ВОЛОХ О. К.,
кандидат юридичних наук,
доцент кафедри
адміністративного права і процесу
*(Національна академія
внутрішніх справ)*

УДК 35.077.2

ОКРЕМІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ПРАВА ОСОБИ НА ПРИВАТНІСТЬ В УМОВАХ РОЗВИТКУ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

У статті розглядаються проблеми забезпечення права особи на невтручання в приватне життя, пов'язані з розвитком інформаційного суспільства. Обгрунтовуються ризики порушення зазначеного права у зв'язку з окремими законотворчими ініціативами. Висвітлюються питання легітимізації доступу до персональних даних громадян України.

Ключові слова: *приватне життя, персональні дані, інформаційне суспільство, інформаційна безпека, верховенство права.*

В статье рассматриваются проблемы обеспечения права лица на невмешательство в приватную жизнь, связанные с развитием информационного общества. Обосновываются риски нарушения указанного права в связи с отдельными законотворческими инициативами. Освещаются вопросы легитимизации доступа к персональным данным граждан Украины.

Ключевые слова: *приватная жизнь, персональные данные, информационное общество, информационная безопасность, верховенство права.*

In the article the problem of maintenance of the right to non-interference in the private life, associated with the development of the information society. Substantiated risk of abuse of these rights in relation to certain legislative initiatives. The issue of legitimizing access to personal data of citizens of Ukraine.

Key words: *privacy, personal data, information society, information security, rule of law.*

Вступ. У зв'язку з розвитком в Україні інформаційного суспільства з'являються нові виклики конституційно гарантованим правам людини і громадянина. Відповідно до ч. 3 ст. 22 Основного Закону України не допускається звуження змісту та обсягу наявних прав і свобод при прийнятті нових законів або внесенні змін до чинних законів. Крім того, Конституція України містить такі важливі норми:

– права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави; держава відповідає перед людиною за свою діяльність; утвердження і забезпечення прав і свобод людини є головним обов'язком держави (ст. 3);

– в Україні визнається і діє принцип верховенства права; закони та інші нормативно-правові акти приймаються на основі Конституції України і повинні відповідати їй (ст. 8) [1].

Постановка завдання. Метою статті є дослідження положень проекту Закону України «Про внесення змін до деяких законів України щодо посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби з кіберзлочинністю» (далі – Законопроект № 2133а) [2] стосовно відповідності їх принципу верховенства права.

Результати дослідження. В умовах розвитку інформаційного суспільства особливого значення набуває забезпечення права особи на приватність. Ризики незаконного доступу до персональних даних громадян, що зберігаються в інформаційних системах, є очевидними.

На цьому тлі доволі дивними виглядають нормотворчі ініціативи окремих народних депутатів України стосовно легітимізації процесу отримання відомостей про особу, обробка яких, за визначенням Уповноваженого Верховної Ради України з прав людини, становить особливі ризики для прав і свобод суб'єктів персональних даних [3].

Йдеться про Законопроект № 2133а. До того ж, серед ініціаторів цього проекту слід назвати Голову комітету Верховної Ради України з питань законодавчого забезпечення правоохоронної діяльності. Ймовірно, для надійності прийняття парламентом Законопроект № 2133а знаходиться на розгляді саме в цьому комітеті.

Комітет з питань правової політики та правосуддя розглянув на своєму засіданні 3 листопада 2015 року (протокол № 36) на відповідність Конституції України аналізований нами Законопроект і дійшов висновку, що він «не суперечить положенням Конституції України» [4].

Проведений нами аналіз свідчить, що норми Законопроекту № 2133а не узгоджуються з принципом верховенства права, отже, проект не відповідає Конституції України. Наша переконаність у цьому базується на таких міркуваннях.

1) Відповідно до Пояснювальної записки Законопроект № 2133а розроблений з метою формування засад державної політики у сфері забезпечення кібернетичної безпеки України, яку буде досягнуто шляхом внесення змін до положень Закону України «Про основи національної безпеки України» та інших законі в частині визначення основних реальних і потенційних загроз національній безпеці України кібернетичного характеру, основних напрямів державної політики та основних функцій суб'єктів забезпечення національної безпеки в цій сфері, а також уведення таких основоположних понять, як «кібернетична безпека (кібербезпека)» та «кібернетичний простір (кіберпростір)» [5].

У зв'язку з цим слід наголосити на тому, що назва Законопроекту № 2133а не відповідає проголошеній меті його прийняття. Так зване посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби з кіберзлочинністю виражається у доповненні Кодексу України про адміністративні правопорушення ст. 188-43 «Невиконання законних вимог посадових осіб Служби безпеки України». Але з цього приводу необхідно зазначити, що Законом України від 23 лютого 2014 року № 767-VII [6] ідентичну за номером, назвою та змістом статтю було виключено з Кодексу. Таким чином, майже півтора роки необхідності у цій статті не було.

Справжня мета Законопроекту № 2133а простежується при аналізі пропонованих змін та доповнень до низки законодавчих актів (зокрема до Законів України «Про оперативно-розшукову діяльність», «Про Службу безпеки України», «Про контррозвідувальну діяльність») і полягає у нічим не обґрунтованому наданні співробітникам Служби безпеки України повноважень щодо надмірного втручання в приватне (особисте і сімейне) життя громадян.

Об'єктивно такі норми суперечать ч. 3 ст. 22 Конституції України, за якою не допускається звуження змісту та обсягу наявних прав і свобод при прийнятті нових законів або внесенні змін до чинних законів.

2) Диспозиція пропонованої до Кодексу України про адміністративні правопорушення ст. 188-43 передбачає відповідальність за невиконання законних *вимог* посадових осіб Служби безпеки України. Водночас ініціатори Законопроекту № 2133а пропонують доповнити ч. 1 ст. 39 Закону України «Про телекомунікації» новим п. 183, у зв'язку з чим оператори телекомунікацій будуть зобов'язані надавати на *вимогу* уповноваженого органу інформацію про своїх абонентів та спожиті / надані ними / ним послуги.

Зазначене свідчить про спробу надати Службі безпеки України законне право збирати інформацію особистого характеру про абонентів мобільного зв'язку та мережі Інтернет.

3) Для України питання забезпечення кібернетичної безпеки актуалізується в міру розвитку й поширення систем «електронного урядування», «електронного банкінгу»,

«електронної комерції», «електронної медицини», «електронної освіти» тощо, які роблять інформаційно-телекомунікаційні системи урядового, оборонного, виробничого, кредитно-фінансового, комунального та інших секторів уразливими для деструктивного впливу з кіберпростору.

Але необхідно зазначити, що інформаційні відносини, пов'язані із забезпеченням кібернетичної безпеки, вже врегульовані Законами України «Про інформацію», «Про науково-технічну інформацію», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про доступ до публічної інформації» тощо.

При цьому ключова роль у забезпеченні кібернетичної безпеки покладається на Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», який регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Зокрема, в ньому визначаються необхідні для відповідних цілей терміни («блокування інформації», «виток інформації», «захист інформації», «комплексна система захисту інформації», «інформаційна (автоматизована) система», «криптографічний захист інформації», «несанкціоновані дії щодо інформації в системі», «технічний захист інформації» тощо), об'єкти захисту та суб'єкти відповідних відносин, умови обробки інформації та способи забезпечення захисту інформації в системі, повноваження державних органів у сфері захисту інформації в автоматизованих системах.

Відповідно до ст. 10 вказаного вище Закону України спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації (ним є Адміністрація Державної служби спеціального зв'язку та захисту інформації України):

– розробляє пропозиції щодо державної політики у сфері захисту інформації та забезпечує її реалізацію в межах своєї компетенції;

– визначає вимоги та порядок створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

– організовує проведення державної експертизи комплексних систем захисту інформації, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації;

– здійснює контроль за забезпеченням захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Згідно зі ст. 10 Закону України «Про Службу безпеки України» до складу Центрального управління Служби безпеки України входить підрозділ контррозвідувального захисту інтересів держави у сфері інформаційної безпеки.

За відповідні правопорушення у зазначеній сфері чинним законодавством передбачена адміністративна та кримінальна відповідальність. Зокрема, ст. 212-6 Кодексу України про адміністративні правопорушення передбачено відповідальність за здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем.

У Кримінальному кодексі України 2001 року (далі – КК України) вказаним діянням присвячено окремий розд. XVI Особливої частини.

З огляду на зазначене є підстави вважати, що чинне законодавство України вже містить достатню кількість правових норм, спрямованих на правову охорону кібернетичної безпеки України.

Тому проблеми, які виникають у сфері забезпечення кібернетичної безпеки України, є не стільки результатом відсутності достатньої законодавчої бази, скільки результатом недостатньо ефективної діяльності відповідних державних органів, уповноважених забезпечувати захист інформації у процесі використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку [7].

4) Законопроект № 2133а поданий до парламенту з порушенням норм Регламенту Верховної Ради України.

У Пояснювальній записці до Законопроекту № 2133а вказано, що «прийняття запропонованих змін та їх реалізація не потребуватимуть додаткових бюджетних витрат». Але змінами до ст. 5 Закону України «Про оперативно-розшукову діяльність» фактично пропонується створити новий функціональний підрозділ Служби безпеки України, який здійснюватиме оперативно-розшукову діяльність. Очевидно, що на утримання співробітників такого підрозділу використовуватимуться кошти з Державного бюджету.

З цього приводу необхідно вказати, що, згідно з ч. 3 ст. 91 Регламенту Верховної Ради України, у разі внесення законопроекту, прийняття якого призведе до зміни показників бюджету (надходжень бюджету та / або витрат бюджету), суб'єкт права законодавчої ініціативи зобов'язаний додати фінансово-економічне обґрунтування (включаючи відповідні розрахунки). Якщо такі зміни показників бюджету передбачають зменшення надходжень бюджету та / або збільшення витрат бюджету, до законопроекту подаються пропозиції змін до законодавчих актів щодо скорочення витрат бюджету та / або джерел додаткових надходжень бюджету для досягнення збалансованості бюджету [8].

При реєстрації Законопроекту № 2133а від 19 червня 2015 року жодної з перелічених вимог не було дотримано. Отже, автором Законопроекту № 2133а було порушено норму ч. 3 ст. 91 Регламенту Верховної Ради України.

Слід наголосити на тому, що, відповідно до ч. 2 ст. 92 Регламенту Верховної Ради України, *у прийнятті на реєстрацію законопроекту має бути відмовлено у разі, якщо він поданий з порушенням вимог ст. 91 цього Регламенту.* Отже, Законопроект № 2133а за нормами закону не можна було навіть реєструвати в апараті Верховної Ради України.

5) Законопроектом № 2133а пропонується доповнити ч. 1 ст. 25 Закону України «Про Службу безпеки України» п. 31 і таким чином надати співробітникам СБУ право *безперешкодно отримувати в установленому законом порядку доступ до інформації, яка обробляється в державних електронних інформаційних ресурсах (реєстри, бази та банки даних, інші інформаційні масиви), інформаційних, інформаційно-телекомунікаційних, телекомунікаційних системах операторів і провайдерів телекомунікацій, інших суб'єктів, які обробляють інформацію в електронному вигляді, незалежно від форм власності, щодо споживача, отриманих при укладанні договору наданих телекомунікаційних послуг, у тому числі отриманих послуг, їх тривалості та змісту, маршрутів передавання.*

Слід зазначити, що внаслідок цього співробітники СБУ матимуть доступ, у тому числі, до величезного обсягу персональних даних громадян. На нашу думку, навіть «для виконання покладених на них обов'язків» це занадто небезпечно у розрізі дотримання прав і свобод людини і громадянина. Тим більше, що, згідно з п. 4.4 Стратегії національної безпеки України, затвердженої Указом Президента України від 26 травня 2015 року № 287/2015, реформа Служби безпеки України передбачає, серед іншого, концентрацію зусиль на сприянні швидкому й ефективному обміну інформацією з державами – членами НАТО, ЄС. Тобто фактично йдеться про заплановану транскордонну передачу персональних даних громадян України до держав – членів НАТО та ЄС.

У зв'язку з цим потрібно згадати правову позицію Європейського суду з прав людини, висловлену у рішенні від 6 вересня 1978 року у справі «Класс та інші проти Німеччини»: «Суд зауважує, що при визначенні умов, за яких має діяти система таємного стеження, законодавчий орган держави користується певним дискреційним правом <…> Водночас, наголошує Суд, це не означає, що державі надається необмежене дискреційне право встановлювати таємне стеження за особами в межах своєї юрисдикції. Усвідомлюючи небезпеку, яку становить такий закон, підриваючи або навіть знищуючи демократію під приводом її захисту, Суд знову наголошує, що держава, яка підписала Конвенцію (Конвенцію про захист прав людини і основоположних свобод – *О. В.*), не має права, під виглядом протидії шпигунству та тероризмові, вживати заходів, які вона вважає необхідними» (п. 49) [9].

На жаль, у парламенті не вперше реєструються законопроекти, які передбачають непропорційний збір персональних даних без встановлення належних гарантій захисту прав суб'єктів даних.

Це також суперечить Рекомендації Комітету Міністрів Ради Європи CM/Rec (2010)13: «Використання профайлів, навіть законне, без обмежень і належних гарантії, може завдати серйозної шкоди людський гідності, а також іншим основоположним правам і свободам, в тому числі економічним і соціальним правам».

6) Викликає сумніви нова редакція терміна «національна безпека», за змістом якої до обсягу поняття «інформаційна безпека» з незрозумілих причин включено поняття «свобода слова». Право на свободу слова, безумовно, має бути захищеним. Але наведене у Законі України «Про Основні засади розвитку інформаційного суспільства на 2007–2015 роки» визначення поняття «інформаційна безпека» не містить у собі жодного натяку на зв'язок зі свободою слова: «Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» [10].

Висновки. Таким чином, враховуючи усі вищенаведені аргументи, необхідно визнати, що Законопроект № 2133а суперечить Конституції України. Він спрямований на чергове скорочення обсягу прав і свобод громадян, що є неприпустимим.

Список використаних джерел:

1. Конституція України від 28 червня 1996 року [Електронний ресурс]. – Режим доступу : http://www.rada.gov.ua.

2. Про внесення змін до деяких законів України щодо посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби з кіберзлочинністю : проект Закону України від 19 червня 2015 року № 2133а [Електронний ресурс]. – Режим доступу : http://www.rada.gov.ua.

3. Про затвердження документів у сфері захисту персональних даних : Наказ Уповноваженого Верховної Ради України від 8 січня 2014 року № 1/02-14 [Електронний ресурс]. – Режим доступу : http://www.rada.gov.ua.

4. Висновок Комітету Верховної Ради України з питань правової політики та правосуддя щодо проекту Закону про внесення змін до деяких законів України щодо посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби з кіберзлочинністю від 19 червня 2015 року № 2133а [Електронний ресурс]. – Режим доступу : http://www.rada.gov.ua.

5. Пояснювальна записка до проекту Закону про внесення змін до деяких законів України щодо посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби з кіберзлочинністю [Електронний ресурс]. – Режим доступу : http://www.rada.gov.ua.

6. Про внесення змін до деяких законодавчих актів України щодо припинення норм законів, схвалених 16 січня 2014 року : Закон України від 23 лютого 2014 року № 767-VII // Відомості Верховної Ради (ВВР). – 2014. – № 17. – Ст. 593.

7. Висновок Головного науково-експертного управління Верховної Ради України на проект Закону «Про внесення змін до Закону України «Про основи національної безпеки України» щодо кібернетичної безпеки України» від 7 березня 2013 року № 2483 [Електронний ресурс]. – Режим доступу : http://www.rada.gov.ua.

8. Про Регламент Верховної Ради України : Закон України від 10 лютого 2010 року № 1861-VI // Відомості Верховної Ради України (ВВР). – 2010. – № 14–15, № 16–17. – Ст. 133.

9. Рішення Європейського Суду з прав людини від 6 вересня 1978 року [Електронний ресурс]. – Режим доступу : http://www.rada.gov.ua.

10. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 9 січня 2007 року № 537-V [Електронний ресурс]. – Режим доступу : http://www.rada.gov.ua.