'єктної та інтерсуб'єктної реальності додатково див.: *Радутний О.Е.* Сакральність кримінально-правовогопростору / Питання боротьби зі злочинністю: зб. наук. пр. / редкол.: В.І. Борисов та ін. – Х.: Право, 2013. – Вип. 26. – 360 с. – с. 42 – 52.; *Радутний О.Е.* Додаткові методи у пізнанні кримінального права в інформаційну епоху /Правова інформатика: Науковий журнал з проблем інформатизації, Інформаційних технологій, інформаційного права,

Інформаційного законодавства та інформаційних ресурсів в інших галузях права / Редакційна рада: В.М. Брижко та ін. – К.: Науково-дослідний інститут інформатики і права Національної академії правових наук України, Інститут законодавства Верховної Ради України, 2015. – №
2(46)/2015. – с. 54 – 61

4. *Сковиков А. К.* Гаэтано Моска об акторах политического управления и власти / А. К. Сковиков // PolitBook. – 2012. – №4. – с. 104–114 – с. 108–109 [Електронний ресурс] – Режим доступу: https://cyberleninka.ru/article/n/gaetano-moska-ob-aktorah-politicheskogo-upravleniya -i-vlasti
5. Флешмо б (також *флеш моб* і *флеш-моб*, англ. *flash mob* – «спалахуючий натовп», *flash* – спалах, *mob* – натовп), або раптівка – неочікувана поява групи людей в заздалегідь запланованому місці; після закінчення запланованої акції, її учасники розчиняються в натовпі перехожих людей, що і викликає ефект раптовості; зазвичай раптівки організовуються через мережу Інтернет або інші сучасні засоби комунікації [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/флешмоб
6. Шпайхер Т. В Европе назвали украинских депутатов «творцами законодательного мусора» / Экономические известия, 13.03.2016 // [Електронний ресурс] – Режим доступу: http://news.eizvestia.com/news_politics/full/655-v-evrope-nazvali-ukrainskih-
deputatov-tvorcami-zakodatelnogo-musora

----------***----------