ПОНОМАРЕНКО К.І., аспірант
(Відкритий міжнародний університет розвитку людини «Україна»)

УДК 342.723

ІНФОРМАЦІЙНА ПРИВАТНІСТЬ ЯК ОБ'ЄКТ ПРАВОВОГО РЕГУЛЮВАННЯ

У цій статті розглядаються проблема надання чіткого визначення поняттю інформаційної приватності як об'єкта правового регулювання, деякі теоретичні підходи до з'ясування необхідності та меж захисту інформаційної приватності, її співвідношення з приватністю комунікації. Також проаналізовано критику ідеї приватності. Зроблено спробу надати визначення інформаційній приватності.

Ключові слова: *приватність, інформаційна приватність, приватність комунікацій, спостереження*.

В данной статье рассматриваются проблема предоставления четкого определения понятию информационной приватности как объекта правового регулирования, некоторые теоретические подходы к определению необходимости и границ защиты информационной приватности, ее соотношения с приватностью коммуникаций. Предлагается анализ критических подходов к трактованию идеи приватности. Осуществляется попытка формулировки определения информационной приватности.

Ключевые слова: *приватность, информационная приватность, приватность коммуникаций, наблюдение.*

At this article the problem of clear definition assignment to the phenomenon of information privacy as an object of law regulation, some theoretical approaches to definition of the necessity and limits of its protection are given. Although, the correlation between information privacy and privacy of communications is analyzed. The critics of privacy paradigm are analyzed. An attempt of the formulation of definition of information privacy is carried out.

Keywords: *privacy, information privacy, privacy of communications, surveillance.*

Дослідження проблематики інформаційних правовідносин в Україні невпинно набуває актуальності з огляду на стрімкий розвиток інформаційних технологій та інформаційного суспільства. Найважливішим завданням законодавця в даних умовах є пристосування чинного законодавства до сучасних умов та динамічного розвитку технологічних можливостей, що разом із утилітарною користю несуть потенційну загрозу завдання істотної шкоди законним правам та інтересам громадян.

Серед вітчизняних вчених значну увагу в своїх дослідженнях питанню правової природи приватності та регулювання суспільних інформаційних відносин приділяють В.М. Брижко, А.В. Пазюк, О.А. Баранов, В.Д. Гавловський, В.С. Цимбалюк та ін.

Метою нашої статті є аналіз феномену інформаційної приватності як об'єкта правового регулювання, її місця у систему прав людини, основних принципів її захисту.

Для того щоб розглядати явище в якості об'єкта правового регулювання, необхідно перш за все виокремити та проаналізувати його істотні ознаки, а також надати йому визначення, окресливши межі його можливого застосування.

Місце права на приватність у системі прав людини

Сьогодні право на захист від втручання в особисте та сімейне життя відносять до особистісних прав людини як можливість збереження, розвитку й захисту морально-психологічної індивідуальності людини, її світогляду та духовності (разом з такими, як право на ім'я, честь, гідність, свободу думки і слова) і розуміють його як недоторканність середовища життя людини, захист її від свавільного втручання державних органів та будь-яких інших сторонніх осіб, у тому числі і членів сім'ї. Це суб'єктивне право, для ефективного захисту якого здебільшого необхідно користуватися прямою чи непрямою допомогою держави [1, с. 92-93].

Тридцята міжнародна конференція уповноважених із захисту даних та приватності, що відбулася 17 жовтня 2008 р. в Страсбурзі, у своїй Резолюції «Про крайню необхідність захисту недоторканності приватного життя в світі без кордонів» чітко висловила позицію стовно місця права на захист даних та недоторканність приватного життя і розглядає ці права у якості осно-

вних прав людини незалежно від національності чи місця проживання. Також у резолюції наголошується на тому, що існуюча в світі нерівність у сфері захисту даних та приватності, зокрема у зв'язку з тим, що багато держав і досі не прийняли належних законів, завдає шкоду обміну персональною інформацією та ефективному глобальному захисту даних [2].

Дослідник А.В. Пазюк зазначає, що право на приватність персоніфікованої інформації історично з'явилось як складова частина права на захист від неправомірного втручання держави у приватне життя, а тому може бути віднесено до категорії «громадянські права» [3, с. 31].

Слід звернути увагу на те, що тлумачення феномену приватності не обмежується лише правом на захист від втручання у приватне життя. Приватність багатозначна – вона передбачає і безперешкодну можливість особи здійснювати контроль над інформацією, що стосується її особистості чи власності, і право створювати на свій розсуд та зберігати в таємниці власний інформаційний портрет, а також право бути залишеним у спокої та інші значення. Таким чином, право на приватність як юридична категорія включає цілий набір правомочностей, таких як право фізичної особи контролювати і знати інформацію про себе, а за необхідності отримувати доступ до такої інформації, яка безпосередньо її стосується; право тримати в таємниці власний інформаційний портрет або створювати та розповсюджувати його на власний розсуд та за власним бажанням; також право мати такий ступінь відокремленості від державних та суспільних інституцій, який би дозволяв особі відчувати себе природно і вільно.

А. Раян, наприклад, вважає центральним елементом ідеї приватності право контролювати, яку інформацію люди мають щодо певних сфер нашого життя, і зобов'язання інших людей оминати ті сфери; за словами науковця, «це не зобов'язання не знати про нас, але зобов'язання не намагатися знати все» [4, с. 151].

Право на приватність також передбачає право фізичної особи приховувати інформацію, що може її дискредитувати. З приводу цього положення є думка судді Р. Познера, яку цитує Д. Солоу у своїй доповіді, яка звучить так: «коли люди сьогодні засуджують недостатній захист приватності, все, чого вони прагнуть, я думаю, – це здебільшого щось інше, ніж просто усамітнення: вони хочуть мати більше ресурсів для приховування тієї інформації про себе, яку інші можуть використати в невигідному для них відношенні». Таким чином, приватність, можливо, покликана слугувати там, де є щось, що необхідно приховати, і це щось містить негативну інформацію про особу. Р. Познер доводить, що закон не повинен захищати людей, які приховують інформацію, що їх дискредитує [5].

Спорідненою до цієї є ідея про необхідність зниження ступеня захисту права на приватність для осіб, що обіймають чи претендують на зайняття державно-владних посад, втілена у ряді національних законів про захист даних. Наприклад, у п. 4 ст. 5 Закону України «Про захист персональних даних» міститься положення, де вказано, що персональні дані фізичної особи, яка претендує зайняти чи займає виборну посаду (у представницьких органах) або посаду державного службовця першої категорії, не належать до інформації з обмеженим доступом, за винятком інформації, яка визначена такою відповідно до закону.

Отже, припускається, що особам, не задіяним у незаконній діяльності, немає про що непокоїтись, а захищати право на приватність осіб, які мають на меті порушувати закон або, наприклад, зайняти виборні посади в представницьких органах, що надасть їм потенційну змогу порушувати та обходити норми закону, взагалі немає сенсу.

Право на приватність є лише однією зі складових феномену права на повагу до приватного життя, воно є багатозначним і включає як складову частину право на інформаційну приватність.

Перша спроба надати об'єктивну понятійну форму феномену приватності належала С. Уорену та Л. Брайндейзу, які визначили його як «право бути залишеним у спокої» [6]. Дане формулювання було широким та неоднозначним, але на той час актуальним, хоча й викликало хвилю критичних зауважень з приводу незрозумілості терміна та особливостей його практичного застосування.

Якийсь час тому вчені вважали, що приватність є настільки заплутаною концепцією, що це робить її малопридатною для використання. Згідно з думкою А. Міллера, приватність «дратуюче невизначена та швидкоплинна». Як вказав Х. Грос, «концепція приватності інфікована згубними незрозумілостями». К. Бенет аналогічно відзначав, що «спроби визначення концепції приватності звичайно не можуть мати ніякого успіху». Р. Пост заявляє, що «приватність – це така складна цінність, так заплутана в конкуруючих та суперечливих вимірах, так нашпигована

різноманітними змістами, що іноді я втрачаю віру у можливість її використання стосовно хоч когось». Дж. Д. Томсон зазначає: «Право на приватність, можливо, найбільш дивна річ, оскільки не видно нікого, хто мав би визначену ідею з приводу того, що це таке».

Д. Солоу влучно зауважує, що частіше за все юристи, політики та вчені просто аналізують проблему, без того, щоб сформулювати концепцію приватності, особливо з огляду на те, що сьогодні існує безліч способів здійснити втручання, не порушуючи при цьому приватності в широкому розумінні. А з іншого боку, така конструкція може передбачати також заборону навіть дивитись на людину [5].

Таким чином, намагаючись дати визначення поняттю, ми ризикуємо розширити його значення, зробивши його занадто узагальненим, або навпаки, звузити його значення до того, що його взагалі буде важко застосувати.

Сьогодні вчені схиляються до плюралістичного розуміння приватності, оскільки неможливо звести усі прояви, контексти та ознаки до єдиної узагальненої сутності. Д. Солоу, наприклад, пропонує термін «приватність» використовувати в якості короткого позначення для мережі пов'язаних понять. Оскільки за межами його використання, як зазначає дослідник, даний термін фактично вносить більше туману, аніж ясності [5].

Намагаючись дати визначення феномену інформаційної приватності, можна згадати визначення Т. Емерсона стосовно феномену права на приватність в цілому: право на приватність – це в дійсності право не розділяти життя з колективом, право залишити суспільство. Тобто право на приватність визначає суверенітет індивідуума. Звідси можна зробити висновок, що інформаційну приватність можна вважати інформаційним суверенітетом особи, а також її правом не розділяти інформацію з колективом, суспільством та державою.

Традиційно розрізняють чотири складові (види) приватності, серед яких фізична, територіальна, інформаційна та приватність комунікацій.

На думку російських дослідників Р.М. Юсупова, В.П. Заболотського, В.П. Іванова, інформаційна приватність має територіальний вимір, оскільки інформаційні потоки циркулюють у певному фізичному просторі. Людина ж є основним джерелом інформації, яка генерується всередині її життєвого простору, і є споживачем інформації, яка надходить до неї ззовні [7].

У літературі неодноразово наголошувалось на складності розмежування інформаційної приватності з комунікаційною, оскільки завдяки розвитку телекомунікаційних технологій з'явилась можливість передавати та отримувати будь-яку інформацію засобами комунікацій, навіть в момент її створення, в інтерактивному режимі або засобами негласного її отримання. Таким чином, інформаційну приватність необхідно розглядати в комплексі та з урахуванням її тісного зв'язку з комунікаційною приватністю. Часто через складнощі відмежування моменту виникнення інформації та початку її розповсюдження шляхом комунікації просто неможливо визначити грані між комунікаційною та інформаційною приватністю.

Як вказує А.В.Пазюк, розвиток інформаційних технологій поступово стирає грані між цими поняттями, оскільки стрімке поширення електронних комунікацій, в яких повідомлення передаються у цифровому вигляді, не дозволяє технічно й нормативно розмежувати, де закінчується комунікаційна приватність та починається приватність персональних даних. Це вимагає пристосування нормативно-правового регулювання до розвитку інформаційних технологій з метою зробити його «технічно нейтральним» [3, с. 18].

На нашу думку, на сучасному рівні розвитку суспільства під інформаційною приватністю доцільно розуміти такий стан фізичної особи, за якого вона як носій та першоджерело інформації про себе має виключне право нею розпоряджатися, розголошувати, приховувати, передавати або змінювати цю інформацію. В такому разі не має значення, який характер носить ця інформація, оскільки, користуючись одним із головних юридичних постулатів, діяльність людини вважається законною, доки протилежне не доведено в судовому порядку.

Захист персональних даних суб'єктів інформаційно-комунікаційної діяльності, а отже, і суб'єктів інформаційної приватності, має ґрунтуватись на певному наборі основоположних ідей та засад, на яких заснована ця діяльність і недодержання яких тягне за собою порушення прав та інтересів суб'єктів права на інформаційну приватність. Дані принципи повинні втілюватися законодавцем у національних нормативно-правових актах, що стосуються зазначеної сфери суспільних відносин. Для того, щоб уніфікувати механізм захисту персональних даних

та регулярно розробляти актуальні рекомендації в цій галузі, щорічно відбуваються міжнародні конференції уповноважених із захисту даних і приватності.

У частині II Резолюції про міжнародні стандарти захисту приватності, розробленій під час 31 Міжнародної конференції уповноважених із захисту даних, що відбулася 5 листопада 2009 р. в Мадриді (Іспанія), визначено такі основні принципи захисту приватності:

1. Принцип законності та справедливості обробки персональних даних – персональні дані мають оброблятися з додержанням національного законодавства, прав і свобод людини, а також у відповідності до цілей та принципів, викладених у Загальній декларації прав людини та Міжнародному пакті про громадянські та політичні права. Зокрема, будь-яка обробка персональних даних, що призводить до незаконних або дискримінаційних заходів стосовно суб'єкта даних, вважається несправедливою.

2. Принцип визначеності цілей обробки – обробка ПД має обмежуватися виконанням конкретної, явної та законної мети відповідальної особи. Відповідальна особа не повинна провадити будь-яку обробку, що є несумісною із цілями, для яких були зібрані персональні дані, якщо вона не має однозначної згоди на це від суб'єкта даних.

3. Принцип пропорційності – обробка ПД повинна бути адекватною, пропорційною та не надмірною щодо її цілей, зокрема, відповідальна особа повинна вжити розумних зусиль для того, щоб обмежити обробку ПД до мінімально необхідного рівня.

4. Якості даних – відповідальна особа завжди має забезпечувати точність, достатність та своєчасне оновлення ПД для того, щоб досягнути цілей, з якими вони обробляються. Відповідальна особа повинна обмежувати період зберігання даних, що обробляються, мінімально необхідним строком. Таким чином, коли ПД більш не є необхідними для досягнення цілей, які робили їх обробку законною, вони мають бути знищені або ж знеособлені.

5. Відкритості – будь-яка відповідальна особа повинна проводити прозору політику відносно обробки ПД. Відповідальна особа повинна надавати суб'єктам даних як мінімум інформацію про відповідальну особу, цілі обробки, одержувачів цих даних, про те, яким чином вони будуть використовуватись, а також будь-яку іншу додаткову інформацію, необхідну для того, щоб гарантувати справедливу обробку ПД. Якщо ПД одержані безпосередньо від суб'єкта даних, інформацію має бути надано під час збирання даних, якщо її ще не було надано. Якщо ПД одержані не безпосередньо від суб'єкта даних, відповідальна особа має повідомити про джерело цих даних. Ця інформація має бути надана протягом розумного строку; дану вимогу може бути замінено на альтернативні заходи, якщо їх виконання неможливе або пов'язане з надмірними зусиллями з боку відповідальної особи. Будь-яку інформацію, що надсилається суб'єкту даних, має бути викладено у зрозумілій формі, з використанням простої мови, зокрема, у випадку обробки інформації, пов'язаної з неповнолітніми. Якщо ПД збираються за допомогою електронних комунікаційних мереж, обов'язки відповідальної особи можуть бути викладені шляхом повідомлення у політиці приватності, простій, доступній та такій, що включає у себе усю перелічену вище інформацію.

6. Звітності – відповідальна особа повинна вживати усіх необхідних заходів для додержання принципів та обов'язків, закріплених національним законодавством, та мати необхідні внутрішні механізми для демонстрації додержання цих принципів та обов'язків як суб'єктами даних, так і наглядовим органом при виконанні своїх обов'язків.

Окремо визначається та розшифровується принцип легітимності обробки. Як правило, персональні дані можуть піддаватися обробці в одній з таких ситуацій:

1) якщо отримано вільну, недвозначну та усвідомлену згоду суб'єкта даних;

2) якщо законні інтереси відповідальної особи виправдовують обробку, при чому законні інтереси, права і свободи суб'єктів даних не превалюють;

3) якщо обробка необхідна для підтримання або реалізації правових відносин між відповідальною особою та суб'єктом даних;

4) якщо обробка необхідна для виконання обов'язків відповідальної особи, визначених чинним національним законодавством, або провадиться державним органом, коли це необхідно для законної реалізації її повноважень;

5) у виключних випадках, що загрожують життю, здоров'ю або безпеці суб'єкта даних або іншої особи.

Відповідальна особа повинна гарантувати просту, швидку та ефективну процедуру, що до-

зволяє суб'єкту даних відкликати свою згоду в будь-який час, процедуру, яка б не викликала невиправданих затримок або витрат і не приносила б жодного прибутку відповідальній особі [8].

Особливу увагу уповноважені із захисту даних та приватності приділяють тлумаченню категорії «вразливі дані». Вразливими вважаються такі персональні дані, що зачіпають найбільш інтимні сфери життя суб'єкта даних, а також дані, що у випадку зловживання можуть призвести до незаконної або довільної дискримінації або становити серйозний ризик для суб'єкта даних. Це, зокрема, дані, які вважаються конфіденційною інформацією і можуть виявити такі аспекти, як расове або етнічне походження, політичні погляди, релігійні або філософські переконання, а також дані, що стосуються здоров'я або сексуального життя. Чинне національне законодавство може закріплювати й інші категорії вразливих даних, якщо додержуються умови захисту даних.

У національному законодавстві мають бути гарантії для захисту прав суб'єктів даних, що передбачають додаткові умови для обробки вразливих персональних даних.

Відповідальна особа може здійснювати обробку персональних даних за допомогою одного чи декількох поставщиків послуг обробки, і це не вважається розголошенням даних третім особам, за умови, якщо вона гарантує, що постачальник послуг обробки забезпечує принаймні такий рівень захисту, що визначений міжнародним та відповідним національним законодавством.

На жаль, Закон України «Про захист персональних даних» не виокремлює цю категорію, надаючи однаковий ступінь захисту будь-яким категоріям даних, але тим самим потенційно ускладнюючи доступ навіть до таких даних, доступ до яких не завдасть істотної шкоди їх суб'єктам. На нашу думку, вказаний закон необхідно доповнити нормою такого змісту: «Особливі категорії даних (вразливі персональні дані) – персональні дані, що свідчать про расову приналежність, політичні, релігійні чи інші переконання особи, а також дані, що стосуються стану її здоров'я чи статевого життя». Також з огляду на те, що поняття вразливості має оціночний характер, доцільно було б розглянути можливість вирішення у судовому порядку (наприклад, під час провадження у кримінальній чи адміністративній справі), чи є певні дані вразливими у кожному конкретному випадку стосовно конкретної особи, якщо вона заявляє клопотання про це.

Будувати механізм захисту приватності в Україні необхідно враховуючи її основні характеристики, принципи захисту персональних даних, рекомендації, що надаються на міжнародному рівні, а також виходячи із потенційних загроз приватності. Серед таких загроз найбільше занепокоєння викликає неврегульованість відносин та передачі інформації засобами Інтернет, зокрема захисту приватності дітей у мережі; а також повторне або нецільове використання персональних даних, зібраних для здійснення конкретної мети і таких, що підлягають негайному знищенню або знеособленню відразу після використання.

Розглянувши деякі аспекти інформаційної приватності, можемо зробити висновок про те, що царина правового регулювання її захисту потребує подальшого розроблення та вдосконалення, а також пристосування до сучасних умов швидкого науково-технічного розвитку суспільства.

Список використаної літератури:

1. Приватне життя і поліція. Концептуальні підходи. Теорія та практика / Відп. ред. Ю.І. Римаренко. – К., 2006.
2. Comments on the Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data // http://www.privacyconference2008.org.
3. Пазюк А.В. Міжнародно-правовий захист права людини на приватність персоніфікованої інформації: Дис. ... канд. юрид. наук. – К., 2004.
4. Ryan A. Private Selves and Public Parts // Public and Private in Social Life / Edited by S. I. Benn and G. F. Gaus. – London, 1983. – P. 135-154
5. Солоу Д. Ошибочные толкования приватности // http://itsec.com.ua/stat-i/oshibochnye-tolkovaniya-privatnosti.html.
6. Warren S., Brandeis L. The Right to Privacy // Harvard Law Review. – 1980. – № 4(5).
7. Юсупов Р.М., Заболотский В.П., Иванов В.П. Человек в информационном пространстве // Проблемы информатизации. – 1996. – № 4. – С. 3-7.
8. 31st International conference of data protection and privacy // http://www.privacyconference2009.org

Надійшла до редакції 12.05.2011