12. Oberschlick v. Austria (no. 1). Рішення від 23 травня 1991 р.; Prager and Oberschlick v. Austria. Рішення від 26 квітня 1995 р.
13. Observer and Guardian v. United Kingdom. Рішення від 26 листопада 1991 р.
14. Tammer v. Estonia. Рішення від 6 лютого 2001 р.; Constantinescu v. Romania. Рішення від 27 червня 2000 р.
15. Ukrainian Media Group v. Ukraine. Рішення від 29 березня 2005 р.
16. Zana v. Turkey. Рішення від 25 листопада 1997 р.
17. Sanoma Uitgevers B. V. v. Netherlands. Рішення від 14 вересня 2010 р.
18. Sunday Times v. United Kingdom. Рішення від 26 квітня 1979 р.
19. Делегація Спілки на чолі з секретарем НСЖУ О. Наливайком перебувала у Страсбурзі і Брюсселі. – 12.03.2012. – Інформаційне агентство УНІАН. – [Електронний ресурс]. – http://www.unian.ua/news/491095-prezident-evroparlamentu-ukrajinskim-jurnalistam-vlada-mae-poboyuvatis-zmi.html

Проблеми протидії правопорушенням в інформаційній сфері: реалії та перспективи

Наталія ОНІЩЕНКО,
завідувач відділу теорії держави і права Інституту держави і права ім. В. М. Корецького НАН України, доктор юридичних наук, професор, заслужений юрист України, член-кореспондент Національної академії правових наук України

Сергій СУНЄГІН,
молодший науковий співробітник відділу теорії держави і права Інституту держави і права ім. В. М. Корецького НАН України, кандидат юридичних наук

В умовах формування глобального інформаційного суспільства інформаційна безпека кожної держави, і зокрема України, починає відігравати чи не основну роль у забезпеченні національної безпеки в цілому. Зрозуміло, що Україна як європейська держава не може залишатися осторонь проблем і небезпек, породжуваних інформаційним суспільством. Інформація як одна з фундаментальних засад, на яких будується навколишній світ, у найрізноманітніших формах стає предметом та продуктом інтелектуальної праці великої кількості людей. У сучасній літературі підкреслюється, що сама людина для збереження статусу «людини розумної» має набувати статусу «людини інформаційної» [1, с. 9]. При цьому розвиток і освоєння інформаційно-комунікаційних технологій набули значення дієвих чинників особистого, суспільного та державного розвитку. Про це, зокрема, свідчить проведений 10 квітня 2012 року «круглий стіл» «Гуманітарно-правові аспекти становлення інформаційного суспільства в Україні», в якому взяли участь наші провідні вчені.

Суспільний обіг інформації регулюється, як правило, двома основними видами соціальних норм: правовими та моральними. Правовий обіг інформації охоплює лише найважливішу частину суспільного обігу інформації, відносини з організації та передавання якої врегульовані правовими нормами.

Дослідження інформаційного суспільства та пов'язаних із ним явищ соціальної дійсності можна здійснювати за допомогою різноманітних підходів, зокрема, соціокультурного, цивілізаційного, структурно-функціонального, порівняльного тощо. Однак у сучасних умовах, на нашу думку, першочерговим і найважливішим підходом до вивчення цього складного явища є саме нормативний підхід, який дає змогу формально визначити ті чи інші аспекти суспільних відносин, що складаються в сфері інформаційного обігу. А сама інформаційна діяльність потребує чіткої правової регламентації, передусім із позиції безпеки.

Крім цього, необхідно враховувати, що з історичним розвитком людства істотних змін зазнавали також способи та форми передачі інформації. Зокрема, відомо, що стародавні інки (приблизно 5000 років тому) передавали інформацію за допомогою так званих кіпу – зв'язок різнокольорових шнурків з вузликами. Згодом, з розвитком писемності, люди навчилися використовувати кам'яні або дерев'яні дощечки, базальтові стовпи тощо для написання відповідних текстів, зокрема, перших пам'яток права. Так, Закони Хаммурапі (XVIII ст. до н. е.) було викарбувано на стовпі з чорного базальту [2, с. 19].

Сьогодні одним з найпоширеніших способів передачі інформації є мережевий спосіб, що використовується під час передавання інформації в електронній формі.

Отже, істотно актуалізуються дослідження питань, пов'язаних із проблемами належного забезпечення протидії правопорушенням в інформаційній сфері, особливо здійснюваних з використанням всесвітньої електронної мережі Інтернет.

Тут треба зазначити, що певні напрями забезпечення інформаційної безпеки в сучасних умовах уже стали предметом дослідження окремих вітчизняних та зарубіжних вчених, серед яких, зокрема, П. Біленчук, Б. Кормич, Т. Костецька, Є. Кравець, Н. Лебедєва, В. Монахов, В. Наумов, Р. Шагієва та інші. Проте, не применшуючи значення наукового доробку цих учених, мусимо констатувати, що проблеми протидії правопорушенням у сучасній інформаційній сфері потребують нових підходів до їх визначення.

Тож **метою** цієї статті є визначення характеру та змісту найважливіших проблем протидії правопорушенням у сучасній інформаційній сфері, а також надання науково обґрунтованих рекомендацій щодо шляхів їх розв'язання в юридичній площині.

Сьогодні з упевненістю можна говорити, і це відзначають деякі вчені, про сформоване глобальне інформаційне суспільство, в якому обробкою інформації та її вищої форми – знань – зайнято більше людей, ніж обробкою сировини та матеріалів. При цьому вчені прогнозують, що в майбутньому весь світовий простір перетвориться на єдине комп'ютеризоване й інформаційне суспільство, всі помешкання будуть оснащені всілякими електронними засобами та комп'ютерними пристроями, діяльність людей зосереджуватиметься головним чином на обробці інформації, а матеріальне виробництво енергії покладатимуть на машини [3, с. 536].

Безперечно, нині ми вже можемо спостерігати певні позитивні риси або результати початкового етапу функціонування інформаційного суспільства, серед яких насамперед варто виокремити: сформованість інформаційної єдності всієї людської цивілізації, вільний доступ будь-якої людини до інформаційних ресурсів, які відображають надбання всієї цивілізації тощо.

Водночас усім добре відомо, що медаль має два боки і що за все в житті треба платити. Не є винятком і інформаційне суспільство, яке приховує в собі низку небезпечних тенденцій, зокрема: 1) реальна ймовірність руйнування приватного життя осіб та секретної діяльності організацій внаслідок впливу проникаючих інформаційних технологій; 2) наявність проблеми відбору достовірної інформації; 3) «труднощі» запобігання обігу «шкідливої» інформації, зокрема тієї, яка містить елементи насильства, публічні заклики до провадження терористичної діяльності, інші екстремістські матеріали, а також матеріали, що суперечать суспільній моралі; 4) збільшення загрози маніпулювання свідомістю людей внаслідок посилення одночасного впливу різноманітних форм засобів масової інформації, особливо її електронної форми; 5) необхідність забезпечення належної адаптації людей до специфічного середовища інформаційного суспільства, що рік у рік стає технічно складнішим тощо [4].

Отже, інформаційна сфера суспільства, сформована нині вже в глобальному масштабі, й надалі активно технологічно розвивається, стає одночасно чинником суспільного прогресу і реальною загрозою його існування. У цьому контексті слід зазначити, що однією з об'єктивних проблем забезпечення адекватної реакції держави на виклики сьогодення, породжувані функціонуванням глобального інформаційного суспільства, є проблема забезпечення дієвої протидії правопорушенням у сучасній інформаційній сфері.

Насамперед варто зазначити, що в сучасній Україні є вже певні позитивні зрушення у правовому регулюванні інформаційних відносин. Так, основними нормативно-правовими актами, які спрямовані на забезпечення належного стану інформаційної безпеки в сучасній Україні, зокрема, є закони України «Про інформацію», «Про доступ до публічної інформації», «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки України», Указ Президента України від 08.07.2009 року № 514/2009 «Про доктрину інформаційної безпеки України» та деякі інші нормативно-правові акти.

Як сказано в Законі України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства й держави, при якому запобігається завдавання шкоди через: неповноту, невчасність та невірогідність використовуваної інформації; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації [5].

Отже, захист інформаційної безпеки є складною системою відносин, що містить цілий комплекс векторів державної політики і зумовлена специфікою об'єктів інформаційної безпеки. При цьому є два комплекси питань, які диференціюються відповідно до природи правових норм, що становлять їх нормативно-правову базу. По-перше, це інформаційна безпека людини й суспільства, яка ґрунтується на конституційних правах особи і вимірюється ступенем її свободи, гарантіями від втручання держави та інших осіб, а також можливостями самореалізації й самовизначення. По-друге, це інформаційна безпека держави, яка пов'язана із застосуванням обмежень, заборон та жорсткою законодавчою регламентацією, невід'ємним елементом яких є сила державного примусу.

Слід зазначити, що відповідно до законодавства відповідальність за порушення законодавства про інформацію несуть особи, винні у вчиненні таких правопорушень: 1) необґрунтована відмова від надання відповідної інформації; 2) надання інформації, що не відповідає дійсності; 3) поширення відомостей, що не відповідають дійсності, ганьблять честь і гідність особи; 4) порушення порядку зберігання інформації; 5) навмисне знищення інформації; 6) розголошення державної або іншої таємниці, що охороняється законом.

Однак, виходячи зі змісту відповідних нормативно-правових актів, особливістю юридичної відповідальності в інформаційній сфері є те, що значна кількість актів, які визначають правові підстави, гарантії та процедури доступу до інформації для її подальшого використання, містять бланкетні норми, що відсилають до інших нормативних актів. Зокрема, ідеться про кодекси, крім того, вони можуть визначати лише вид правопорушень щодо інформації, не виокремлюючи при цьому конкретний механізм реалізації юридичної відповідальності за правопорушення в інформаційній сфері. Отже, нормативно-правове регулювання цього питання має досить хаотичний та несистемний характер.

Водночас велика кількість об'єктивних проблем притягнення винних осіб за правопорушення в інформаційній сфері пов'язана з усеохопним поширенням усіх видів інформації в електронній формі, і насамперед через мережу Інтернет. На цих проблемах варто зупинитися окремо.

«Інтернет», «кіберпростір», «віртуальна реальність» – це поняття, які за останнє десятиліття ввійшли не тільки в повсякденний обіг наших співвітчизників, а й почали активно «захоплювати» і наукову сферу людської діяльності. Однак, на жаль, мусимо визнати, що нині майже всі відносини, пов'язані зі збиранням, обробкою, передачею та іншим використанням інформації в електронній формі, не врегульовані правом, а на нормативному рівні навіть не визначені дефініції основних понять, на формально визначеній основі яких має будуватися правове регу-

лювання (наприклад, кіберпростір, кіберзлочинність, протокол передачі даних, шлюз, проксі-сервер тощо).

Слід зауважити, що в сучасних умовах складність забезпечення належної протидії правопорушенням в інформаційній сфері, і особливо в сфері електронно-цифрової інформації (використання всесвітньої мережі Інтернет), зумовлена багатьма об'єктивними причинами, серед яких насамперед доцільно виділити: 1) відсутність географічних кордонів та обмежень для миттєвого поширення, збирання, обробки та використання інформації, внаслідок чого Інтернет з його глобальними комунікаціями залишається поза сферою правового регулювання законів будь-якої держави, яка завжди має певну обмежену територію, на яку поширюється її суверенітет (поняття юрисдикції або дії нормативно-правового акта у просторі); 2) анонімність, яка підриває традиційне застосування юридичної відповідальності за скоєне правопорушення або злочин в інформаційній сфері, що забезпечує високий рівень латентності та низький рівень розкриття правопорушень; 3) легкодоступна змінюваність інформації в електронній формі: на відміну від стабільної документально оформленої інформації електронна інформація не має форми, сталої у часі та просторі. У зв'язку з цим електронна інформація циркулює переважно неконтрольовано та хаотично [6, с. 563].

Коли говоримо про кіберпростір, то маємо на увазі саме простір, а не територію, яка завжди має зв'язок з національними географічними кордонами, які, в свою чергу, впливають на компетенцію держав, чітко визначаючи її обмежену юрисдикцію. У зв'язку з цим варто погодитися з думкою, що помилково вважати кіберпростір територією зі змішаним міжнародно-правовим статусом. Усе-таки, його слід вважати міжнародним планетарним простором, що має специфічні особливості, а саме:

1) він об'єднує глобальні комп'ютерні мережі та інформаційні ресурси, що не мають чітко визначеного власника та забезпечують інтерактивну комунікацію фізичних і юридичних осіб;

2) взагалі не обмежений жодними кордонами;

3) має децентралізований статус, яким повністю не володіє та не управляє жодна держава, об'єднання держав, жодна міжнародна організація, а також жоден оператор зв'язку;

4) у кіберпросторі будь-яка особа може вільно діяти, висловлюватися та навіть працювати [7; с. 14, 15].

Ці ознаки кіберпростору переконливо свідчать, що він потребує спеціального правового регулювання, яке неможливо забезпечити лише в національному режимі.

З огляду на зазначені виклики на міжнародному рівні, насамперед держав–членів Ради Європи, було прийнято Конвенцію про кіберзлочинність від 23.11.2001 року (далі – Конвенція), ратифіковану Верховною Радою України із застереженнями і заявами 07.09.2005 року, яка набрала чинності в Україні 01.07.2006 року. Ця Конвенція вперше на міжнародному рівні класифікувала злочини, скоювані з використанням інформаційних комп'ютерних систем, на чотири відносно самостійні групи, а саме:

1) злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (наприклад, незаконний доступ до комп'ютерної системи; нелегальне перехоплення комп'ютерних даних, які не призначені для публічного користування, незаконне втручання в комп'ютерні дані, тобто навмисне пошкодження, знищення, погіршення, зміна або приховування комп'ютерної інформації без права на це тощо);

2) злочини, пов'язані з комп'ютерами (наприклад, шахрайство, пов'язане з комп'ютерами, тобто незаконне навмисне вчинення дій, що призводять до втрати майна іншої особи шляхом будь-якого введення, зміни, знищення чи приховування комп'ютерних даних або будь-якого втручання у функціонування комп'ютерної системи, з шахрайською, нечесною метою неправомірного набуття економічних переваг для себе чи іншої особи);

3) злочини, пов'язані зі змістом інформації в комп'ютерних системах (наприклад, злочини, пов'язані з виробленням та розповсюдженням дитячої порнографії за допомогою комп'ютерних систем);

4) злочини, пов'язані з порушенням авторських та суміжних прав (наприклад, незаконне розповсюдження комп'ютерних програм за допомогою комп'ютерних систем з комерційною метою) [8].

Отже, Конвенція про кіберзлочинність на офіційному міжнародно-правовому рівні окреслила основні категорії або групи злочинів, які можуть скоюватися за допомогою використання інформаційних комп'ютерних систем, і зокрема Інтернету. Безперечно, вказаний приблизний перелік кіберзлочинів із розвитком інформаційних технологій розширюватиметься, що потребуватиме адекватної правової реакції з боку національних держав, котрі в будь-якому разі мають чітко визначену юрисдикцію щодо притягнення осіб на власній території до кримінальної та інших видів юридичної відповідальності.

Крім цього, актуальним питанням, яке завжди виникає в разі необхідності притягнути особу до юридичної відповідальності за правопорушення в інформаційній сфері, є збирання відповідних доказів для доведення вини порушника (найважче це забезпечити, якщо інформація має електронну форму вираження). Слід також зазначити, що під час розгляду відносин з використання Інтернету необхідно враховувати й складний суб'єктний склад, який зумовлюється насамперед участю в цих відносинах операторів зв'язку (так званих провайдерів), що також спричиняє чимало додаткових питань за необхідності притягнення особи до юридичної відповідальності, які на сьогодні не вирішені у правовому полі. Зокрема, якщо умовно зобразити суб'єктний склад, який бере участь в інформаційних відносинах в Інтернеті, то він матиме такий вигляд: користувач або споживач певної інформації → провайдер або особа, яка забезпечує доступ користувача до мережі Інтернет → інформаційний ресурс, до якого звертається користувач → провайдер або особа, яка забезпечує доступ користувача до конкретного інформаційного ресурсу (так званий провайдер інформаційного ресурсу) → власник інформаційного ресурсу, до якого звертається користувач [9].

Усе це певним чином підриває застосування класичного принципу юридичної відповідальності – принцип персоніфікації відповідальності та покарання, який має особливо важливе значення під час реалізації адміністративної та кримінальної відповідальності та є однією з необхідних передумов забезпечення її законного та обґрунтованого застосування. З огляду на це важливим видається визначення на нормативному рівні відповідних підходів або критеріїв розмежування дій зазначених учасників інформаційного обігу в мережі Інтернет, що дало б змогу більш рельєфно підходити до питання про їх конкретну вину у тому чи іншому правопорушенні або злочині, а також міру або ступінь їх можливої співучасті.

Зокрема, дії інформаційних провайдерів в мережі Інтернет мають чітко визначену специфіку, на яку не можна не зважати в заявленому контексті. Так, провайдер самостійно не ініціює інформаційні відносини, не обирає зміст інформації, що передається, а також її отримувача, не впливає на зміст інформації та зберігає її тільки в межах часу, визначеного технічними стандартами та протоколами для потреб передачі інформації. Однак відповідальність провайдерів ґрунтується на тому, що вони мають організаційно-технічну можливість будь-якої миті впливати на інформаційні відносини своїх користувачів шляхом, наприклад, блокування шкідливого або небезпечного інформаційного обміну та інформування третіх осіб про зміст інформації, що передається [10].

Ще одна проблема полягає в необхідності розв'язати питання про контроль над інформацією, що поши-

рюється в електронних мережах, насамперед в Інтернеті. Крім цього, стає очевидним, що жодна сучасна держава не спроможна самостійно вирішити всі питання, пов'язані з розвитком електронного інформаційного простору, а тому в цьому напрямі необхідна організаційно-правова координація зусиль міжнародної спільноти. Всі ми пам'ятаємо про справи із закриттям файлообмінників «*Infostore.org*» та «*Ex.ua*», які були розміщені в датацентрі компанії-провайдера «Воля» та так і не одержали судового вирішення. В останньому випадку Інтернет-ресурс і сьогодні працює лише з деякими суто технічними обмеженнями. Схожих прикладів зі світової практики можна навести багато.

Враховуючи зазначені аспекти заявленої проблематики, можемо зробити певні висновки:

1) активний розвиток віртуального інформаційного простору та Інтернету як його центральної частини значно ускладнив механізм притягнення винних осіб до юридичної відповідальності за правопорушення в інформаційній сфері. Таке ускладнення має об'єктивний характер і пов'язане насамперед з технічно-комунікаційною сутністю кіберпростору та специфічними властивостями зберігання й поширення в ньому інформації в найрізноманітніших формах;

2) вирішити питання протидії правопорушенням в інформаційній сфері лише шляхом вдосконалення норм чинного законодавства неможливо. У цьому контексті варто передовсім наголосити на необхідності поєднання правових та організаційно-технічних засобів протидії правопорушенням в інформаційній сфері (наприклад, створення та застосування безпечних протоколів збереження та передачі інформації в електронних мережах). Мусимо констатувати, що позитивне право в цьому випадку певною мірою почало залежати від технічних нововведень, пов'язаних із віртуальним інформаційним простором;

3) поступовий розвиток глобального інформаційного суспільства потребує забезпечення його належного правового регулювання і на міжнародному, і на національному рівнях. Отже, на нашу думку, забезпечення ефективного правового регулювання всього інформаційного простору на національному рівні в Україні можливо досягти, зокрема, шляхом прийняття кодифікованого законодавчого акта (наприклад, Кодекс законів про інформацію в Україні або Кодекс інформаційного права України), який максимально враховував би права й законні інтереси всього суб'єктного складу відповідних правовідносин та забезпечив єдині підходи і принципи до регламентації відносин у кіберпросторі та юридичної відповідальності за незаконні дії в ньому чітко визначених суб'єктів. Дотримання цих умов значною мірою сприятиме безпеці розвитку інформаційної сфери України, захисту національного інформаційного простору, ринку від інформаційного тероризму та інформаційної війни тощо.

Джерела

1. *Монахов В.Н.* СМИ и Интернет: проблемы правового регулирования / Отв. ред. М. В. Горбаневский. – М.: ЭКОПРИНТ, 2003. – 320 с.

2. *Нерсесянц В. С.* Право и закон. Из истории правовых учений / Отв. ред. Л. С. Мамут. – М.: Наука. – 366 с.

3. Актуальные проблемы теории государства и права: Учеб. пособ. / Отв. ред. Р. В. Шагиева. – М.: Норма: ИНФРА-М, 2011. – 576 с.

4. Там само. – С. 536–537.

5. Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [Електронний ресурс]. – http://zakon2.rada.gov.ua/laws/show/537-16/print1330337542993813

6. Актуальные проблемы теории государства и права: Учеб. пособие / Отв. ред. Р. В. Шагиева. – М.: Норма: ИНФРА-М, 2011. – С. 563–576.

7. *Рассолов И. М.* Право и Интернет. Теоретические проблемы. – 2-е изд., доп. – М.: Норма, 2009. – 384 с.

8. Конвенція про кіберзлочинність. – [Електронний ресурс]. – http://zakon2.rada.gov.ua/laws/show/994_575/print1330337542993813

9. *Наумов В. Б.* Право и Интернет: Очерки теории и практики. – М.: Книжный дом «Университет», 2002. – 432 с.

10. Там само. – С. 18.

Безпека правоохоронних органів та особиста безпека правоохоронців під час охорони громадського порядку при проведенні спортивно-масових заходів Євро-2012

Анатолій СУББОТ,
кандидат педагогічних наук,
професор кафедри спеціальних дисциплін
та організації професійної підготовки
Національного університету державної
податкової служби України

Проведення фінальної частини Євро-2012 в Україні потребує від керівництва нашої держави продуманих і виважених заходів щодо якнайшвидшої адаптації різних сфер життєдіяльності суспільства до вимог організації спортивних змагань такого рівня. Адже зміна звичайного ритму життя населення, обмеження руху транспорту, скупчення великої кількості людей на певній території – усе це, як наслідок, сприяє зростанню емоційного напруження серед громадян. З огляду на це та відповідно до Закону України «Про організацію та проведення фінальної частини чемпіонату Європи 2012 року з футболу в Україні» основною метою правоохоронних органів є «забезпечення безпеки та правопорядку під час проведення турніру» [7]. Деталізовано ці завдання правоохоронців у відповідних державних, галузевих та регіональних цільових програмах.