

Харитонов Євген Олегович,
*доктор юридичних наук, професор, член-кореспондент НАПрН України,
заслужений діяч науки і техніки України, зав. кафедри цивільного права
Національного університету «Одеська юридична академія»*

COVID-19 ТА ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В умовах надзвичайних ситуацій, зокрема таких масштабних як епідемії/пандемії, для адекватної відповіді на породжені ними Виклики, крім належного рівня медицини, налагодженої системи охорони здоров'я та санітарно-епідеміологічної служби, важливе значення мають такі чинники як інформація та інформаційна безпека, призначенням яких є забезпечення поінформованості населення про перебіг пандемії та її наслідки, з одночасним уникненням панічних настроїв, істеричності або байдужості. У свою чергу, вимоги дотримання інформаційної безпеки можуть стати чинником обмеження інформації, усунення неправдивої інформації тощо, внаслідок чого виникає колізія права приватної особи на інформацію та права на безпечну інформацію (на безпеку інформації).

Значення згаданих категорій зумовлює необхідність визначитися щодо розуміння таких понять як «інформація», «інформаційна безпека», «загрози інформаційній безпеці».

Отже, виходимо з того, що інформація – це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді (стаття 1 Закону України «Про інформацію»). Як випливає з наведеного визначення ознаками інформації є те, що це: 1) будь-які відомості та /або дані, тобто, інформація, як така; 2) ці відомості та /або дані можуть бути зафіксовані будь-яким чином [1].

«Інформаційна безпека» розуміється як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [7]. При цьому поняття «загрози інформаційній безпеці» охоплює як ті загрози, котрі створює сама інформація, так і ті, що виникають для неї «ззовні». З погляду цивілістичного це означає, що у першому випадку йдеться про попередження шкоди та ліквідацію шкоди, що виникає внаслідок неналежного використання інформації та інформаційно-комунікативних технологій. Оскільки у цьому разі інформація є засобом реалізації

протиправного наміру, зняряддям протиправних дій, тут можна вести мову про «небезпеку від інформацію» або ж про «інформаційну безпеку».

У другому випадку йдеться про захист інформації як об'єкту цивільних прав, попередження та ліквідацію наслідків активних протиправних дій осіб, які зазіхають на інформацію, намагаються спотворити інформацію, знищити її тощо.

До числа загроз інформаційній безпеці, яким надається правове значення і які мають попереджатися (усуватися), належать: 1) неповнота, невчасність та невірогідність інформації, що використовується; 2) негативний інформаційний вплив; 3) негативні наслідки застосування інформаційних технологій; 4) несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Істотні загрози інформаційній безпеці створюють «інформаційні війни», поняття та концепція яких сформувалися протягом 90-х років минулого століття [2] і набувають нового наповнення та забарвлення в умовах пандемії COVID-19 тощо. При цьому «воєнні дії» практично повністю зміщуються у онлайн сферу, головним чином у соціальні мережі [6].

В умовах інформаційної війни широко використовується такий засіб, як фейк, що є спотворенням правди. Він відрізняється від піару чи пропаганди, які усе ж таки так чи інакше, більшою чи меншою мірою базуються на правді, можливо, викривляючи її. Фейк не хоче бути правдою, для нього важливіші досягнення власних цілей, а не інформування людини. Фейки є навмисним спотворенням інформації, але виконаним таким чином, щоб споживач інформації цього не помітив.

Не буде перебільшенням твердження, що найбільшу загрозу інформації в умовах пандемії становлять саме фейки. До прикладу, протягом 2020 року 40 відсотків дописів про COVID-19 були створені фейковими сторінками [4]. Втім, у такому активному поширенні фейків, мабуть, немає нічого дивного, якщо врахувати, що їхнім поширенням (зокрема, стосовно коронавірусу) займається величезна кількість фігурантів, у тому числі ботів та людей, які фактично виконують функції ботів [8].

З урахуванням викладеного розглянемо загрози, що їх створюють інформаційні війни в умовах COVID-19, а також шляхи їх подолання. Нагальність вивчення цього питання зумовлена тим, що саме безпека інформації є найбільш вразливим елементом змагання влади і суспільства з пандемією COVID-19. Якщо за умови належного функціонування і відповідним чином налагодженої системи охорони здоров'я власне лікування хворих відбувається за встановленим протоколом об'єктивно спрямовує до

позитивного результату, то кінцевий результат залежить не лише від зусиль влади і медиків, а потребує ще й бажання і готовності населення до подолання пандемії, вакцинації тощо чинників неможливі без відповідного інформаційного забезпечення та безпечності інформації у цій сфері. І це є «слабкою ланкою».

Визначаючи шляхи її зміцнення, зауважимо, що загрози інформаційній безпеці у соціальних мережах не можуть бути подолані за допомогою використання лише технічних засобів, оскільки останні здатні впливати лише на технічну складову ІТ-сфери, залишаючи поза увагою «соціальний елемент» яким є учасники відповідних відносин. Це не можна визнати виправданим, оскільки наразі саме соціальний елемент є головним чинником порушення інформаційної безпеки, а людину називають поміж Топ-10 цифрових загроз ХХІ століття [3].

Отже, у пошуках впливу на цю складову ІТ-сфери маємо розглянути засоби правового тощо впливу на людський чинник як джерело загроз інформаційній безпеці.

Важливим профілактичним засобом боротьби з інформаційними загрозами є інформаційна гігієна.

Експерти зазначають, що безпечність українців в інформаційному просторі та відсутність гігієни в Мережі вбиває імунітет до кіберзагроз. На їхню думку, суспільство практично не захищене. Про безпеку люди думають дуже мало. Всі читають про кібератаки і хитрих хакерів, але водночас ставлять собі примітивні паролі просто через те, що їм так зручно, викладають про себе інформацію, яку стороннім знати не обов'язково. Низька культура безпеки є чинником вірусмейкерства у Мережі [5].

З погляду юридичного, «інформаційну гігієну» слід визнати чинником формування правосвідомості, умовою ефективності застосування правових засобів, поміж яких важливе місце займають засоби публічно-правового впливу.

Тому вирішення проблеми безпеки інформації (безпечності інформації) потребує врахування двох аспектів: законодавчого та правозастосовного.

Разом із тим, хоча створення актів законодавства, спрямованих на гарантування інформаційної безпеки має важливе значення, але не менш важливим є активізація застосування вже існуючого законодавства, норми якого у багатьох випадках дозволяють достатньо ефективно захищати права та інтереси учасників ІТ-відносин пов'язані з інформаційною безпекою.

Оскільки застосування заходів інформаційної безпеки припускає застосування певних обмежень та засобів державного примусу, неминуче

виникає колізія використання згаданих засобів здійснення та права на інформацію.

Особливо гостро постає ця проблема, коли йдеться про обмеження у сфері ІТ, котра за своєю сутністю є феноменом, що забезпечує вільний доступ до різноманітної інформації і, до того ж, має транскордонний характер.

Зазначимо, що право на інформацію деталізоване у Законі про інформацію, котрий передбачає низку гарантій здійснення цього права. Так, ст. 5 Закону про інформацію передбачає, що кожен має право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів. Разом із тим, ст. 2 цього Закону встановлює, що основними принципами інформаційних відносин є: гарантованість права на інформацію; відкритість, доступність інформації, свобода обміну інформацією; достовірність і повнота інформації; свобода вираження поглядів і переконань; правомірність одержання, використання, поширення, зберігання та захисту інформації. Водночас, ст. 3 Закону про інформацію передбачає певні зобов'язання держави у цій галузі, визначаючи, що основними напрямками державної інформаційної політики є: забезпечення доступу кожного до інформації; забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації; створення умов для формування в Україні інформаційного суспільства тощо. У свою чергу, вимогою до реалізації права на інформацію є те, що вона не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб.

Підсумовуючи викладене, можна зробити висновок, що, хоча головні засади інформаційної безпеки (у тому числі, в умовах пандемії) визначені Законом про інформацію, в умовах пандемії COVID-19, загострюється колізія права приватної особи на інформацію та її ж права на безпеку інформації (безпечну інформацію), котра потребує спеціального дослідження.

ЛІТЕРАТУРА:

1. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12>
2. Курбан О.В. Інформаційні війни у соціальних онлайн мережах: монографія. К., 2017. С. 21-24.
3. Макаревич Е. ТОП-10 цифровых угроз XXI века. Фокус. 2017. № 27. С. 20-23.
4. Мороз О. Борьба за правду: Як мій дядько переміг брехню. Київ, 2020. С. 131-132.

5. Мороз О. Нація овочів? Як інформація змінює мислення і поведінку українців. Київ, 2020. С. 260-278.
6. Сінгер П.В., Брукінг Емерсен Т. Війна лайків. Зброя в руках соціальних мереж. Харків. 2019. 319 с.
7. Харитонов Є.О. Інформація, безпека та приватне право. Інформаційна безпека: проблеми приватного права: навчальний посібник; За ред. Є.О. Харитонов; Одеса, 2019. С.7-15.
8. Смаль Ю. Як я була ботом. Київ, 2019. 152 с.

Харитонova Олена Іванівна,
*доктор юридичних наук, професор, член-кореспондент НАПрН України,
завідувачка кафедрою права інтелектуальної власності та патентної юстиції
Національного університету «Одеська юридична академія»*

КОНФЛІКТ ІНТЕРЕСІВ ТА ШЛЯХИ ЙОГО ПОДОЛАННЯ У КОНТЕКСТІ ПАНДЕМІЇ COVID-19

Право на охорону здоров'я є одним з основних прав людини і тому є визначальним у формуванні державної політики у цьому напрямку. Реалізація і дотримання цього права залежать від багатьох факторів і не в останню чергу від балансу інтересів всіх учасників правовідносин, які при цьому виникають.

Права інтелектуальної власності, з одного боку, є важливим стимулом для розробки нових продуктів у сфері охорони здоров'я та водночас, є чинником серйозних суперечок між Світовою організацією торгівлі (СОТ) та Всесвітньою організацією охорони здоров'я (ВООЗ). Ця проблема не є новою.

Зокрема, ВООЗ висловлював побоювання в тому, що патентний захист нових лікарських препаратів за відсутності механізму контролю над цінами може стати чинником подорожчання цих ліків. Однак виготовлення аналогу препарату без згоди патентовласника є правопорушенням. Ці суперечки посилюються у зв'язку з прийняттям Угоди TRIPS, що діє в межах СОТ і передбачає уніфіковані правила регулювання патентів.

Проблема патентного захисту лікарських препаратів була предметом обговорення на міністерській конференції СОТ у столиці Катару Дохі. Бразилія і Індія запропонували негайно переглянути Угоду TRIPS, а саме ті її положення, що перешкоджають безоплатному копіюванню запатентованих ліків. В свою чергу, США і Швейцарія заперечували проти цього, аргументуючи свою позицію тим, що це зачіпає права розробників, що неприпустимо в умовах чесної конкуренції.