СЕРЬОГІН В.О.,
кандидат юридичних наук, доцент
(Харківський національний університет внутрішніх справ)

УДК 342.72

КІБЕРПРОСТІР ЯК СФЕРА ЗАХИСТУ ПРАЙВЕСІ

Досліджено сучасну проблематику охорони недоторканності приватного життя у кіберпросторі. Звернено увагу на зарубіжне та вітчизняне законодавство у даній сфері. Запропоновано принципові підходи до нормативного забезпечення даного права в умовах динамічного розвитку комп'ютерних технологій та електронних мереж.

Ключові слова: *права людини, прайвесі, недоторканність приватного життя, кіберпростір, Інтернет.*

Исследуется современная проблематика охраны неприкосновенности частной жизни в киберпространстве. Обращается внимание на зарубежное и отечественное законодательство в данной сфере. Предлагаются принципиальные подходы к нормативному обеспечению данного права в условиях динамичного развития компьютерных технологий и электронных сетей.

Ключевые слова: *права человека, прайвеси, неприкосновенность частной жизни, киберпространство, Интернет.*

The article deals with contemporary issues of protection of privacy in cyberspace. Attention is paid to foreign and domestic legislation in this area. Offered basic approaches to the regulatory provision of the law in the context of the dynamic development of computer technologies and electronic networks.

Key words: *human rights, privacy, inviolability of private life, cyberspace, Internet.*

На сьогодні Інтернет досить глибоко увійшов у ділове й повсякденне життя. Наше приватне життя й наша професійна діяльність поступово стають міцно пов'язаними із всесвітньою мережею. Пересічні громадяни починають створювати у мережі власні веб-сайти та вебсторінки; мережа Інтернет сприяє більш енергійному просуванню товарів та послуг, і цим успішно користуються бізнесмени. З іншого боку, новітні інформаційні технології стають важливою складовою публічного життя. Так, електронний уряд (англ. E-Government) стає неодмінною ознакою транспарентної, плюралістичної демократії. Крім того, Інтернет стає ареною діяльності правоохоронних органів й ефективним способом протидії тероризму, наркотрафіку, незаконній торгівлі зброєю тощо.

На жаль, вітчизняна юридична наука поки що відстає від потреб сьогодення, зумовлених бурхливим розвитком комп'ютерних технологій та електронних мереж. Тим більш це стосується дослідження проблем, які постають у цьому зв'язку перед суспільством у сфері забезпечення прав людини, у т.ч. щодо забезпечення недоторканності приватного життя (прайвесі). У публікаціях з даної проблематики, опублікованих у країнах СНД, серед яких слід відзначити дослідження В.І. Бобрика, Н.С. Мамедова, І.Л. Петрухіна, Г.Б. Романовського, Ф.М. Рудинського, В.С. Сивухіна, Р.Б. Тополевського та ін., здебільшого йдеться про „традиційні" загрози приватності (незаконне прослуховування, незаконне збирання та поширення персональних даних тощо), тоді як новітні виклики, у т.ч. й у кіберпросторі, залишаються поза межами уваги. Означені фактори зумовлюють актуальність теми нашого дослідження, його теоретичну і практичну значущість.

Метою даної статті є загальна характеристика кіберпростору як нової реальності, що потребує правового впливу, аналіз основних загроз недоторканності приватного життя (прайвесі), існуючих у даній сфері, а також з'ясування шляхів протидії цим загрозам з урахуванням наявних юридичних та матеріально-технічних можливостей.

Розпочинаючи наше дослідження, слід відзначити, що поняття кіберпростору (англ. cyberspace) – метафорична абстракція, що використовується у філософії та комп'ютерних науках; це певний світ як „всередині" комп'ютерів, так і „всередині" комп'ютерних мереж. Кіберпростір є віртуальною реальністю, що представляє Ноосферу. Слово „кіберпростір" (від „кібернетика" і „простір") уперше було запроваджено В. Гібсоном, канадським письменником-фантастом, у 1982 р. у його новелі „Спалення Хрома". Згодом, у 1984 р., воно було популяризоване в ще одному творі В. Гібсона – романі „Нейромант".

Як і фізичний простір, кіберпростір включає об'єкти (файли, поштові повідомлення, графіки тощо) та різноманітні режими їхнього транспортування й доставки. На відміну від реального простору, дослідження кіберпростору не вимагає фізичного руху, крім натискання клавіш на клавіатурі чи пересування „миші". Водночас кіберпростір не слід плутати з реальним Інтернетом. Цей термін часто вживається для описання об'єктів, поширених у комп'ютерній мережі; наприклад, веб-сайт може бути метафорично описаний як такий, що „перебуває у кіберпросторі". Використовуючи таку інтерпретацію, можна сказати, що Інтернет-події не відбуваються у країнах чи містах, в яких фізично перебувають сервери чи учасники, а відбуваються у кіберпросторі. Це стане раціональним поглядом на речі в той момент, коли розподілені сервіси стануть широко використовуватися, коли особа і місцезнаходження учасників мережі буде неможливо визначити через анонімний чи псевдоанонімний зв'язок. Застосовувати закони кожної держави у кіберпросторі стане неможливо.

Кіберпростір можна охарактеризувати як абсолютно нову культурну цілісність, у межах якої певні соціальні, політичні та економічні структури тільки починають розвиватися. У даному контексті прайвесі є засобом як підтримання індивідуальності особи, так і розбудови міжабонентських стосунків. Чим більше цей культурний простір буде оформлюватися, стане дедалі більш необхідним визначити права тих, хто проживає в його межах та охороняти ці права відповідними приписами.

Слід мати на увазі, що кожне досягнення в галузі комп'ютерної індустрії та електронних технологій має дві сторони: з одного боку, вони суттєво збільшують можливості людини, суспільства і держави у задоволенні їхніх потреб, а з іншого – можуть бути використані на шкоду їм.

Тому кіберпростір слід розглядати не просто як технологічну новацію, що полегшує зв'язок, але й як сферу культури, що характеризується специфічними формами соціальної організації та правилами взаємодії. Унікальна соціальна й геополітична структура електронного довкілля свідчить проти традиційних уявлень про сутність приватності й вимагає розробки нових підходів до права на прайвесі, які б обмежували спроможність інших здійснювати зовнішнє спостереження та здійснювати збір персональної інформації.

Веб-сайти збирають дані про відвідувачів. Он-лайнова бібліотека не працює як слід без включених файлів cookies. Інтернет-магазин пропонує заповнити анкету – без цього неможливо зробити замовлення. Популярний форум вимагає реєстрації, інакше ви не зможете відправити туди ваше повідомлення. Інформація про Інтернет-користувачів збирається, обробляється, зберігається, і частіш за все ніхто не несе ні за що ані найменшої відповідальності. Буває, що користувач навіть не підозрює, що на нього складено відповідне електронне „досьє".

Як справедливо зазначає К. С. Байфорд, нерегульований збір комерційних даних породжує відчуження, оскільки позбавляє особу контролю над доступом до власної персональної інформації [1, с. 1-2]. Неврегульованість також дозволяє тим, хто збирає таку інформацію, накопичувати соціальну владу за рахунок особи; такий процес у кінцевому рахунку може унеможливити подальший розвиток демократії в кіберпросторі.

Як цілком обґрунтовано стверджують експерти, існуючі інструкції, адресовані на забезпечення прайвесі в контексті електронних комунікацій, неадекватні існуючим у цій сфері загрозам. Регулятивна структура має розвиватися поступово, або покладаючись на саморегуляцію з боку елементів мережі, або дозволяючи створити гарантії прайвесі через договірні засоби. Жодна альтернатива не визнає відмінності між владою індивідуальних користувачів та інформаційних провайдерів. До того ж жодна альтернатива не надає ефективних засобів для створення однорідного й послідовного підходу до прайвесі у кіберпросторі.

Мало того, що приватні особи підпорядковані урядам, що контролюють їхні вчинки, вони також стикаються зі стеженням за собою у приватному секторі з боку корпорацій, котрі в такий спосіб випробовують свої тактики маркетингу, і навіть з боку інших користувачів Інтернету. Сьогодні, в нашому залежному від технологій житті, усі ми багато чого робимо або в режимі он-лайн, або по телефону чи за допомогою інших електронних приладів, і в такий спосіб ставимо себе під контроль і стеження. Справді, кожен електронний лист чи бесіда, яку ми ведемо он-лайн чи по телефонній лінії, можуть бути переведені у форму, придатну для читання чи прослуховування будь-ким. „Технологічний прогрес, надавши чимало суттєвих переваг, – відзначає Дж. Тех, – водночас значною мірою позбавив нас нашої приватності, руйнуючи відмінність між приватними і суспільними

справами, змушуючи жити у „скляних" будинках, аби нас бачив увесь світ" [2, с. 7].

Слід визнати, що Інтернет повністю перетворив і поліпшив наше життя за рахунок прайвесі. Інтернет-технології спроможні повністю знищити наше прайвесі, створюючи оруеллівське суспільство, в якому приватність є застарілим поняттям. Такі можливості яскраво виявляються у тих випадках, коли технологічні та прибуткові аспекти використання кіберпростору в бізнесових цілях закінчувалися шкідливими наслідками для прайвесі-споживачів. Недарма доволі поширеним серед дослідників став вислів: „Інтернет є вбивцею прайвесі".

Дійсно, невдача запропонованих механізмів захисту прайвесі у кіберпросторі призвела до того, що наша можливість контролювати інформацію, що поширюється про нас безпосередньо, скоро стане повною фікцією. Втрата спроможності керувати інформацією про себе матиме страшні наслідки як для пересічних громадян, так і для суспільства в цілому. Наприклад, це може спричинити так звану „втрату індивідуальності", оскільки ми намагаємося висунути на загальний огляд тільки те, що дає нам змогу бути соціально прийнятними, показуючи тільки наші публічні обличчя, ніби ми є акторами на сцені щохвилини нашого життя. Це скінчилося б створенням суспільства, в якому кожна людина позбавлена індивідуальності й особливої унікальності, суспільства, в якому кожна особа є точним віддзеркаленням іншої.

„Ерозія" прайвесі має негативні наслідки не тільки для творчого потенціалу, індивідуальності й унікальності особи, але й для засад розвитку демократії, соціального й технічного прогресу. Суспільство, в якому не існує приватності, скінчилося б побоюванням громадян стикнутися з критикою, соціальними санкціями чи упередженістю з боку оточуючих у випадку невідповідності уявленням, що поділяються іншими. Самоцензура врешті-решт призводить до згортання свободи думки, слова і волевиявлення, а відмова від експериментування через побоювання постати перед іншими в негативному світлі перешкоджає формуванню нових ідей та винаходів.

Через невдачу саморегулювання та суто технологічних рішень всебічне законодавство має захистити інтереси осіб, аби зберегти їхнє право на прайвесі у кіберпросторі, оскільки цьому фундаментальному праву має бути надано пріоритет перед правами тих, хто прагне втрутитися у їхнє приватне життя. За словами Дж. Радванські, Спеціального уповноваженого Канади з питань прайвесі, поняття дозволу, вибору і згоди є критичними у цій новій „культурі прайвесі", що спирається на широке визнання того, що наша особиста приватність перебуває зараз під такою загрозою, як ніколи раніше [3].

При цьому надання згоди на основі повної інформації вимагає обізнаності особи про збирання, використання і поширення відповідної інформації, їх наслідки та існування доступних альтернатив. Свобода вибору є критичною щодо прайвесі. Наявні випадки інформаційної асиметрії, котрі існують між споживачами та організаціями, що збирають персональні дані, вимагають розробки і прийняття законодавства, яке б чітко встановлювало вимогу щодо повної поінформованості та явної згоди клієнта на збирання, використання і поширення його персональних даних.

Звертаючись до сформульованих у сучасній науці визначень прайвесі у кіберпросторі, можна зробити висновок, що переважна більшість авторів зводять його до конкретного прояву інформаційного прайвесі, тобто до права особи контролювати те, яка інформація про неї стає загальнодоступною [2, с. 9-10; 4, с. 3; 5, с. 15-16]. Проте такий підхід видається надто вузьким, оскільки залишає поза увагою декілька важливих аспектів. Зокрема, прайвесі у кіберпросторі – це не тільки можливість особи зберігати певні факти про себе закритими для інших учасників віртуального спілкування; це ще й право бути „залишеним у спокої" у своєму „куточку віртуального світу", аби ніхто не турбував її нав'язливими пропозиціями, не чинив необґрунтованих перепон у задоволенні її потреб за допомогою електронних послуг та не витісняв із кіберпростору. Слід мати на увазі, що новітні технології вже сьогодні надають змогу долучати до „освоєння" кіберпростору всі органи чуттів, адаптуючи віртуальний світ до світу реального у тому вигляді, як його звикла сприймати людина. Відповідно, прайвесі у кіберпросторі – це комплекс усіх аспектів прайвесі (інформаційного, фізичного, комунікативного і навіть територіального), але не в реальному світі, а у віртуальному, породженому електронними технологіями.

У кіберпросторі існує, по суті, три головних джерела інформації про користувачів: персональні комп'ютери (PC), провайдери Інтернет-послуг (ISPs) і веб-сайти [2, с. 18]. У кожному з названих джерел може створюватися й зберігатися чимало байтів персональних даних, про існування яких іноді може бути невідомо навіть самому користувачеві. Так, персональні комп'ютери

зберігають кеш-файли (cash-files), котрі з метою збільшення швидкості підключення заносять в оперативну пам'ять та на жорсткий диск ті дані, що часто використовуються (як-то веб-сторінки та IP-адреси). Відповідно, шукаючи на браузері персонального комп'ютера „історію" і кеш-файли, можна легко встановити, які сайти попередньо відвідувалися, і повернутися до них. До цих кеш-файлів через Мережу можуть звертатися також досвідчені програмісти, зокрема, знайомі з "Java scripts" чи "Java applets" [6, с. 1609].

Коли користувач підключається до мережі Інтернет, його комп'ютер надає серверу Мережі три види інформації про користувача: його ідентичність, конфігурацію комп'ютера і роботу браузера. Ідентичність користувача частково показується через IP-адресу, котру його комп'ютер надає серверу, з яким він бажає увійти у контакт, оскільки взаємний обмін IP-адресами вимагається для зв'язку між двома комп'ютерами. Однак навіть у тому випадку, коли користувач використовує громадський комп'ютер, наприклад, у певній установі чи навчальному закладі, його ідентичність все одно може бути показана, якби він мав увійти на веб-сайт з обмеженим доступом, оскільки він мав би назвати свою ідентичність і пароль, як це вимагається сервером. Далі, комп'ютер також розкриває людську мову користувача, яка (у міру поширеності певної мови в Мережі) показує етнічну приналежність користувача [7]. Інформація про конфігурацію комп'ютера користувача, зокрема, про тип його браузера (Netscape Navigator або Internet Explorer), операційну систему (Mac OS або Windows), та платформу апаратних засобів ЕОМ (наприклад, ПК IBM-PC чи Macintosh), також повідомляється серверу.

Нарешті, сервер отримує деталі пошукової діяльності користувача, зокрема час і дату відвідування, бажаний ресурс з єдиного покажчика ресурсів (англ. ***URL*** – Uniform Resource Locator), обсяг і *URL ресурсу, з якого було зроблено запит. Наприклад, коли користувач натискає на лінк, знайдений пошуковою системою, сервер, з яким з'єднується користувач, може встановити, яка пошукова система використана, а також ключові слова, що при цьому використовуються. Крім того, через відповідність* IP-адреси та інформації про ідентичність їхнім відбиткам у часі чи за допомогою „кукі" сервер може проаналізувати характер інформаційного потоку.

Забезпечуючи надання Інтернет-послуг, провайдери здатні обґрунтовано збирати детальну інформацію про своїх клієнтів, котрі добровільно вказують своє ім'я, номер телефону, адресу і номер кредитної картки, аби оформити підписку на отримання відповідних послуг. Крім того, провайдер також долучений до інформації про спосіб пошуку чи активність у кіберпросторі, про яку їхні клієнти навіть не здогадуються, але значно менше хотіли б розкривати. Відповідно, провайдер – це потужне джерело цінної й приватної інформації про споживача, тим більш що записи провайдера можуть використовуватися для того, щоб ідентифікувати користувачів Інтернету, пов'язуючи їхні псевдоніми з їхньою поведінкою он-лайн.

Здатність провайдерів спричинити низку проблем своїм клієнтам за відсутності належних правових механізмів захисту прайвесі яскраво ілюструє справа *McVeigh v. Cohen,* що мала місце у США у 1998 р. [8]. У цій справі абонент одного з найбільших американських провайдерів – America Online – отримав повідомлення від псевдоніма „boysrch" за підписом „Тім" і захотів з'ясувати особу відправника. Пошук за псевдонімом у довіднику провайдера вивів на інформацію про профіль відправника цього повідомлення, в якому містилися відомості, що він є військовослужбовцем ВМС США, проживає у м. Гонолулу (Гаваї), є веселою людиною і займається колекціонуванням зображень молодих дівчат і хлопців. У графі „сімейний стан" була позначка „гей". Оскільки служба гомосексуалістів у ВМС США була законодавчо заборонена, про всі ці дані було повідомлено керівництво ВМС, яке розпочало власне розслідування. Запитувач інформації, котрий навіть не назвав себе представником ВМС США, отримав від провайдера інформацію про те, що абонентом є Тімоті Маковей, а також персональні дані цього абонента, у т.ч. відомості про його судимості та гомосексуальність. У підсумку Тімоті Маковей, який прослужив на підводному човні понад 17 років, був звільнений з ВМФ, хоча й надав до суду докази своєї гетеросексуальності. Згодом було встановлено, що той самий провайдер – America Online – продавав різноманітні дані про абонентів торговельним компаніям [6, с. 1609-1610].

Доктор Кевін О'Хара, співробітник університету Саутгемптона (Великобританія), нещодавно провів опитування серед Інтернет-користувачів, аби більше взнати про вплив на суспільство інформації, котру люди публікують в он-лайні. „Якщо ми розглянемо прайвесі з точки зору закону, то побачимо, що однією з важливих концепцій є раціональне очікування приватності. Оскільки дедалі більше приватної інформації виноситься в он-лайн, раціональні очікування скорочу-

ються", – стверджує дослідник [9]. На думку О'Хари, зростання соціальних мереж розмило кордони того, що можна вважати особистою інформацією, і зробило їх вужчими, ніж це визначено законом. Ми живемо в епоху під назвою „Інтимність 2.0", коли люди діляться в он-лайні надзвичайно конфіденційною інформацією. Коли наші раціональні очікування скорочуються (що й відбувається), наша потреба в юридичному захисті також скорочується.

Судові справи в галузі порушення прайвесі у кіберпросторі були доволі поодинокими до випадку з президентом міжнародної автомобільної федерації (FIA) Максом Мослі у 2008 р. Пан Мослі подав позов до британського таблоїду „News of the World" з приводу публікації відвертих фотографій за його участю, зроблених таємно під час оргії. Він стверджував, що публікація фотографій стала порушенням його права на прайвесі й виграв процес.

Хоча Макс Мослі захистив своє прайвесі, дослідників непокоїть той факт, що ігнорування прайвесі в он-лайні плавно „перетече" в інші сфери суспільного життя. Свідченням того, що цей процес уже розпочався, є нестихаючі дебати з приводу того, чиє порушенням права на прайвесі сканування тіла в аеропортах та засоби відеоспостереження. Нещодавні рішення в галузі безпеки викликали дискусії з питань недоторканності приватного життя, однак якщо постраждає безпека, то постраждає й усе суспільство, тому в процесі регулювання має бути забезпечений розумний баланс між обома вказаними цінностями.

На жаль, законодавче регулювання питань щодо забезпечення прайвесі у кіберпросторі в усьому світі відстає від потреб сучасного інформаційного суспільства. Фактично, кіберпростір залишається terra incognita для сучасного законодавця, незалежно від особливостей правової системи чи рівня політико-правового розвитку.

Навіть у США – країні, що є безумовним лідером у сфері новітніх комп'ютерних технологій, законодавство про захист прайвесі у кіберпросторі на федеральному рівні відсутнє. Лише окремі штати захищають це право на рівні законодавства, зокрема, вимагаючи від Інтернет-провайдерів тримати у таємниці інформацію про своїх клієнтів і розкривати її тільки за згодою самого клієнта. Так, §325 Зводу законів штату Міннесота забороняє Інтернет-провайдерам розкривати персональні дані, у т.ч. фізичну чи електронну адресу клієнта або номер його телефону, дані про те, які сайти він відвідує, або зміст будь-яких користувацьких пристроїв зберігання даних. Водночас передбачається низка випадків, коли інформація має бути розкрита, зокрема: 1) для великого журі (колегії присяжних), 2) для працівника правоохоронного органу штату чи федерації, що діє на підставі закону; 3) згідно з постановою суду. Порушення цього закону тягне за собою накладення штрафу розмірі 500 дол. або обов'язок відшкодувати шкоду та судові витрати [10].

На думку багатьох експертів, законодавство з питань захисту прайвесі має бути розширене, аби бути спроможним забезпечити приватність тих висловлювань і дій, котрі раніше вважалися часткою публічного життя [11, с. 106]. Відставання чинного законодавства від потреб сучасного інформаційного суспільства змусило адміністрацію США розпочати розробку нової політики щодо прайвесі в Інтернеті, що передбачає розробку нових законів і розширення можливостей державних органів із контролю за дотриманням прав користувачів електронних послуг [12].

Принагідно слід звернути увагу на новітній досвід захисту конфіденційності IP-адрес у Швейцарії. Якщо раніше у цій країні користувач, скачавши неліцензійну програму, міг попастися „на гачок" завдяки оперативній роботі приватних фірм, що відстежують IP, то тепер це залишилося в минулому. Верховний суд Швейцарії своєю постановою наклав заборону на подібні дії з боку приватних компаній, що пропонують свої послуги правовласником, визнавши їх такими, що порушують прайвесі користувачів [13]. Підхід швейцарської Феміди виглядає цілком обґрунтованим: не можна захищати одні права людини (у даному випадку – авторські права) шляхом порушення інших прав. Вважаємо, що такий підхід має бути відображений і в новому вітчизняному законодавстві про захист прайвесі.

Приклад конституційного закріплення права на прайвесі у кіберпросторі дає нам Португалія, де регламентація відповідних питань на рівні Основного закону є найбільш докладною і всебічною. Стаття 35 Конституції Португалії проголошує: „1. Усі громадяни мають право знати інформацію про себе, занесену до електронних картотек і реєстрів, та про цілі, для яких вона призначена, причому вони можуть вимагати оновлення інформації та внесення до неї змін без шкоди для положень закону про державну таємницю та судову таємницю. 2. Заборонено доступ до електронних картотек і реєстрів для отримання персональних даних про третіх осіб, якщо тільки це не робиться у винят-

кових випадках, передбачених законом. 3. Інформація не може бути використана для розголошення відомостей, що стосуються філософських чи політичних переконань, партійного чи профспілкового членства, віросповідання або приватного життя, за винятком випадків обробки статистичних даних, що мають анонімний характер. 4. Закон визначає поняття персональних даних для цілей електронної реєстрації, а також баз і банків даних та відповідні умови їхнього створення, доступу до них і використання публічними й приватними організаціями. 5. Забороняється присвоювати громадянам єдиний у національному масштабі номер. 6. Закон визначає режим руху даних через кордони, встановлюючи форми, що забезпечують захист персональних даних, охорона яких перебуває у сфері національних інтересів" [14, с. 529-530].

Водночас слід вказати, що Конституція Португалії є скоріше винятком із загального правила. Переважна більшість чинних на сьогодні конституцій або взагалі обходять увагою питання захисту прайвесі у кіберпросторі (у т.ч. конституції Австралії, Бразилії, Канади, ПАР, Росії, США, України, Франції, ФРН та ін.), або обмежуються вказівкою на те, що кожна особа має право на захист від зловживання її персональними даними (ч. 2 ст. 13 Конституції Швейцарії) [15, с. 471], а порядок інформування про бази даних на осіб, використання таких баз, а також виправлення включеної до них інформації встановлюється законом (ч. 3 ст. 10 Конституції Нідерландів) [16, с. 478]. Таке становище можна вважати цілком закономірним, якщо взяти до уваги, що переважна більшість чинних конституцій приймалася у другій половині XX ст., коли комп'ютер ще не розглядався як атрибут домашнього інтер'єра, а кіберпростір був здебільшого місцем розгортання сюжету фантастичних романів.

У країнах СНД захист прайвесі у кіберпросторі спирається на загальні конституційні приписи про неприпустимість втручання у приватне і сімейне життя, неприпустимість збирання, зберігання, використання й поширення конфіденційної інформації про особу без її згоди, а також право на судовий захист від зловживань персональними даними (ст. 20 Конституції Вірменії, ч.1 ст. 23, ч. 1 ст. 24 Конституції Росії, ст. 32 Конституції України та ін.) [17, с. 87, 445; 18]. Подібні загальні приписи не враховують специфіку кіберпростору та наявних у ньому загроз, а тому виявляються малоефективними для формування ефективної законодавчої бази щодо захисту прайвесі в електронних мережах.

Проведене дослідження дає змогу дійти певних висновків**.** Передусім, кіберпростір має бути „безпечною зоною" з точки зору недоторканності приватного життя, що вимагає розробки й запровадження системи відповідних нормативних, організаційних та технологічних заходів з боку держави. По-друге, очевидно, що вирішення названої проблеми має й конституційний рівень, свідченням чому є політико-правова практика провідних країн західної демократії. По-третє, надійне забезпечення недоторканності приватного життя у кіберпросторі вимагає з'ясування потенційних загроз прайвесі, що несуть із собою нові комп'ютерні технології, узагальнення реальних прикладів порушення прайвесі, накопичених правозастосовчою практикою, а також виокремлення передового досвіду конституційно-правової регламентації суспільних відносин, пов'язаних із реалізацією інформаційних потреб громадян та захистом приватного життя від протиправних посягань. Вирішення названих проблем є перспективними напрямками подальших досліджень у даній сфері.

Список використаної літератури:

1. Byford K. S. Privacy in cyberspace: constructing a model of privacy for the electronic communications environment // Rutgers computer & technology law journal. – 1998. – March. – P. 1-74.
2. Teh J. Privacy wars in cyberspace: an examination of the legal and business tensions in information privacy // Yale journal of law & technology. – 2001-2002. – Vol. 4. – P. 7-55.
3. Radwanski G. Address by the Privacy Commissioner of Canada delivered to the Institute of Canadian advertising, Feb. 27, 2001 // http://www.privcom.gc.ca/speech.
4. Geist M. Privacy law needs open disclosure // The Globe and mail. – 2001. – Vol. 31. – P. T3.
5. Гарфинкель С. Всё под контролем: Кто и как следит за тобой / Пер. с англ. – Екатеринбург, 2004.
6. Schwartz P. Privacy and democracy in cyberspace // Vanderbilt law review. – 1999. – Vol. 52. – P. 1609-1625.
7. Kang J. Information privacy in cyberspace transactions // Stanford law review. – 1998. – Vol. 50. – P. 1193-1226.
8. McVeigh v. Cohen, 983 F. Supp. 215 (D.D.C. 1998).
9. Как сетевая жизнь может нарушить неприкосновенность личной жизни // Webplaneta.de. // http://www.webplaneta.de/articles.php?article=844.
10. Internet privacy // Wikipedia, the free encyclopedia // http://en.wikipedia.org/wiki/Internet_privacy.

11. Solove D.J. Do social networks bring the end of privacy? // Scientific American. – 2008. – Vol. 299. – P. 100-106.
12. Angwin J. Watchdog planned for online privacy // The Wall Street Journal. – 2010. – November 11.
13. Неприкосновенность частной жизни в Швейцарии // http://www.seoded.com/2010/09/blog-post_19.html.
14. Конституции государств Европейского Союза / Под общ. ред. Л.А. Окунькова. – М., 1997.
15. Конституция Швейцарской Конфедерации от 18 апреля 1999 г. // Королева-Борсоди Н.В. Основы конституционного права Швейцарии: Учебно-метод. пособ. – К., 2009.
16. Конституции государств-участников СНГ / Ред. кол. Л.А. Окуньков (рук.), В.В. Оксамытный, М. Я. Булошников. – М., 2001.
17. Конституція України від 28 червня 1996 р. // ВВР. – 1996. – № 30. – Ст. 141.

Надійшла до редакції 09.02.2011

ШАПОВАЛ В.Д., кандидат юридичних наук
(Кременчуцький національний університет ім. Михайла Остроградського)

УДК 342.5

ІННОВАЦІЇ КЕРІВНИЦТВА В ОРГАНАХ МІСЦЕВОГО САМОВРЯДУВАННЯ УКРАЇНИ

Зростання ролі місцевого самоврядування у вітчизняних управлінських реформах визначається загальносоціальним процесом формування самоврядної парадигми соціального управління. Системоутворююча роль місцевого самоврядування стосовно управлінських новацій проявляється у визначенні ним основних принципів функціонування системи публічного та державного управління. Конституювання сучасної системи місцевого самоврядування здійснюється передусім через процеси децентралізації. Найбільш актуальним аспектом подальших досліджень проблеми є адаптація європейського досвіду розвитку засад самоврядування для потреб вітчизняної адміністративної реформи.

***Ключові слова**: місцеве самоврядування, публічне та державне управління, реформа, регіон, публічна влада.*

Возрастание роли местного самоуправления в отечественных управленческих реформах определяется общесоциальным процессом формирования самоуправляемой парадигмы социального управления. Системообразующая роль местного самоуправления относительно управленческих новаций проявляется в определении им основных принципов функционирования системы публичного и государственного управления. Конституирование современной системы местного самоуправления осуществляется прежде всего благодаря процессам децентрализации. Наиболее актуальным аспектом дальнейших исследований проблемы является адаптация европейского опыта развития принципов самоуправления для потребностей отечественной административной реформы.

***Ключевые слова:** местное самоуправление, публичное и государственное управление, реформа, регион, публичная власть.*

The development of the role of self-government in national managerial reforms determines by means of common social process of social management self-government paradigm. System-formative role of local self-government concerning managerial innovations reveals in the determination of its main principles of public and state government functioning. Constitutionality of modern system of local self-government implements through decentralization processes. The most actual aspect of further study is the adaptation of European experience of self-government grounds development for national administrative reform needs.

***Key words:** local self-government, public and state government, reform, region, public authority.*

Зростання ролі місцевого самоврядування становить магістральний напрям реформування системи управління в Українській державі. З інноваційними змінами самоврядного характеру пов'язуються не тільки принципові зміни в системі державного управління, а й можливості становлення в Україні сучасного інформаційного суспільства.

Питання реформування місцевого самоврядування у контексті адміністративної реформи розглядаються у працях В. Бакуменка, Ю. Бальція, Н. Нижник, В. Шаповала та інших вітчизняних авторів. У центрі уваги знаходиться концептуальна визначеність реформ у системі са-