УДК 34.03+[336.719:004.056.5-027.552]

С. О. Биченко**, слухач магістратури 2-го року навчання заочної форми навчання юридичного факультету ДВНЗ "Українська академія банківської справи Національного банку України"; науковий керівник ст. викл. кафедри цивільно-правових дисциплін та банківського права ДВНЗ "Українська академія банківської справи Національного банку України", канд. юрид. наук **Р. В. Афанасієв

ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В БАНКІВСЬКІЙ СФЕРІ

Значний прогрес у розвитку інформаційних технологій у двадцятому та двадцять першому століттях, а саме: практично повсюдне запровадження інформаційно-комп'ютерних технологій і телекомунікаційних мереж, пов'язане з цим збільшення обсягів і напрямів використання персональних даних у різних сферах суспільного життя, їх передача новітніми комунікаційними засобами, істотно поширили можливості щодо збирання, зберігання і обробки інформації відносно фізичних осіб, а також швидке отримання даних з інших джерел. Дослідження проблеми правового регулювання відносин у банківській сфері, що виникають у зв'язку з обробкою (збиранням, зберіганням, використанням, поширенням) та захистом персональних даних, є необхідним для запровадження адекватного юридичного механізму в національну юридичну практику, що сприятиме ефективній реалізації положень Конституції України.

Ключові слова: правове регулювання, персональні дані, банки.

Постановка проблеми. Питання захисту персональних даних в банківській сфері, після прийняття Закону України "Про захист персональних даних", стало досить актуальним. Виникла й необхідність у вирішенні питань захисту персональних даних у банківській сфері в державі згідно принципів європейських стандартів. Водночас теоретичні та практичні питання правового регулювання відносин захисту персональних даних саме у банківській сфері до цього часу залишалися поза увагою представників науки.

Аналіз останніх досліджень і публікацій. Правове регулювання захисту персональних даних здійснюється на основі національних законодавчих актів, серед яких Закони України "Про захист персональних даних", "Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних", "Про інформацію", "Про банки і банківську діяльність" та низки роз'яснень до них, а також підзаконних нормативних актів та рекомендацій Національного банку України та Державної служби України з питань захисту персональних даних. Нажаль, проблемні питання, пов'язані із захистом персональних даних в банківській сфері, залишаються не вирішеними. Питання захисту персональних даних фізичної особи досліджують вітчизняні вчені: А. Баранов, В. Брижко, Ю. Базанов, В. Галаган, М. Гуцалюк, О. Жуковська, В. Лужецький, А. Пазюк, В. Цимбалюк, Т. С. Шалига та ін.

Не вирішена раніше частина загальної проблеми. Механізм захисту персональних даних в банківській сфері на сьогодні не достатньо досконалий і потребує суттєвого доопрацювання. Процес роботи банківських установ з персональними даними має врегульовуватися не тільки шляхом прийняття локальних процедурних документів, а й на державному рівні (зокрема, шляхом прийняття відповідного спільного документу Національним банком України та Державною службою України з питань захисту персональних даних).

Метою статті є аналіз сучасного стану правового регулювання захисту персональних даних в банківській сфері та пошук нових пропозицій та рекомендацій щодо побудови результативної державної та внутрішньобанківської системи захисту персональних даних клієнтів.

Виклад основного матеріалу. Банківська діяльність тісно пов'язана з використанням інформації, в тому числі персональних даних. Банківські установи в ході своєї діяльності стають розпорядниками та мультиплікаторами численних інформаційних масивів різного формату та призначення, для кожного з яких має бути встановлений окремий контрольований режим використання. Важливість урегулювання процесів роботи з інформацією в банках має коріння насамперед у конфіденційному характері даних, якими

розпоряджається фінансова установа. Конфіденційна інформація, яка містить персональні дані, характерна тим, що може бути розповсюджена тільки з дозволу та в порядку, узгодженому з власником інформації. Відтак у межах банківської діяльності угода банку з клієнтом і є тим основоположним документом, який передбачає порядок використання персональних даних [1, с. 320].

Під нормативно-правовим регулюванням захисту персональних даних слід розуміти здійснюване державою за допомогою права і сукупності правових засобів упорядкування, юридичне закріплення, охорону та розвиток суспільних відносин в сфері захисту персональних даних.

Дослідження значної кількості дефініцій поняття персональні дані, показало, що всі вони майже тотожні. Чинне національне законодавство дає таке визначення поняттю персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована (ст. 2 Закону України "Про захист персональних даних") [2]. На нашу думку, під поняттям "персональні дані" слід розуміти дані про живу людину, яка ідентифікована або може бути ідентифікована на основі цих даних або на основі цих даних і додаткової інформації, що може потрапити до особи, яка контролює дані, і які містять вираження ставлення до цієї людини і вказівку на певну мету або плани відносно цієї людини з боку особи, яка контролює дані, або іншої особи. Майже тотожне визначення містить Акт про захист персональних даних Великобританії (Data Protection Act 1998) [3]. Дане визначення є конкретизованим та, що найголовніше – робить акцент саме на мету використання інформації про особу, яка відповідно до положень ст. 6 Закону України "Про захист персональних даних", обов'язково має бути сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, які регулюють діяльність володільця бази персональних даних, та відповідати законодавству про захист персональних даних.

Проект Типового порядку обробки персональних даних у базах персональних даних (далі – Типовий порядок) визначає таку класифікацію персональних даних:

за природою – об'єктивні та суб'єктивні відомості про фізичну особу;

за способами обробки – текстові, графічні відомості, відомості у фото-, кіно-, аудіо-, голо- та відеоформаті;

за носіями – на папері або в електронній формі;

за ступенем зв'язку з особою – дані, що стосуються її безпосередньо або опосередковано;

за терміном обробки (зберігання) – короткострокові, середньострокові, довгострокові та безстрокові;

за змістом – ідентифікаційні дані, паспортні дані; особисті відомості, склад сім'ї, освіта, професія, біометричні дані, психологічні дані, житлові умови, спосіб життя, фінансова інформація та ін.;

за суб'єктним складом – відомості громадян, найманих працівників, посадових осіб, платників податків та зборів, клієнтів, покупців, споживачів, абонентів, пацієнтів, пасажирів, батьків, суб'єктів відносин у сфері страхування, суб'єктів фінансових відносин та інших осіб [4].

Погоджуючись з думкою вчених Д. О. Гетманцева та Н. Г. Шукліної, слід відмітити, що персональні дані є невід'ємною частиною відомостей, які становлять банківську таємницю, та набагато ширші, ніж поняття "персональні дані, які стали відомі банку". Всі обставини життя клієнта не можуть бути відомі банку. Коректно було б охоплювати режимом банківської таємниці не всі персональні дані, а лише ті, надання яких банк вимагає від своїх клієнтів. Режимом банківської таємниці повинні охоплюватися лише ті персональні дані клієнта, які банк отримує офіційно, тобто в ході безпосереднього здійснення своєї діяльності [5].

Положення міжнародних стандартів передбачають для всіх суб'єктів інформаційних відносин обов'язок, при якому персональні дані повинні:

– бути отримані законним шляхом;

– оброблятися за згодою на це суб'єкта даних і в кількості мінімально необхідній для визначеної діяльності;

– бути точними і оновлюватися;

– використовуватися тільки в суворо визначених цілях;

– бути доступними для суб'єкта даних та захищеними від несанкціонованого доступу.

Нормативно-правове регулювання захисту персональних даних в Україні здійснюється на основі Конституції України, Законів України "Про захист персональних даних", "Про інформацію", "Про нотаріат", "Про банки і банківську діяльність" та ін. Національні стандарти захисту персональних даних в Україні знаходяться на зародковому рівні. Україна лише намагається на правовому рівні закріпити загальні засади захисту (визначити інформацію, що відноситься до персональних даних; порядок роботи уповноваженого державного органу з питань захисту персональних даних; побудови механізму захисту і т.д.).

Закон України "Про захист персональних даних" запровадив прогресивні норми, які покликані охороняти конфіденційні дані та приватну інформацію громадян під час їх обробки та зберігання у різноманітних базах даних. При цьому Закон все ж є базовим документом, на основі якого почалася та триває активна робота із розробки цілої низки підзаконних актів, що деталізуватимуть норми Закону на стадії їх практичного застосування.

Правовий механізм захисту персональних являє собою систему взаємодіючих між собою елементів, серед яких виділяють правові засоби реалізації прав особи, а також засоби охорони та захисту. Правові засоби реалізації включають в себе сукупність повноважень суб'єкта персональних даних. Засоби охорони включають заходи спрямовані на недопущення порушення прав особи пов'язаних з її персональними даними. Ними є: наявність спеціально уповноваженого органу з питань захисту персональних – Державної служби з питань захисту персональних даних України; спеціальний Державний реєстр баз персональних даних – єдина державна інформаційна система збору, накопичення та обробки відомостей про зареєстровані бази персональних даних та ін. Засоби захисту призводять до відновлення порушених прав спричинених неправомірними діями і притягнення до відповідальності осіб, винних у вчиненні правопорушень.

Згідно з п. 3.6. Типового порядку банк, як володілець бази персональних даних, з метою належного функціонування системи управління персональними даними має забезпечувати:

1) затвердження необхідних процедур (методичних рекомендацій та правил тощо) стосовно вжиття заходів із забезпечення поточного функціонування системи управління персональними даними у базах персональних даних;

2) захист персональних даних у базі персональних даних від незаконної обробки, а також від незаконного доступу до них;

3) здійснення періодичної та поточної оцінки ефективності функціонування системи управління персональними даними у базах персональних даних;

4) організацію внесення пропозицій керівництву володільця щодо удосконалення системи управління персональними даними у базах персональних даних;

5) обов'язкову реєстрацію баз персональних даних в Державному реєстрі баз персональних даних;

6) розробку, впровадження та забезпечення належного функціонування системи управління персональними даними;

7) підтримку вимог бізнесу процедурами захисту персональних даних у базах персональних даних;

8) реєстрацію інцидентів в системі управління персональними даними [4].

Аналіз Закону України "Про захист персональних даних" (далі – Закону), в розрізі його впливу на банківську сферу, показав, що саме його прийняття стурбувало гравців ринку фінансових послуг. Дискусії навколо положень Закону поглиблюються, особливо з

наближенням дати введення в дію Закону України “Про внесення змін до деяких законодавчих актів України щодо порушення законодавства про захист персональних даних”. Підтримуючи думки членів Асоціація українських банків та Асоціації “Український Кредитно-Банківський Союз” слід звернути увагу на те, що термінологічний блок Закону не висвітлює низки понять, про які йдеться в документі. Так, не надано визначення поняття, процесу та параметрів проведення ідентифікації, з якою пов’язано ряд напрямків роботи з персональними даними. Трактування персональних даних як відомостей, за якими особу може бути ідентифіковано, є неповним, оскільки принципи ідентифікації не встановлено. Розпливчастим є формулювання ознак третьої особи як суб’єкта відносин по використанню персональних даних, оскільки тісно перетинається з визначенням альтернативного розпорядника даних. Проголошені вимоги Закону щодо роботи з персональними даними в деяких напрямках докорінно деформують встановлені процедури інформаційної діяльності банків. При цьому з посиланням на вимоги Закону “Про захист персональних даних” банки позбавлені можливості здійснювати стосовно клієнта маркетингові та інші ініціативні активності, якщо така мета обробки персональних даних клієнта не визначена в договорі [6; 7]. Тому, суперечливі неузгоджені положення чинних законодавчих актів викликають ускладнення та унеможливлюють інформаційну, в тому числі і маркетингову діяльність банківських установ.

Встановлено, що система захисту персональних даних в банківській сфері являє собою в єдності й погодженості сукупність правових норм та інститутів, спрямованих на забезпечення захисту персональних даних при здійснення банківської діяльності та повинна включати наступні елементи – отримання згоди суб’єкта персональних даних, реєстрацію баз персональних даних, заходи щодо захисту персональних даних у відповідності до Типового порядку обробки персональних даних у базах персональних даних та ін.

Продовжуючи дослідження системи захисту персональних даних в банківській сфері, на нашу думку, доцільно було б розглянути Проект Рекомендації щодо забезпечення захисту персональних даних у базах персональних даних від незаконної обробки, а також від незаконного доступу до них (далі – Проект Рекомендацій) [8]. Відповідно до положень вищезазначеного проекту саме банк, як володілець бази персональних даних, повинен створювати умови для захисту персональних даних та забезпечувати захист цих персональних даних від незаконної обробки, а також від незаконного доступу до них. У кожному випадку банк може провести детальний аналіз загроз та інших факторів, які впливають на рівень ризику. На основі аналізу ризиків він має вирішити, який рівень захищеності бази персональних даних є необхідним для створення умов щодо захисту персональних даних. Забезпечення банком умов для захисту персональних даних у базах персональних даних є постійним процесом, який зазвичай має включати:

- розробку політики захисту персональних даних від незаконної обробки, а також від незаконного доступу до них, виходячи з характеристик діяльності організації, цілей, процесів та процедур, суттєвих для управління ризиком небажаних подій щодо обробки персональних даних з урахуванням серйозності наслідків таких небажаних подій;
- впровадження політики захисту персональних даних від незаконної обробки, а також від незаконного доступу до них та забезпечення функціонування заходів, процесів та процедур захисту персональних даних;
- оцінювання і, за можливості, вимірювання продуктивності процесів захисту персональних даних згідно з прийнятою політикою, цілями і практичним досвідом, підготовка пропозицій щодо коригувальних заходів;
- вживання коригувальних та запобіжних дій щодо захисту персональних даних на підставі результатів внутрішніх перевірок, періодичний перегляд політики захисту персональних даних, постійне удосконалення заходів, процесів та процедур.

Слід відмітити, що такий елемент національного механізму захисту персональних даних як застосування юридичної відповідальності займає особливе місце. Законом України “Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності

за порушення законодавства про захист персональних даних" [9] встановлена адміністративна та кримінальна відповідальність за порушення законодавства в сфері захисту персональних даних, яка виступає в якості примусового засобу реалізації державного управління в сфері захисту персональних даних, як засіб забезпечення охорони прав суб'єктів персональних даних та як засіб застосування санкцій за вчинення адміністративних правопорушень та злочину.

Можливість застосування відповідальності за порушення законодавства в сфері захисту персональних даних стала тією мотивацією та важелем, які прискорюють приведення володільцями баз персональних даних своєї діяльності у відповідність до положень чинних нормативних актів, тим самим створюючи більш надійні умови для реалізації суб'єктами персональних даним свої законних прав в цій сфері.

У відповідності до положень Кодексу України про адміністративні правопорушення, особами, які мають право складати протоколи про адміністративні правопорушення у справах про порушення законодавства у сфері захисту персональних даних є уповноважені на те посадові особи спеціально уповноваженого центрального органу виконавчої влади з питань захисту персональних даних – Державної служби України з питань захисту персональних даних. Проаналізувавши її структуру, ми вважаємо, що фіксація правопорушень у сфері захисту персональних даних буде здійснюватися не досить ефективною, у зв'язку з тим, що ввесь штат працівників даного органу знаходиться в м. Києві, а проводити роботу з виявлення правопорушень необхідно буде здійснювати по всій території України. Саме відсутність територіальних управлінь (підрозділів) Державної служби України з питань захисту персональних даних принаймні в обласних центрах призведе до неефективності виявлення правопорушень і буде виступати передумовою порушення чинного законодавства.

Висновки. Встановлено, що на сьогодні здійснення повного аналізу системи захисту персональних даних в банківській сфері залишається проблематичним. На сьогодні окрім Закону України "Про захист персональних даних" та деяких інших підзаконних актів загального характеру, існує лише один Лист Національного банку України стосовно врегулювання питання захисту персональних даних в банківській сфері, в якому сказано, що порядок обробки персональних даних, які належать до банківської таємниці, затверджується Національним банком України. При чому, Національний банк України лише після ухвалення відповідними органами нормативних актів у сфері захисту персональних даних, у разі потреби, внесе зміни до чинних Правил зберігання, захисту, використання і розкриття банківської таємниці, затверджених Постановою Правління Національного банку України № 267 від 14.07.2006, або затвердить нові. До цього моменту банки повинні забезпечувати зберігання, захист, використання та розкриття банківської таємниці (в тому числі персональних даних) відповідно до чинних Правил. Положення ж вищезазначених Правил щодо зберігання, захисту інформації, що містить банківську таємницю, не охоплюють всіх проблемних питань пов'язаних із захистом персональних даних.

Наголошуємо, що Державною службою України з питань захисту персональних даних спільно з Національним банком України повинно прискоритися вжиття заходів щодо розробки Порядку обробки персональних даних, які належать до банківської таємниці. При цьому розробка професійними банківськими об'єднаннями корпоративних кодексів поведінки з метою забезпечення ефективного захисту прав суб'єктів персональних даних може стати важливим чинником забезпечення дотримання законодавства в банківській сфері.

Список використаних джерел

1. Шалига Т. С. Регулювання порядку роботи з інформацією при банківському дистанційному обслуговуванні / Т. С. Шалига // Проблеми і перспективи розвитку банківської системи України : збірник наукових праць / Державний вищий навчальний заклад "Українська академія банківської справи Національного банку України". – Суми, 2010. – Т. 30. – С. 316–328.

2. Про захист персональних даних : Закон України від 01.06.2010 року № 2297-VI [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2297-17. – Назва з екрана.
3. Data Protection Act 1998 [Electronic resource]. – Access mode: http://www.legislation.gov.uk/ukpga/1998/29/contents. – Title from the screen.
4. Проект Типового порядку обробки персональних даних у базах персональних даних [Електронний ресурс]. – Режим доступу: http://www.zpd.gov.ua/R/indexResources.html. – Назва з екрана.
5. Гетьманцев Д. О. Банківське право України / Д. О. Гетьманцев, Н. Г. Шукліна. – К. : ЦУЛ, 2007. – 344 с.
6. Асоціація українських банків просить Президента накласти вето на Закон "Про захист персональних даних" [Електронний ресурс]. – Режим доступу: http://www.khpg.org/index.php?id=1277073426. – Назва з екрана.
7. Закон про захист персональних даних нівелює банківську таємницю? [Електронний ресурс]. – Режим доступу: http://www.epravda.com.ua/news/2011/02/3/269543/. – Назва з екрана.
8. Проект Рекомендації щодо забезпечення захисту персональних даних у базах персональних даних від незаконної обробки, а також від незаконного доступу до них [Електронний ресурс]. – Режим доступу: http://www.zpd.gov.ua/R/perelik/perelik/0822%202011_IT_security.htm. – Назва з екрана.
9. Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних : Закон України від 02.06.2011 року № 3454-VI [Електронний ресурс]. – Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/ed_2011_06_02/T113454.html. – Назва з екрана.