3.3. Доступ до публічної інформації у формі відкритих даних через мережу Інтернет

Правовий режим публічної інформації в мережі Інтернет

Сучасний етап розвитку нашого суспільства і держави Україна свідчить про те, що особливої ваги в ньому набула інформація як специфічний об'єкт, з приводу якого складається велика кількість суспільних відносин. Не є винятком і публічно-правова сфера, суб'єкти якої виступають у ролі джерела інформації, тобто в результаті їхньої діяльності з'являється нова, трансформується чи оновлюється вже відома інформація.

Загалом, під інформацією розуміють продукт взаємодії даних і методів, розглянутий в комплексі цієї взаємодії. Інформація – це динамічний об'єкт, що не існує в природі сам по собі, а утворюється в ході взаємодії даних і методів[1].

Відповідно до Закону України «Про інформацію» за змістом інформація може поділятися на невизначену кількість різноманітних видів. Це інформація про фізичну особу (персональні дані), довідково-енциклопедичного характеру, про стан довкілля (екологічна інформація), про товар (роботу, послугу), науково-технічна, податкова, правова, статистична, соціологічна та інші види[2].

Спеціальними законами щодо окремих видів інформації за змістом можуть встановлюватися спеціальні правові режими такої інформації. Прикладами є, зокрема, персональні дані, статистична, екологічна інформація.

За рівнем доступу публічна інформація поділяється на відкриту інформацію та інформацію із обмеженим доступом, а остання, у свою чергу, на конфіденційну, таємну і службову. Разом із тим, належність інформації до певного виду інформації за змістом не визначає наперед безумовного віднесення такої інформації до кате-

[1] Клімушин П. С. Електронне урядування в інформаційному суспільстві : [монографія] / П. С. Клімушин, А. О. Серенок. – Харків : Магістр, 2010. – 311 с.

[2] Про інформацію : Закон України від 2 жовт. 1992 р. № 2657-XII // Відом. Верхов. Ради України. – 1992. – № 48. – Ст. 650.

горії відкритої чи інформації із обмеженим доступом. Не всі персональні дані є конфіденційною інформацією, і не вся екологічна інформація є відкритою, а статистична – службовою інформацією. Наприклад, закон встановлює загальне правило, за яким екологічна інформація не може бути віднесена до інформації із обмеженим доступом. Разом із тим, закон передбачає і виключення із цього правила (інформація про місце розташування військових об'єктів може бути обмежена у доступі).

У сфері інформації виділяють два основних напрями забезпечення прав і свобод громадянина:

– «право на інформацію», що включає права і свободи думки, слова, творчості, світогляду і віросповідання, зібрань, звернень до органів державної влади і органів місцевого самоврядування і ЗМІ, вільного доступу до інформації про стан довкілля, якість харчових продуктів тощо;

– «право на доступ до інформації», яке пов'язується з відкритістю діяльності публічної влади та передбачає правову можливість громадян отримати відомості, які мають органи публічної влади у зв'язку з реалізацією ними своїх повноважень[1].

Логічним є з'ясувати сутність двох ключових понять – «публічна інформація» та «доступ» до неї.

Відповідно до положень статті 1 Закону України «Про доступ до публічної інформації» публічна інформація – це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена у процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом[2].

Таким чином, публічна інформація це інформація:

– отримана або створена розпорядниками – суб'єктами владних повноважень (надалі – СВП) у процесі виконання їх обов'язків;

[1] Жиляєв І. Б. Інформаційне право України: теорія і практика : [монографія] / І. Б. Жиляєв. – Київ : Парлам. вид-во, 2009. – 103 с.

[2] Про доступ до публічної інформації : Закон України від 13 січ. 2011 р. № 2939-VI // Відом. Верхов. Ради України. – 2011. – № 32. – Ст. 314.

– знаходиться у володінні інших розпорядників, визначених цим законом.

Таким чином, будь-яка інформація за змістом у будь-якій матеріальній формі (на паперових чи електронних носіях) у вигляді тексту, зображення, карти, схеми чи фото, запису звуку або відео, отримана або створена суб'єктом владних повноважень має статус публічної інформації. Відносно розпорядників – суб'єктів владних повноважень, юридичних осіб, які виконують делеговані повноваження, у тому числі надають державні послуги, чи фінансуються за рахунок державного бюджету статус публічної інформації безпосередньо пов'язаний із статусом розпорядників, тобто із створенням, збиранням, зберіганням і обробленням інформації за рахунок бюджетних коштів. Поширення положень закону і на осіб, що здійснюють делеговані повноваження чи фінансуються із державного бюджету, перекликається із Конвенцією про доступ до інформації, участь громадськості у процесі прийняття рішень та доступ до правосуддя з питань, що стосуються довкілля (надалі – Оргуська конвенція). Ще у 1999 році із ратифікацією Конвенції Україна взяла на себе міжнародне зобов'язання налагодити правові та інституційні інструменти для забезпечення вільного доступу до екологічної інформації не лише безпосередньо органами влади, але й будь-якими фізичними чи юридичними особами, які виконують державні адміністративні функції, відповідно до національного законодавства, включаючи здійснення діяльності чи надання послуг у сфері навколишнього середовища.

З технічної точки зору мережа Інтернет являє собою сукупність інформаційних ресурсів і систем, з'єднаних за допомогою електрозв'язку, обмін інформацією у яких здійснюється на базі єдиної системи стандартів і протоколів. У ній власники Інтернет ресурсів мають можливість розміщувати власну інформацію або інформацію третіх осіб за допомогою різноманітних технологій і систем, а користувачі наділені можливістю одержувати цю інформацію різними методами, серед яких переважають доступ до інформаційних ресурсів (сайтів) у мережі Інтернет і використання електронної пошти[1].

[1] Жилінкова І. Правове регулювання Інтернет відносин / І. Жилінкова // Право України. – 2003. – № 5. – С. 12–127.

Розглядаючи правовий режим інформаційних ресурсів і доступу до них, варто зважити на те, що нині найскладнішою є проблема правового регулювання відповідних аспектів функціонування глобальної світової мережі Інтернет. Труднощі починалися навіть від того, що протягом тривалого часу не було чіткого визначення суті цього явища, що для права взагалі є критичним фактором. Адже брак чітко окресленого предмета регулювання стає неефективним або взагалі неможливим. Спроби сформулювати його були спрямовані, насамперед, на групуванні певних функціональних ознак мережі Інтернет. Наприклад, мережу Інтернет визначали як універсальну систему об'єднаних мереж, які уможливлюють забезпечення включення будь-яких масивів інформації для надання її користувачам, надання довідкових і інших інформаційних послуг, а також здійснення різних цивільно-правових угод на основі комбінації інформаційно-комунікаційних технологій. Проте подібні йому формулювання не передбачали головного – можливості чітко окреслити правовий статус цієї системи та суб'єктів, діяльність яких пов'язана з нею. В українському законодавстві правове визначення поняття мережі Інтернет міститься у нормах ст. 1 Закону України «Про телекомунікації», згідно з яким мережа Інтернет – це всесвітня інформаційна система загального доступу, яка логічно пов'язана глобальним адресним простором і базується на Інтернет-протоколі, визначеному міжнародними стандартами[1].

На основі цього визначення можна сформулювати низку ключових ознак мережі Інтернет, що виражають особливості правового регулювання окремих її функцій:

1. Мережа Інтернет – це інформаційна система, тобто сукупність телекомунікаційних мереж і засобів для накопичення, опрацювання, зберігання та передавання даних. Інформаційна система Інтернет має ще дві додаткові ознаки, якими вона відрізняється від різних спеціалізованих, закритих, або локальних інформаційних систем (наприклад, військових, банківських, локальних комп'ютерних систем і мереж різних установ, підприємств і організацій).

[1] Про телекомунікації : Закон України від 18 листоп. 2003 р. № 1280-IV // Відом. Верхов. Ради України. – 2004. – № 12. – Ст. 155.

2. Додатковими ознаками є всесвітній характер доступу, тобто відкритість мережі Інтернет для доступу з будь-якої можливої точки світу, де є необхідне обладнання та загальний характер доступу, тобто можливість будь-якої особи без додаткових обмежень або дозволів отримати доступ та користуватися основними послугами мережі.

3. Невід'ємною характеристикою цієї мережі є глобальний адресний простір, тобто сукупність адрес мережі Інтернет, за допомогою яких впорядковуються та пов'язуються між собою окремі інформаційні ресурси (Інтернет-сторінки) та користувач дістає можливість переходити від одного інформаційного ресурсу до іншого.

4. Згідно із Законом України «Про телекомунікації», адреса мережі Інтернет – це визначений чинним у мережі міжнародними стандартами цифровий та (або) символьний ідентифікатор доменних імен в ієрархічній системі доменних назв. Фактично це назва, яка присвоюється окремому електронному інформаційному ресурсу – Інтернет-сторінці. Наприклад, адресою Інтернет-сторінки Верховної Ради України є http://www.rada.gov.ua/.

5. Використання так званого Інтернет-протоколу, який визначається міжнародними стандартами. Це її певний технічний стандарт, використання якого забезпечує можливість окремим персональним комп'ютерам з'єднуватися між собою, використовуючи дротові й бездротові телекомунікаційні мережі. Міжнародний характер цього технічного стандарту зумовлений глобальним характером мережі Інтернет, за якого окремі держави не здатні вводити національні стандарти, що відрізняються від нього, оскільки це виключило б інформаційні мережі такої держави із загальної мережі. Слід також виділити такий термін, як національний сегмент мережі Інтернет, який використовують у національних і міжнародних актах. Цей термін означає сукупність адрес мережі Інтернет, яким присвоєно код країни, визначений міжнародними стандартами. Кожна держава має право визначати певні нормативно-правові стандарти та правила реєстрації, використання й адміністрування подібних адрес. Український сегмент мережі Інтернет охоплює сукупність електронних інформаційних ресурсів, яким присвоєні адреси, побудовані на домені «UA».

На основі зазначеного вище тлумачення сутності поняття «Інтернет» можна визначити основні підходи до правових аспектів цього явища:

1. Мережа Інтернет в цілому не є суб'єктом права. Це є сукупність інформаційного обладнання й інформаційних ресурсів. Але він не є ні міжнародною організацією, ні юридичною особою, ні будь-якою іншою організованою структурою, яка може вступати в правовідносини.

2. Інтернет у цілому не є об'єктом права. У мережі Інтернет немає єдиного конкретного власника, як і немає такого суб'єкта, який би управляв або контролював досить значну частину цієї мережі. Понад те, через технічні особливості жодна складова не є критичною для функціонування всієї системи.

Для правильного аналізу видів інформаційної діяльності, що проводиться за допомогою мережі Інтернет, слід також визначити два основні способи поширення інформації за допомогою цієї мережі; активне – через електронну пошту і пасивне – розміщення інформації на електронних сторінках, до яких користувач звертається самостійно. Ці види поширення інформації мають принципово різні основи правового регулювання. Так, активне може здійснюватися проти волі її адресата. Масові розсилання рекламної або іншої інформації, яку користувач не замовляв, дістали назву «спам». Через це спочатку провайдерами мережі, а в деяких країнах і на законодавчому рівні, застосовують певні обмеження таких дій. Ключовим мотивом у цьому є те, що користувач змушений оплачувати прийняття електронних листів, які йому не потрібні.

Іншим важливим аспектом є те, що розміщення інформації на електронних сторінках є пасивним способом поширення інформації. Користувач самостійно, на власний розсуд, звертається до такої сторінки. Саме ця особливість поширення інформації у мережі Інтернет уможливлює визначення, що мережа в цілому не є ЗМІ. Адже законодавство однозначно відносить мережу Інтернет до одного з видів телекомунікацій, тобто до засобів передавання і приймання інформації в електронному вигляді. Власник інформаційного ресурсу не робить ніяких активних дій щодо доставки інформації до користувача. Натомість і друковані, й електронні ЗМІ (телебачення та

радіомовлення) передбачають певні способи доставки інформації до користувача (поширення через передплату, роздрібну торгівлю, трансляцію тощо).

Зазначимо, що спроби визначити мережу Інтернет як якесь специфічне середовище, тобто як певну віртуальну субстанцію, може стати спробою вивести цей засіб комунікації з правового поля, що гарантує свободу слова, конфіденційність кореспонденції тощо. Подібні спроби вже робили у деяких державах і вони були припинені лише завдяки ефективній роботі правозахисних механізмів. Так, у червні 1997 р. Верховний Суд США відкинув положення закону «Про пристойність у засобах зв'язку», згідно з якими поширення матеріалів непристойного змісту, до яких може отримати доступ неповнолітня особа, кваліфікується як злочин, оскільки це було б порушенням захищеною конституцією права свободи слова. В аспекті визначення правового статусу інформаційних ресурсів мережі Інтернет і пов'язаних із цим питань захисту прав фізичних і юридичних осіб варто згадати також Постанову Вищого арбітражного суду України «Про питання захисту авторських прав в Інтернеті». Вона визнає, що розміщення творів у мережі у вигляді, доступному для публічного використання, є їх відтворенням у розумінні ст. 4 Закону України «Про авторське право і суміжні права», у зв'язку з чим на розміщення творів у мережі Інтернет поширюється дія цього Закону»[1].

В юридичній науці вже сформовано загальну систему теоретичних концепцій, які охоплюють собою основні визначальні особливості обміну інформацією та зумовлюють необхідність розроблення і формування специфічного правового регулювання такого роду відносин.

Так, науковці виділяють наступні особливості обігу інформації в мережі Інтернет:

1) обмін інформацією відбувається в електронній цифровій формі, що у зв'язку з можливою легкістю й оперативністю створення, поширення, модифікації або знищення інформації, зумовлює виникнення проблем щодо забезпечення доказування і, відповідно, – умови для об'єктивного ускладнення захисту прав та інтересів осіб;

[1] Про авторське право і суміжні права : Закон України від 23 груд. 1993 р. № 3792-XII // Відом. Верхов. Ради України. – 1994. – № 13. – Ст. 64.

2) створення й розвиток інформаційних ресурсів та систем у мережі Інтернет і поширення інформації відбуваються винятково в рамках узгоджених міжнародних технічних стандартів і протоколів, що визначає високу значимість технічних норм для характеру відносин та їх регулювання;

3) в силу існуючого рівня технологій обмін інформацією може відбуватися у режимі реального часу (без помітної часової затримки для суб'єктів відносин);

4) у мережі Інтернет прийнята єдина система адресації ресурсів і систем, тому будь-яка особа з будь-якої точки мережі має однакову технічну можливість доступу до інформації та її поширення;

5) суб'єктами суспільних відносин, що виникають у зв'язку з використанням мережі Інтернет, виступають не тільки особи, з волі яких поширюється й споживається та або інша інформація, а й особи, які володіють інформаційними ресурсами, системами, мережами електрозв'язку, якими відбувається інформаційний обмін. Таким чином, наявність організаційно-технічних можливостей впливати на характер цих відносин визначає актуальну для мережі Інтернет проблему відповідальності інформаційних провайдерів (посередників);

6) наявність широких можливостей і затребуваності механізмів саморегулювання, коли власники інформаційних ресурсів і систем мають можливість оперативно визначати обсяг інформації та контролювати обмін нею;

7) суб'єкти відносин взаємовіддалені у просторі, у результаті чого виникає проблема визначення юрисдикції регулювання відносин з боку різних держав і адміністративно-територіальних утворень.

Варто відзначити, що в той же час, публічна інформація може бути поширена різними способами, у різних формах. Надання інформації відрізняється: за правовою і організаційною формою (звіти депутатів і місцевих голів про свою діяльність, інформаційні конференції тощо); за кількісним охопленням членів територіальної громади (індивідуальні – особистий контакт; колективні – збори, конференції); за характером передачі (усна, документальна, через ЗМІ, Інтернет тощо)[1].

[1] Лиска О. Г. Участь територіальної громади в місцевому самоврядуванні / О. Г. Лиска // Держ. буд-во. – 2008. – № 1. – С. 90–99.

Як зазначає М. Лациба[1], можна виділити такі основні форми оприлюднення інформації державними органами:

– офіційні сайти державних органів, включаючи інформацію у форматі сайту на електронних носіях – дисках чи інших електронних повідомленнях, що їх видають державні службовці;

– офіційні повідомлення власних інформаційних служб державних органів, включаючи прес-конференції та публічні виступи уповноважених посадових осіб;

– офіційні засоби масової інформації (друковані та електронні ЗМІ та інші видання, наприклад бюлетені та збірники, визначені законом або регулюючим органом);

– повідомлення безпосередньо зацікавленим особам або їх представникам (усні, письмові, надані засобами зв'язку чи за допомогою спеціальних засобів, як-от криптографії чи сурдоперекладу);

– державні архіви та власні архіви державних органів;

– повідомлення в інших друкованих та електронних засобах масової інформації, а також у мережі Інтернет.

Враховуючи сучасні тенденції трансформації політичної сфери у зв'язку із впровадженням інформаційно-комунікаційних технологій, Інтернет необхідно розглядати як основний засіб реалізації права людини на доступ до публічної інформації. Так, Інтернет забезпечує можливість знайти інформацію в он-лайн режимі стосовно конкретних життєвих подій або питань державної політики через використання пошукових механізмів, програм для перевірки стилю чи підвищення розбірливості офіційних текстів; використовуючи багатомовні переклади офіційних документів; через глосарії тощо[2].

Україна також долучається до світових тенденцій, доказом чого є прийняття Національної програми інформатизації. Її головною метою є створення необхідних умов для забезпечення громадян та суспільства своєчасною, достовірною та повною інформацією шляхом широкого використання інформаційних технологій, так як відкритість інформації державних органів є основним засобом контролю з боку

[1] Інформаційна відкритість органів державної влади України / за заг. ред. М. Лациби. – Київ : Укр. незалеж. центр політ. дослідж., 2005. – 156 с.

[2] Управління за участю громадян: Міжнародний досвід та рекомендації для України / Верхов. Рада України. – Київ, 2004. – С. 110.

суспільства за діями держави. І саме Інтернет вперше створив адекватне середовище для впровадження такого контролю[1].

Говорячи про Інтернет як засіб для громадськості отримати інформацію, необхідно розуміти, що ініціаторами поширення певної інформації не завжди виступає одна і та ж інстанція. Зокрема, існує:

– низхідне поширення інформації – має місце тоді, коли влада інформує громадян про конкретні питання розробки публічної політики, а також про їх роль та обов'язки;

– висхідне поширення інформації – має місце тоді, коли громадяни виражають своє занепокоєння з приводу наявної проблеми і бажання отримати роз'яснюючу інформацію;

– поширення інформації, що не було ініційоване жодною із сторін, тобто отримання певної інформації, як результат пошуку за визначеними ознаками та невизначеним джерелом походження[2].

Суб'єктний склад відносин, пов'язаних із використанням публічної інформації у формі відкритих даних через мережу Інтернет

Відповідно до положень Закону України «Про доступ до публічної інформації» суб'єктами відносин із доступу до публічної інформації є:

1) запитувачі інформації – фізичні, юридичні особи, об'єднання громадян без статусу юридичної особи, крім суб'єктів владних повноважень;

2) розпорядники інформації:

– суб'єкти владних повноважень – органи державної влади, органи місцевого самоврядування, інші суб'єкти, що здійснюють владні управлінські функції відповідно до законодавства та рішення яких є обов'язковими для виконання;

– юридичні особи, що фінансуються з державного, місцевих бюджетів, бюджету Автономної Республіки Крим, – стосовно інформації щодо використання бюджетних коштів;

---

[1] Харечко І. З. Політико-правові аспекти доступу до публічної інформації в Україні через мережу Інтернет / І. З. Харечко / Актуал. проблеми політики. – 2013. – Вип. 49. – С. 131–140.

[2] Сидора В. С. Типізація форм та механізмів взаємодії між органами влади і онлайн-спільнотами / В. С. Сидора // Наук. вісн. Акад. муніцип. упр. Серія «Управління». – 2010. – Вип. 3. – С. 501–508.

– особи, якщо вони виконують делеговані повноваження суб'єктів владних повноважень згідно із законом чи договором, включаючи надання освітніх, оздоровчих, соціальних або інших державних послуг, – стосовно інформації, пов'язаної з виконанням їхніх обов'язків;

– суб'єкти господарювання, які займають домінуюче становище на ринку або наділені спеціальними чи виключними правами, або є природними монополіями, – стосовно інформації щодо умов постачання товарів, послуг та цін на них;

– суб'єкти господарювання, які володіють: а) інформацією про стан довкілля; б) інформацією про якість харчових продуктів і предметів побуту; в) інформацією про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, що сталися або можуть статися і загрожують здоров'ю та безпеці громадян; г) іншою інформацією, що становить суспільний інтерес (суспільно необхідною інформацією);

3) структурний підрозділ або відповідальна особа з питань доступу до публічної інформації розпорядників інформації[1].

Таким чином, крім безпосередньо суб'єктів владних повноважень, положення закону щодо забезпечення доступу до публічної інформації покладається і на інших суб'єктів – інших розпорядників. Це зумовлено суспільним інтересом до певних видів інформації, в силу чого на таку інформацію поширюється режим публічної, навіть якщо знаходиться у володінні суб'єктів господарювання (наприклад, екологічна інформація). Закон розкриває зміст поняття публічної інформації через поняття розпорядників такої інформації, адже фактично говорить, що публічною є інформація, яка знаходиться у суб'єктів, визначених законом розпорядниками публічної інформації.

Існують наступні можливі варіанти суб'єктів у сфері обігу публічної інформації:

1) суб'єкти владних повноважень – органи державної влади, інші державні органи, органи місцевого самоврядування, органи влади Автономної Республіки Крим, інші суб'єкти, що здійснюють владні управлінські функції відповідно до законодавства та рішення яких є обов'язковими для виконання;

[1] Про доступ до публічної інформації : Закон України від 13 січ. 2011 р. № 2939-VI // Відом. Верхов. Ради України. – 2011. – № 32. – Ст. 314.

2) особи, якщо вони виконують делеговані повноваження суб'єктів владних повноважень згідно із законом чи договором, включаючи надання освітніх, оздоровчих, соціальних або інших державних послуг;

3) суб'єкти господарювання, які володіють інформацією, що становить суспільний інтерес (є суспільно необхідною інформацією);

4) юридичні особи, що фінансуються з державного, місцевих бюджетів, бюджету Автономної Республіки Крим;

5) суб'єкти господарювання, які займають домінуюче становище на ринку або наділені спеціальними чи виключними правами, або є природними монополіями[1]

В юридичній науці немає єдиного сталого підходу до розуміння кількісного суб'єктного складу інформаційних відносин у мережі Інтернет.

Так, Г. Г. Почепцов та С. А. Чукут, в якості основних суб'єктів інформаційних відносин які виникають, функціонують та реалізуються в мережі Інтернет, називають:

– власників інформації і власників інформаційних ресурсів в Інтернеті;

– інформаційних посередників (провайдери);

– користувачів[2].

В той же час, на думку В. А. Копилова, у даний час можна виділити три групи суб'єктів, які діють в Інтернеті. Перша група – це розробники транскордонних інформаційних мереж, інших технічних засобів, які становлять інфраструктуру Інтернету. У другу групу входять фахівці, які виробляють і поширюють інформацію в Інтернеті і надають різні послуги. І третя група – це різноманітні споживачі (громадяни, організації, фірми тощо)[3].

Ю. Є. Булатецький стосовно відносин сегмента Інтернету виділяє в якості суб'єктів, з одного боку, провайдера (оператора), тобто юридичну особу (фізичну особу – підприємця), яка має ліцензію

[1] Основні положення Закону України «Про доступ до публічної інформації» в контексті інформації про стан довкілля : посіб. для суб'єктів влад. повноважень на місц. рівні / ТзОВ «Компанія «Манускрипт», 2012 р. – 40 с.

[2] Татарова В. С. Особливості правового регулювання мережі інтернет / В. С. Татарова // Упр. розвитком. – 2014. – №6 (169). – С. 105–108.

[3] Копылов В. А. Информационное право / В. А. Копылов. – М., 2008. – С. 130–140.

Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації (а також провайдери, які не мають власної ліцензії, але купують інтернет-трафік у операторів, які мають її) на надання відповідних онлайнових послуг, включаючи поштове обслуговування, зберігання файлової інформації та ін. З іншого боку, користувача-клієнта, тобто фізичну або юридичну особу, яка використовує Інтернет для власних потреб (реклами, укладення угод, пошуку партнерів, замовлень і т.д.). Ці суб'єкти можуть перебувати у різних частинах світу[1].

Є. П. Литвинов пропонує свою власну концепцію розподілу і класифікації суб'єктів інформаційних відносин в мережі Інтернет, яка виглядає наступним чином: суб'єкти інформаційних відносин у мережі Інтернет – це власники або носії певних прав та обов'язків у віртуальному просторі Інтернету. І суб'єктами тут можуть виступати як юридичні особи (провайдери, які мають ліцензії на надання он-лай нових послуг, так і ті провайдери, які купують інтернет-трафік у операторів, які мають ліцензію), фізичні особи (громадяни – споживачі інформації: громадяни України, іноземці, особи без громадянства та ін.). Причому зазначені особи повинні відповідати вимогам міжнародного та національного законодавства в частині правоздатності, дієздатності, деліктоздатності.

Таким чином, на думку автора, основними учасниками мережі Інтернет виступають:

1) користувачі;

2) оператори зв'язку;

3) сервіс-провайдери, які забезпечують доступ до Мережі;

4) хост-провайдери, що мають за плату дисковий простір на своєму сервері клієнтам, а також інші базові послуги Інтернету;

5) розробники транскордонних інформаційних мереж та мережевих технологій;

6) спеціалісти[2].

---

[1] Булатецкий Ю. Е. Правовое обеспечение электронной торговли / Ю. Е. Булатецкий // Коммерческое (торговое) право / под ред. Ю. Е. Булатецкого. – М., 2002. – С. 880–886.

[2] Литвинов Є. П. Правовідносини в інтернет-праві / є. П. Литвинов // Часопис Київ. ун-ту права. – 2013. – №3. – С. 145–149.

Цікаву наукову концепцію щодо суб'єктного складу інформаційних відносин в мережі Інтернет пропонує О. І. Яременко. Так, на думку цього вченого: суб'єктами інформаційно-правових відносин є їх учасники, які володіють інформаційною правосуб'єктністю, що включає дві юридичні якості: інформаційну правоздатність, яка полягає у можливості мати інформаційні права і обов'язки та інформаційну дієздатність – можливість своїми діями набувати інформаційні права і створювати обов'язки. У залежності від обсягу інформаційних прав та обов'язків можна виділити загальних та спеціальних суб'єктів.

Загальними суб'єктами інформаційно-правових відносин є держава та її органи, крім органів, що володіють спеціальною інформаційною компетенцією; фізичні особи та юридичні особи, для яких інформаційна діяльність не є основним видом діяльності. Варто підкреслити, що саме держава є одним із найважливіших суб'єктів інформаційно-правових відносин так як вона здійснює правове регулювання інформаційної сфери, визначає засади інформаційної політики, вживає заходи щодо розвитку національного інформаційного простору, бере участь в міжнародному інформаційному обміні, забезпечує інформаційну безпеку. Інформаційна діяльність держави проявляється у публічно-політичній сфері, де інформаційні зв'язки та комунікації відіграють ключову роль.

До кола спеціальних суб'єктів інформаційно-правових відносин належать юридичні особи, установчими документами яких передбачено інформаційну діяльність як основну: інформаційні агентства, друковані засоби масової інформації, видавництва, телерадіокомпанії, провайдери Інтернет, бібліотеки, архіви тощо, а також державні органи, для яких нормативно-правовими актами встановлено виконання управлінських, регулятивних чи інших функцій в інформаційній сфері[1].

На нашу думку, саме цю класифікацію слід взяти за основу при подальшому формуванні концепції суб'єктного складу учасників відносин, пов'язаних із правовим регулюванням доступу до публічної інформації у мереж Інтернет.

[1] Яременко О. І. Інформаційні відносини як предмет правового регулювання: теоретичний аспект / О. І. Яременко // Вісн. Хмельниц. ін-ту регіон. упр. та права. – 2014. – №1–2. – С. 156–161.

Так, Закон України «Про доступ до публічної інформації» хоча і називає надзвичайно широкий перелік суб'єктів у сфері доступу до публічної інформації, про те він не враховує специфіки суб'єктного складу цих відносин, опосередкованих обміном інформації через мережу Інтернет.

Так, положення вказаного нормативного документу доцільно доповнити рядом додаткових суб'єктів, таких як: 1) користувачі; 2) оператори зв'язку; 3) сервіс-провайдери, які забезпечують доступ до Мережі; хост-провайдери, що мають надавати за плату дисковий простір на своєму сервері клієнтам, а також інші базові послуги Інтернету.

Всі ці суб'єкти, через технічні особливості та нюанси поширення відомостей, які є публічною інформацією, мають всі технічні можливості для її збирання та накопичення. Саме через це, їх права та обов'язки також мають бути визначені чинним законодавством України. Це дозволить убезпечити публічну інформацію від її незаконного збирання, накопичення та подальшого використання з метою, яка протирічить стратегічним інтересам нашої держави та суспільства.

Засоби захисту прав володільців публічної інформації у формі відкритих даних у мережі Інтернет

В юридичній науці прийнято розділяти всі існуючі можливості захисту будь-якої інформації в мережі Інтернет на дві групи. До першої із них прийнято відносити технічні засоби захисту такої інформації від самовільного копіювання і виділяти правове регулювання, яке пов'язане із таким захистом. До другої групи прийнято відносити правові гарантії володільців інформації, яка хоча і поширюється мережею Інтернет із їх дозволу проте на їх вимогу може бути обмежена для використання певною категорією суб'єктів (користувачів) чи її правові умови поширення не передбачатимуть можливості вільного подальшого її поширення.

Так, до першої групи умовно названих «технічних засобів» захисту, прийнято відносити наступні прийоми та технологічні засоби захисту:

Шифрування інформації. Шифрування використовується для автентифікації і збереження таємниці. Шифрування – метод пере-

творення первісних даних у закодовану форму. Криптографічні технології (методи захисту даних з використанням шифрування) забезпечують три основних типи послуг для електронної комерції: автентифікацію, неможливість відмови від здійсненого, збереження таємниці. Автентифікація – метод перевірки не тільки особистості відправника, а й наявності чи відсутності змін у повідомленні. Реалізація вимоги неможливості відмови полягає в тому, що відправник не може заперечити, що він відправив певний файл (дані), а отримувач – що він його отримав (це схоже на відправлення замовного листа поштою). Збереження таємниці – захист повідомлень від несанкціонованого перегляду.

В основу шифрування покладено два елементи: криптографічний алгоритм і ключ. Криптографічний алгоритм – математична функція, яка комбінує відкритий текст або іншу зрозумілу інформацію з ланцюжком чисел (ключем) з метою отримати незв'язний (шифрований) текст.

Шифрування з ключем має дві переваги:

1. Використовуючи ключ, можна застосовувати той самий алгоритм для відправлення повідомлень різним людям. Головне – закріпити окремий ключ за кожним респондентом.

2. Якщо хтось «зламає» зашифроване повідомлення, щоб продовжити шифрування інформації, достатньо лише змінити ключ. Надійність алгоритму шифрування залежить від довжини ключа.

Симетричне шифрування або шифрування з таємним ключем. Це найдавніша форма шифрування з використанням ключа. Під час шифрування за такою схемою відправник і одержувач володіють одним ключем, з допомогою якого обидва можуть зашифровувати і розшифровувати інформацію.

Однак існують проблеми з автентичністю, оскільки особистість відправника або одержувача повідомлення гарантувати неможливо.

Криптографія з відкритим ключем. Заснована на концепції ключової пари. Кожна половина пари (один ключ) шифрує інформацію так, що її може розшифрувати тільки інша половина (другий ключ). Одна частина ключової пари – особистий ключ – відома тільки її власнику. Інша половина – відкритий ключ – розповсюджується серед усіх його респондентів, але зв'язана тільки з власником. Клю-

чові пари володіють унікальною властивістю: дані, що зашифровані будь-яким з ключів пари, можуть бути розшифровані тільки іншим ключем з цієї пари.

Відкрита частина ключової пари може вільно розповсюджуватися, і це не перешкодить використовувати особистий ключ. Ключі можна використовувати і для забезпечення конфіденційності повідомлення, і для автентифікації його автора.

Дайджест. Незважаючи на назву, дайджест повідомлення не є його стислим викладенням. Існують криптографічні алгоритми для генерації дайджестів повідомлення – однобічні хеш-функції. Однобічна хеш-функція не використовує ключа. Це звичайна формула для перетворення повідомлення будь-якої довжини в один рядок символів (дайджест повідомлення). При використанні 16-байтової хеш-функції оброблений нею текст матиме на виході довжину 16 байтів. Наприклад, повідомлення може бути надане ланцюжком символів VCC349RTУasdf904. Кожне повідомлення формує свій випадковий дайджест. Якщо зашифрувати дайджест особистим ключем, то можна отримати цифровий підпис.

Використання цифрових сертифікатів. Цифровий сертифікат – електронний ідентифікатор, який підтверджує справжність користувача, містить інформацію про нього, слугує електронним підтвердженням відкритих ключів.

Сертифікаційні центри несуть відповідальність за перевірку с особистості користувача, надання цифрових сертифікатів, перевірку їх справжності.

Інші способи захисту інформації:

1. Захист Web-додатків за допомогою S-HTTP і SSL-протоколів.

2. Захист електронної пошти за допомогою стандартів: PEM, S/MINE, PGP.

3. Захист мереж міжмережевими екранами (брандмауери, firewall).

Для захисту комерційної інформації їх поділяють на дві групи: 1) системи на основі пластикових карток; 2) системи на основі цифрових грошей[1].

[1] Безпека і захист інформації в Internet [Електронний ресурс]. – Режим доступу: http://www.ukr.vipreshebnik.ru/2012-06-25-182109/1540--internet.html.

Існують також додаткові, альтернативні класифікації технічних засобів захисту інформації в мережі Інтернет. Так, С. С. Трач, пропонує наступний перелік засобів захисту інформації в мережі Інтернет:

Адміністративні (організаційні) – це заходи, що регламентують процес функціонування системи, використання її ресурсів, діяльність персоналу тощо. До них відносяться :

1) розробка правил обробки інформації;

2) проектування будівель для обробки інформації з урахування впливу зовнішнього середовища;

3) відбір персоналу;

4) організація пропускної системи, організація обліку;

5) зберігання і знищення документів та носіїв конфіденційної інформації;

6) організація розподілу зберігання паролів, криптографічних ключів;

7) сертифікація технічних і програмних засобів.

Фізичні заходи захисту включають охорону приміщень, техніки та персоналу, встановлення на дверях приміщень шифрувальних замків тощо.

Технічні засоби передбачають використання пристроїв, які зменшують ймовірність руйнування та викрадання інформації. Серед найбільш відомих технічних засобів можна назвати: блоки безперебійного живлення (UPS), які дозволяють працювати на ЕОМ деякий час після виключення електричного струму; ключі запирання клавіатури; спеціальні комп'ютери разом із специфічним програмним забезпеченням (брандмауери), які обмежують або фільтрують доступ до інформаційної системи із глобальних мереж; електронні картки.

Програмні засоби використовуються для :

– визначення та обмеження прав користувачів по доступу до системи;

– шифрування та розшифровки інформації, що зберігається;

– фіксування дій користувачів по доступу до системи або інформації;

– відновлення знищеної інформації на носіях, якщо знищення відбулось на логічному, а не фізичному рівні тощо.

Подібні програми можуть входити у стандартний комплект поставки того чи іншого програмного продукту загального призначення,

або розроблятися під конкретне робоче місце проектувальниками інформаційних систем.

Технологічні засоби передбачають включення у технологічний процес спеціальних операцій, які будуть перешкоджати та запобігати пошкодженню, руйнуванню та витоку інформації.

Такі засоби повинні надавати можливість відновити інформацію і програмні засоби з мінімальними витратами часу і праці. Технологічні засоби тісно пов'язані із програмними. Більшість технологічних операцій по захисту інформації вимагають роботи спеціальних програм.

3. Технологія захисту інформації при роботі у мережі.

Види ризиків при роботі у мережі.

1) з погляду прийнятої користувачем політики безпеки, можуть бути ризики пов'язані з конфігурацією системи.

2) ризики, що виникають у наслідок помилок у програмному забезпеченні залежать від:

– міри відкритості системи.

– наявності помилок у операційній системі

– швидкості їх виправлення.

Засоби захисту інформаційних ресурсів:

1. Перевірка системних установок (або її незмінність з часу останньої перевірки здійснюється за допомогою програм класу «сканер безпеки». Такі програмні продукти існують для більшості ОС. До них відносяться :

– ASET (компонент ОС Solaris),

– KSA (для платформ NetWare и NT),

– SSS (System Security Scanner) (Unix-платформы).

Ці програми аналізують стан безпеки, що виникає як зовні (у цьому випадку тестування проводиться по глобальній мережі з використання спеціальної програми (наприклад Internet Scanner, що входить до складу System Security Scanner), так і усередині мережі (у цьому випадку тестування проводиться з самої ОС комп'ютера).

Здійснюється: перевірка прав доступу; перевірка прав власності файлів; конфігурація мережевих сервісів; перевіряються програми аутентифікации, (наприклад, паролі); перевіряється поточна конфігурація (до неї відноситься файли конфігурації, версії ПЗ, незвичайні файли перевірка небезпечних змін у системі).

2. Перевірка небезпечних змін у системі (перевіряються сліди несанкціонованого доступу до системи: (програма S3):

1) зміна розмірів файлів;

2) зміна прав доступу до файлів;

3) зміна змісту окремих файлів;

4) зміна в установках ресурсів користувача;

5) переключення мережевого інтерфейсу в режими робота, що дозволяють передавати дані на зовнішні комп'ютери.

За результатами сканування створюється звіт.

3. Ааналіз захисту мережевих сервісів.

Прикладом таких засобів захисту є:

1. Пакет програм SATAN, автор F. Venema програма розповсюджується безкоштовно. До складу системи входять більш ніж 20 тестів для перевірки вразливості системи.

2. Пакет Internet Scanner SAFEsuite. Цей пакет надає можливість ідентифікувати та корегувати більш ніж 140 відомих вразливих місць та постійно спостерігати за станом безпеки мережевих технічних засобів, що працюють з TCP/IP.

Пакет складається з трьох програм:

Web Security Scanner, призначена для пошуку слабких місць на web-серверах. Програма забезпечує: аудит ОС ,проводить тестування конфігурації сервера, проводить оцінку файлової системи, створює звіт з рекомендаціями по підвищенню рівня безпеки.

Firewall Scanner, проводить пошук слабких місць в межмережевих екранах.

Intranet Scanner, призначена для пошуку слабких місць усередині мережі. Забезпечує перевірку різних мережевих пристроїв : UNIX hosts, систем, що працюють під Microsoft NT/Windows 95, маршрутизаторів, web-серверів.

4) засоби автоматичного реагування на спроби НСД.

Прикладом такого засобу є продукт RealSecure компании Internet Security Systems (США).

Цей інструментальний засіб призначений для адміністративного управління великими обсягами мережевої інформації:

1) відслідковує події, що порушують безпеку системи цілодобово;

2) реєструє спроби НСД;

3) організовує комплекс активних засобів захисту.

Пакет працює під ОС SunOS, Solaris и Linux.

З метою захисту інформації, що передається по мережі необхідного забезпечити виконання наступних вимог:

1. Інформація, що передається по мережі повинна бути закритою, тобто повідомлення може бути прочитане тільки тим, кому воно адресоване;

2. Цілісність, випадкове чи навмисне пошкодження повідомлення повинно бути виявлене при його прийомі;

3. Необхідно встановлювати аудентичність відправника (при прийомі повідомлення одночасно виявляти хто його відправив);

Для захисту електронних повідомлень використовуються криптографічні методи захисту інформації. Засоби криптографічного захисту можуть бути з одним ключем для шифрування та дешифрування та з різними ключами.

При використанні одного ключа виникає проблема передачі кореспонденту копії ключа. У другому випадку такою проблеми не виникає.

Прикладом системи з двома ключами є розроблена Филипом Циммерманном програма Pretty Good Privacy (PGP) . Один ключ привселюдний, а інший секретний. Це означає, що можна повідомляти свій привселюдний ключ , при цьому користувачі програми зможуть відправляти зашифровані повідомлення іншим користувачам, і ніхто, крім адресата не зможе розшифрувати повідомлення. Розшифрування повідомлення здійснюється за допомогою іншого, секретного ключа, що тримається в таємниці.

Вважається, що розшифровка повідомлення може тривати на протязі століття.

Програма PGP широко доступна у мережі. У зв'язку з обмеженнями на експорт криптографічної продукції, що діють у США, резиденти і нерезиденти США повинні використовувати різні місця для завантаження програми[1].

[1] Трач С. С. Безпека інформації при електронній комерції [Електронний ресурс] / С. С. Трач. – Режим доступу: http://lubbook.org/book_491_glava_1_Bezpeka%C2%A0_%D1%96nforma%D1%81%D1%96%D1%97_pri_e.html.

До другої групи умовно названих «індивідуальних засобів захисту», прийнято відносити наступні прийоми та правові механізми, які можуть бути використані володільцем публічних даних для захисту своїх прав і законних інтересів:

Конституція України містить Розділ ІІ «Права, свободи та обов'язки людини і громадянина», який увібрав у себе всі основні положення міжнародно-правових актів з прав людини. Проте, немає жодного посилання на онлайнові права чи на рівний захист прав людини в онлайновому середовищі[1]. Стаття 8 Конституції України гарантує звернення до суду для захисту конституційних прав та свобод людини і громадянина безпосередньо на підставі Конституції України.

У Конституції України закріплюється право особи звертатися за захистом своїх прав до Уповноваженого Верховної Ради України з прав людини (стаття 55) і визначається, що через нього здійснюється парламентський контроль за додержанням конституційних прав і свобод людини і громадянина (стаття 101). Статус, функції та компетенція Уповноваженого Верховної Ради України з прав людини закріплені у Законі України «Про Уповноваженого Верховної Ради України з прав людини»[2].

Стаття 13 Закону передбачає, що Уповноважений має право з метою захисту прав і свобод людини звертатися до суду про захист прав і свобод осіб, які через фізичний стан, недосягнення повноліття, похилий вік, недієздатність або обмежену дієздатність неспроможні самостійно захистити свої права і свободи; брати участь у судовому розгляді справ, провадження в яких відкрито за його позовами (заявами, клопотаннями (поданнями); вступати у справи, провадження в яких відкрито за позовами (заявами, клопотаннями (поданнями) інших осіб, на будь-якій стадії їх судового розгляду; ініціювати незалежно від його участі у судовому провадженні перегляд судових рішень. До суттєвих функцій Уповноваженого належить також прове-

[1] Конституція України : Закон України від 28.06.1996 № 254к/96-ВР // Відом. Верхов. Ради України. – №30. – Ст. 141.

[2] Про Уповноваженого Верховної Ради України з прав людини : Закон України від 23 груд. 1997 р. №776/97-ВР // Відом. Верхов. Ради України. – 1998. – №20. – Ст. 99.

дення моніторингу за дотриманням та захистом прав і свобод людини і громадянина в Україні органами державної влади, місцевого самоврядування, об'єднаннями громадян, підприємствами, установами, організаціями незалежно від форми власності та їх посадовими та службовими особами, які своїми діями (бездіяльністю) порушували права і свободи людини і громадянина.

Результати таких моніторингів та комплексна оцінка стану додержання та захисту прав і свобод людини і громадянина в Україні презентуються у Верховній Раді України у вигляді щорічних доповідей про стан дотримання та захисту прав та свобод людини і громадянина в Україні.

Слід також зазначити, що стан дотримання прав людини онлайн не покривається моніторинговими механізмами Уповноваженого. Інформація щодо порушення прав людини в мережі Інтернет та при користуванні засобами телекомунікацій в Уповноваженого з прав людини відсутня. У зв'язку з обмеженим фінансуванням освітні заходи у сфері захисту прав людини Секретаріат Уповноваженого реалізує лише у співпраці з інститутами громадянського суспільства та міжнародними організаціями у формі участі представників Секретаріату Уповноваженого в якості доповідачів або тренерів на семінарах, тренінгах, конференціях тощо[1].

Відповідно до статті 22 Закону України «Про захист персональних даних»[2] на Секретаріат Уповноваженого Верховної Ради України з прав людини покладено функції контролю за додержанням законодавства про захист персональних даних. Проте, відсутність належного матеріально-технічного забезпечення діяльності Уповноваженого та його Секретаріату обмежує можливості щодо здійснення оперативної перевірки і реагування на порушення прав людини у зв'язку з відсутністю регіональних представництв[3].

[1] Правові засоби захисту та відновлення прав користувачів Інтернету в Україні в контексті застосування Посібника Ради Європи з прав людини для інтернет-користувачів / за ред. А. В. Пазюка. – Київ : ФОП Клименко, 2015. – 128 с.

[2] Про захист персональних даних : Закон України від 1 черв. 2010 р. № 2297-VI // Відом. Верхов. Ради України. – 2010. – № 34. – Ст. 481.

[3] Правові засоби захисту та відновлення прав користувачів Інтернету в Україні в контексті застосування Посібника Ради Європи з прав людини для інтернет-користувачів / за ред. А. В. Пазюка. – Київ : ФОП Клименко, 2015. – 128 с.

Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації є державним колегіальним органом, підпорядкованим Президенту України та підзвітним Верховній Раді України. Створена у 2011 році Указом Президента України на виконання Закону України «Про телекомунікації», НКРЗІ є органом державного регулювання у сфері телекомунікацій, інформатизації, користування радіочастотним ресурсом та надання послуг поштового зв'язку.

У визначеній сфері НКРЗІ здійснює повноваження органу ліцензування, дозвільного органу, регуляторного органу та органу державного нагляду (контролю). НКРЗІ здійснює державний нагляд (контроль) за додержанням законодавства про радіочастотний ресурс України та запобігання правопорушенням при користуванні радіочастотним ресурсом України у смугах радіочастот загального користування. НКРЗІ також є одним із державних органів, що втілює концепцію запровадження в Україні інформаційного суспільства.

У контексті захисту прав людини та прав споживачів в НКРЗІ функціонує Відділ по роботі із споживачами та зверненнями громадян, що відповідає за забезпечення діяльності НКРЗІ щодо захисту прав споживачів. За даними НКРЗІ, отриманими на запит про надання публічної інформації, на розгляд цього Відділу надійшло звернень споживачів у 2013 році – 2340; у 2014 році – 2508, з яких скарги на доступ до Інтернету становили 128 (5,47%) і 111 (4,43%) відповідно. Аналіз структури таких звернень свідчить, що більшість з них стосуються технічних аспектів обслуговування, а саме: неякісного надання послуг, а також порушень при розміщенні інформації в мережі Інтернет, блокування інформаційних ресурсів у мережі Інтернет, незгоди з розміром виставлених рахунків, тарифів, тривалої відсутності доступу під час ремонту. Крім того, було повідомлено, що питання щодо «покращення обізнаності користувачів Інтернету стосовно прав людини не належать до повноважень НКРЗІ.

Відповідно до статті 55 Конституції України кожен має право після використання всіх національних засобів правового захисту звернутися за захистом своїх прав і свобод до відповідних міжнародних судових установ чи до відповідних органів міжнародних організацій, членом чи учасницею яких є Україна.

Кіберзлочинність порушує на право приватне життя, свободу вираження та інші основоположні свободи, так само як й негативно впливає на суспільну значущість Інтернету. Україна як й інші країни-учасниці Ради Європи має позитивне зобов'язання та відповідальність захистити індивідів від злочинності онлайн, так само як оффлайн та забезпечити законність в Інтернеті.

Україна є учасником Конвенції про кіберзлочинність (ратифікувала 07.09.2005 р. та набрала чинності 01.07.2006 р.), а також Додаткового протоколу до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи (ратифікувала 21.07.2006 р. та набрав чинності для України 01.04.2007 р.).

Уповноваженим органом з розслідування кіберзлочинів є Міністерство внутрішніх справ України (Управління боротьби з кіберзлочинністю), нагляд за діяльністю співробітників якого здійснює Генеральна прокуратура України.

За відомостями, наданими Генеральною прокуратурою України, з Єдиного реєстру досудових розслідувань у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку у 2014 році було обліковано 443 кримінальних правопорушень. Передано до суду з обвинувальним вироком – 201, тобто 45%[1].

Крім всіх названих інституційних засобів захисту даних в мережі Інтернет, особливе місце займає Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»[2]. Так, відповідно до положень цього нормативно-правового документу, тільки власником інформації встановлюється правовий режим її використання у будь-яких телекомунікаційних системах, в тому числі і в мережі Інтернет (ст. 4). При цьому, таке право власника інформації не є виключним та може бути обмежене у порядку встановленому чинним законодавством

[1] Правові засоби захисту та відновлення прав користувачів Інтернету в Україні в контексті застосування Посібника Ради Європи з прав людини для інтернет-користувачів / за ред. А. В. Пазюка. – Київ : ФОП Клименко, 2015. – 128 с.

[2] Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 5 лип. 1994 р. №80/94-ВР // Відом. Верхов. Ради України. – 1994. – №31. – Ст. 286.

України. А саме це обмеження має бути визначено виключно нормативно-правовим актом не нижче рівня Закону України.

Цим же документом визначено обов'язок будь-якого учасника відносин, пов'язаного із поширенням інформації в мережі Інтернет, за першою вимогою власника інформації обмежити чи припинити доступ всіх інших користувачів до інформації, що розповсюджується не у спосіб, який визначений її власником та/або володільцем.

Всіх цих засобів недостатньо для забезпечення належного рівня захисту публічної інформації. Особливо у випадках, коли відомості про фізичну особу чи її персональні дані, стають публічною інформацією. Це може відбуватись тоді, коли така особа набула правового статусу державного службовця, чи, наприклад стала власником будь-якого нерухомого майна.

Чинне законодавство України, на сьогоднішній день, не передбачає жодного правового механізму, який би міг за наявності будь-яких спеціальних підстав обмежити чи припинити доступ до публічної інформації в мережі Інтернет, яка стосується фізичної особи.

На нашу думку, такий правовий механізм обов'язково має бути імплементований в національну правову систему та має виглядати наступним чином:

1. Має бути обмежено коло інформації, яка є публічними даними і доступ до якої має бути обмежений чи припинений. Так, такою інформацією можуть виступати лише відомості про особу, її персональні дані та інформація про її фінансовий, майновий стан чи структуру належного їй майна. До таких відомостей не можуть бути віднесені всі інші відомості, які є публічною інформацією.

2. Має бути визначено коло користувачів, для яких доступ до такої інформації має бути обмежено. При цьому, у правоохоронних органів доступ до такої інформації має залишитися.

3. Має бути визначено чіткий перелік підстав для прийняття рішення про обмеження чи припинення вільного доступу користувачів до публічної інформації, яка є персональними даними про конкретну особу. Наприклад такими підставами можуть бути: (а) загроза життю чи здоров'ю фізичної особи; (б) наявність стратегічної зацікавленості у держави до діяльності такої особи, через що, вона вимушена

вживати засобів персонального захисту такої особи; (в) інші підстави, які надають можливість проігнорувати публічні інтереси суспільства на користь особистої безпеки конкретної особи та/або стратегічних інтересів держави.

4. Має бути визначено процедуру прийняття рішення про обмеження чи припинення вільного доступу користувачів до публічної інформації про фізичну особу. Найбільш доцільним є покладення цього обов'язку на судову гілку влади, а саме на систему адміністративних судів в порядку позовного провадження.

Використання такої системи захисту при неухильному дотриманні всіх визначених критеріїв та принципів, дозволить дотриматись дієвого пріоритету між особистими немайновими правами, пов'язаними із захистом персональних даних, та публічним інтересом громадянського суспільства до використання такої інформації для контролю за діяльністю органів державної влади та місцевого самоврядування.

НАЦІОНАЛЬНА АКАДЕМІЯ ПРАВОВИХ НАУК УКРАЇНИ

НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ
ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІННОВАЦІЙНОГО РОЗВИТКУ

ПРАВОВЕ РЕГУЛЮВАННЯ ВІДНОСИН У МЕРЕЖІ ІНТЕРНЕТ

Монографія

За редакцією
С. В. Глібка, К. В. Єфремової

Харків
«Право»
2016

УДК 346.7:004.77
ББК 67.9(4УКР)303+65.2/4
П68

Рекомендовано до друку вченою радою
Науково-дослідного інституту правового забезпечення
інноваційного розвитку Національної академії правових наук України
(протокол № 10 від 17.11.2016 р.)

Рецензенти:

С. М. Прилипко, доктор юридичних наук, професор, академік НАПрН України, професор кафедри трудового права Національного юридичного університету імені Ярослава Мудрого;

В. Л. Яроцький, доктор юридичних наук, професор, член-кореспондент НАПрН України, завідувач кафедри цивільного права № 2 Національного юридичного університету імені Ярослава Мудрого

Колектив авторів:

Д. І. Адамюк – підрозд. 2.3 розд. II; *Ю. Є. Атаманова* – підрозд. 3.1 розд. III; *Д. В. Бойко* – підрозд. 2.2 розд. II; *О. В. Бринцев* – підрозд. 4.3 розд. IV; *А. П. Гетьман* – підрозд. 1.1 розд. I (у співавт. із К. В. Єфремовою); *С. В. Глібко* – вступ (у співавт. із К. В. Єфремовою), підрозд. 2.5 розд. II; *О. А. Гончаренко* – підрозд. 3.5 розд. III; *О. М. Давидюк* – підрозд. 3.3 розд. III; *К. В. Єфремова* – вступ (у співавт. із С. В. Глібком), підрозд. 1.1 розд. I (у співавт. із А. П. Гетьманом); підрозділи 1.2, 1.3 розд. I; *Ю. М. Жорнокуй* – підрозд. 3.4 розд. III; *К. Ю. Іванова* – підрозд. 2.4 розд. II; *В. С. Мілаш* – підрозд. 2.1 розд. II; *О. О. Осадько* – підрозд. 3.2 розд. III; *І. Є. Погребняк* – підрозд. 4.2 розд. IV; *І. А. Спасибо* – підрозд. 4.1 розд. IV; *А. В. Стріжкова* – підрозд. 4.4 розд. IV

Правове регулювання відносин у мережі Інтернет : монографія / П68 [А. П. Гетьман, Ю. Є. Атаманова, В. С. Мілаш та ін.] ; за ред. С. В. Глібка, К. В. Єфремової. – Харків : Право, 2016. – 360 с.

ISBN 978-966-937-090-7

Монографію присвячено дослідженню положень чинного законодавства України і права ЄС, що регулюють суспільні відносини, які виникають при організації і користуванні мережею Інтернет, виявлено особливості здійснення правочинів і правового статусу суб'єктів таких відносин, а також співвідношення приватних і публічних інтересів у них з метою визначення оптимальних правових механізмів забезпечення та захисту.

Монографія розрахована на науковців, викладачів, докторантів, аспірантів, студентів юридичних вищих навчальних закладів, спеціалістів у сфері інформаційних технологій, а також усіх тих, хто цікавиться проблемами розвитку відносин у мережі Інтернет.

УДК 346.7:004.77
ББК 67.9(4УКР)303+65.2/4

ISBN 978-966-937-090-7

Зміст

IV. РОЗВИТОК ПРАВОВОГО РЕГУЛЮВАННЯ ВІДНОСИН В ІНТЕРНЕТ: ВИКЛИКИ ТА ТЕНДЕНЦІЇ