

ГРАЖДАНСКОЕ ПРАВО И ПРОЦЕСС

УДК 347.121.2

ПІДСТАВИ ЗАХИСТУ ПРАВ СУБ'ЄКТА ПЕРСОНАЛЬНИХ ДАНИХ

Юлія БЄЛОВА,

аспірант кафедри цивільного права та процесу
Хмельницького університету управління та права

АНОТАЦІЯ

У статті проаналізовано питання визначення підстав захисту прав суб'єктів персональних даних. Особливості правової природи персональних даних (як об'єкта цивільних правовідносин) зумовлюють специфіку підстав їх захисту. Сьогодні в науковій літературі достатньо широко обговорюється питання про розширення переліку підстав захисту суб'єктивних цивільних прав. Порушення прав суб'єкта персональних даних може полягати в незаконному ненаданні відомостей про джерела збирання, місцезнаходження своїх персональних даних, мету оброблення, місцезнаходження або місце проживання (перебування) власника чи розпорядника персональних даних; незаконному ненаданні інформації про умови надання доступу до персональних даних, зокрема інформації про третіх осіб, яким передаються його персональні дані; ненаданні інформації про механізм автоматичного оброблення персональних даних; незаконному автоматизованому рішенню, яке має для суб'єкта персональних даних правові наслідки; незаконному неповідомленні суб'єкта персональних даних про дії з персональними даними. Ураховуючи взаємозв'язок права на персональні дані з іншими особистими немайновими правами, слід допустити можливість невизнання та (або) оспарення інших особистих немайнових прав, інформація про які відображається в персональних даних фізичної особи (наприклад, право на ім'я, індивідуальність, особисті папери, зображення тощо).

Ключові слова: персональні дані, «фейк», порушення, способи захисту персональних даних.

GROUNDS FOR PROTECTION RIGHTS OF THE DATA SUBJECT

Yuliia BIELOVA,

Postgraduate Student at the Department of Civil Law and Process
of the Khmelnytsky University of Management and Law

SUMMARY

In the article was analyzed the issue of determining grounds for protection rights of data subject (person). Features of legal nature of personal data as an object of civil legal relationship stipulate specifics of grounds for their protection. Today, the issue of extension the list of grounds for protection of subjective civil rights is widely discussed in the scientific literature. Violation of rights of data subject may consist in: unlawful failure to provide information about sources of compilation, location of his personal data, purpose of its processing, location or place of residence (place of temporary residence) of data subject or manager of personal data; unlawful failure to provide information about conditions for providing access to personal data, in particular information about third parties to whom their personal data are transmitted; failure to provide information about mechanism for automatic processing of personal data; unlawful automated solution, which has legal consequences for data subject; unlawful non-notification of data subject about actions with personal data. Considering the interrelation of right to personal data with other personal non-property rights, should assume possibility of non-recognition and (or) contest of other personal non-property rights, information about whose is displayed in personal data of individual (such as right to a name, individuality, personal papers, image, etc.).

Key words: personal data, "fake", violation, ways of protection personal data.

Постановка проблеми. Ч. 1 ст. 8 Закону України «Про захист персональних даних» проголошує особисті немайнові права на персональні дані непорушними. Ідеться про закріплення принципу непорушності права на персональні дані. Цей принцип є галузевим утіленням принципу непорушності прав і свобод людини (ст. 21 Конституції України). У найбільш загальному розумінні цей принцип означає захист персональних даних від необґрунтованого втручання (як із боку держави, так і з боку інших осіб) та охоплює принаймні два положення. З одного боку, ніхто не може зазнавати протиправного втручання в його право на персональні дані чи обмеження у його здійсненні; з іншого – суб'єкт права на персональні дані може бути обмежений у його здійсненні лише у випадках і в порядку, вста-

новлених законом. ЦК України в ч. 1 ст. 15 зумовлює право на захист суб'єктивного цивільного права, зокрема права на персональні дані, його порушенням чи невизнанням. Розуміння вказаних понять, тобто порушення, невизнання та оспарювання суб'єктивного цивільного права, базується на тому, що усі вони є складниками більш широкого поняття – «підстави захисту суб'єктивного цивільного права» [1, с. 168] (або тріади підстав захисту суб'єктивних цивільних прав [2, с. 182]). Спільним є те, що вони полягають у посяганні на суб'єктивне цивільне право. Під посяганням прийнято розуміти не передбачений законом вплив на суб'єктивне право учасника цивільного обігу, що полягає у запереченні суб'єктивного права уповноваженої особи та виявляється у формах невизнання права, оспарювання

права, порушення права [2, с.189]. Тому підстави захисту суб'єктивних цивільних прав визначають момент, із якого особа (носіїв відповідного суб'єктивного права) має можливість реалізувати своє повноваження щодо захисту вказаного права [3, с.181].

Актуальність теми дослідження. Актуальність дослідження прав суб'єкта персональних даних у системі суб'єктивних цивільних прав зумовлена таким. Розвиток інформаційних технологій сприяв надзвичайному поширенню відносин щодо оброблення персональних даних. Ще ніколи так гостро перед суспільством не стояло питання можливостей зберігання досє на осіб для різних «потреб» і породжених цим ризиків порушення недоторканності приватного життя (з боку як публічних так і приватних установ) за допомогою комплексного використання новітніх технологій.

Стан дослідження. Питання прав суб'єкта персональних даних (як суб'єктивних цивільних прав) неодноразово ставали предметом вітчизняних цивілістичних досліджень, серед яких слід назвати праці таких учених: О.А. Дмитренко, О.В. Кохановської, О.О. Кулінич, О.А. Підпригори, С.О. Сліпченка, І.І. Романюк, Н.В. Устименко, С.В. Шевчука, Р.Б. Шишки та інших учених.

Метою та завданням статті є з'ясування питання визначення підстав захисту прав суб'єктів персональних даних.

Виклад основного матеріалу. У найбільш загальному вигляді ці поняття розкриті, на наш погляд, Ю. В. Білоусовим, який вважає, що під поняттям «порушення» слід розуміти такий стан суб'єктивного права, за якого воно зазнало протиправного впливу з боку правопорушника, внаслідок якого суб'єктивне право зазнало зменшення або знищення; під поняттям «невизнання» – дії учасників цивільного правовідношення, яке несе юридичний обов'язок перед уповноваженою особою, спрямовані на заперечення в цілому або в певній частині суб'єктивного права іншого учасника цивільних правовідносин, внаслідок чого уповноважена особа позбавлена можливості реалізувати своє право; під поняттям «оспорення» – такий стан цивільного правовідношення, за якого між учасниками існує спір щодо наявності чи відсутності суб'єктивного права у сторін, а також приналежності такого права певній особі [4, с. 29]. Указані визначення можна застосувати і до підстав захисту персональних даних.

Очевидним є те, що особливості правової природи персональних даних (з одного боку, як об'єкта цивільних правовідносин, а з іншого – правової природи права на персональні дані (як суб'єктивного цивільного права)) зумовлюють специфіку підстав захисту. Наприклад, О.П. Радкевич класифікує цивільні правопорушення у сфері обігу персональної інформації в мережі Інтернет на такі види: незаконне, свавільне втручання у сферу особистого й приватного життя та його таємниці (збирання, зберігання й розповсюдження інформації конфіденційного характеру); порушення права на таємницю кореспонденції в мережі Інтернет (отримання незаконного доступу до електронної документації); порушення права особи, яку зображено на фотографіях та в інших художніх творах у мережі Інтернет (використання фото, відеоматеріалів із протиправною метою) [5, с. 16]. Незважаючи на те, що така класифікація виконує важливе наукове завдання, вона не володіє ознакою універсальності, а тому не може бути використана для розкриття всієї різноманітності порушень права на персональні дані.

Варто зазначити, що чинне законодавство містить поряд із поняттям «порушення прав суб'єкта персональних даних» пов'язане із ним поняття «порушення законодавства про захист персональних даних» (або схоже, але нетотожне – «порушення вимог Закону України «Про захист

персональних даних»). Так, «порушення законодавства про захист персональних даних» визнаються підставою для застосування суб'єктом персональних даних засобів правового захисту (п. 9 ч. 2 ст. 8 Закону України «Про захист персональних даних»), а також підставою для встановленої відповідальності (ст. 28 Закону України «Про захист персональних даних»). Системний аналіз свідчить, що вказані поняття мають відмінний зміст та обсяг, а тому не є тотожними. «Порушенням законодавства про захист персональних даних» може бути неповідомлення або несвоєчасне повідомлення Уповноваженого Верховної Ради України з прав людини про оброблення персональних даних або про зміну відомостей, які підлягають повідомленню згідно із законом; повідомлення неповних чи недостовірних відомостей; невиконання законних вимог (приписів) Уповноваженого Верховної Ради України з прав людини або визначених ним посадових осіб секретаріату Уповноваженого Верховної Ради України з прав людини щодо запобігання або усунення порушень законодавства про захист персональних даних. Указані «порушення законодавства про захист персональних даних» не завжди будуть призводити до «порушення прав суб'єкта персональних даних». Тобто ці поняття так співвідносяться, як родові та видові, при цьому «порушення прав суб'єкта персональних даних» є видом «порушенням законодавства про захист персональних даних», однак не вичерпує зміст останнього.

Закон України «Про захист персональних даних» називає такі види порушень права на персональні дані, як незаконне оброблення; втрата; знищення; пошкодження; приховування; ненадання чи несвоєчасне надання; надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи (п. 7 ч. 2 ст. 8); незаконне відстрочення або відмова у доступі до персональних даних (ст. 18); незаконний доступ до персональних даних (ч. 1 ст. 24). Системний аналіз Закону дозволяє дійти висновку, що цей перелік не може вважатися повним, оскільки порушення прав суб'єкта персональних даних може також полягати в незаконному ненаданні відомостей про джерела збирання, місцезнаходження персональних даних, мету оброблення, місцезнаходження або місце проживання (перебування) власника чи розпорядника персональних даних; незаконному ненаданні інформації про умови надання доступу до персональних даних, зокрема інформації про третіх осіб, яким передаються його персональні дані; ненаданні інформації про механізм автоматичного оброблення персональних даних; незаконному автоматизованому рішенні, яке має для суб'єкта персональних даних правові наслідки; незаконному неповідомленні суб'єкта персональних даних про дії з персональними даними (зокрема про передавання персональних даних третій особі, а також про зміну, видалення чи знищення персональних даних або обмеження доступу до них). Однак і після цього перелік порушень прав суб'єкта персональних даних не може претендувати на вичерпність.

Найбільш поширеним порушенням права на персональні дані є незаконне оброблення. Порушення права на персональні дані можливе, наприклад, коли журналісти, не запитавши дозволу у відомої особи, знімають подробиці її особистого (інтимного) життя прихованою камерою [6, с. 209]. Оброблення персональних даних є незаконним, коли вона відбувається за відсутності хоч однієї з установлених Законом підстав для її проведення. Способи такого оброблення відрізняються багатоманітністю. Ними є такі: незаконне збирання, зберігання, накопичення, адаптування, зміна, розповсюдження, передавання персональних даних [7, с. 37]. Відповідно до легального визначення, поняття «оброблення персональних даних» розуміється будь-якою дією або сукупністю таких дій, як збирання, реєстрація,

накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передавання), знеособлення, знищення персональних даних, зокрема з використанням інформаційних (автоматизованих) систем (ст. 2 Закону України «Про захист персональних даних»). Крім того, Закон також містить розкриття окремих дій з оброблення персональних даних:

- збирання персональних даних є складником процесу оброблення, що передбачає дії з підбирання чи впорядкування відомостей про фізичну особу (ч. 1 ст. 12);

- накопичення персональних даних передбачає дії щодо поєднання та систематизації відомостей про фізичну особу чи групу фізичних осіб або внесення цих даних до бази персональних даних (ч. 1 ст. 13);

- зберігання персональних даних передбачає дії щодо забезпечення цілісності та відповідного режиму доступу до них (ч. 2 ст. 13);

- використання персональних даних передбачає будь-які дії власника щодо оброблення цих даних, дії щодо захисту, а також дії щодо надання часткового або повного права оброблення персональних даних іншим суб'єктам відносин, пов'язаних із персональними даними (ч. 1 ст. 10);

- поширення персональних даних передбачає дії щодо передавання відомостей про фізичну особу за згодою чи без згоди суб'єкта персональних даних або уповноваженої ним особи лише у випадках, визначених законом, лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту та прав людини (ч. 1, 2 ст. 14).

Таким чином, чинне законодавство не містить визначення поняття «порушення права на персональні дані». Нормативно встановлюються окремі склади порушень прав на персональні дані, які за своєю природою можуть бути як цивільно-правовими, зокрема деліктами, так і публічно-правовими. До останніх належать такі: адміністративне правопорушення (ст. 188-39 Кодексу України про адміністративні правопорушення [8]) – порушення законодавства у сфері захисту персональних даних; злочин (ст. 182 Кримінального кодексу України [9]) – порушення недоторканності приватного життя, зокрема незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації.

Крім того, право на персональні дані може бути порушено в межах трудових правовідносин. Наприклад, якщо працівники суб'єктів відносин, пов'язаних із персональними даними, які здійснюють використання персональних даних відповідно до своїх професійних, службових або трудових обов'язків, допустять розголошення персональних даних, які їм було довірено або які стали відомими у зв'язку з виконанням професійних чи службових або трудових обов'язків.

До винного працівника в такому разі можливе застосування тільки одного з передбачених ч. 1 ст. 147 КЗпП дисциплінарного стягнення – догани. Водночас працівники підприємства (установи, організації), які не забезпечили зберігання персональних даних працівника, можуть бути притягнуті роботодавцем до обмеженої матеріальної відповідальності на підставі ст. 132 КЗпП. Притягнення винного працівника до повної матеріальної відповідальності в такому разі не є можливим, оскільки ст. 134 КЗпП установлений вичерпний перелік випадків повної матеріальної відповідальності працівників [10, с. 252].

Новий підхід щодо цього закріплено в Загальному регламенті про захист даних, який містить легальне визначення поняття «порушення захисту персональних даних» («personal data breach», що також може бути перекладено «витоком персональних даних»). Так, відповідно до п. 12 ч. 1 ст. 4 указанного Регламенту, під порушенням захисту пер-

сональних даних розуміють порушення безпеки, що призводить до випадкового чи незаконного знищення, втрати, пошкодження, несанкціонованого розкриття або доступу до персональних даних, які передано, збережено або оброблено іншим чином. Необхідність запобігання витоку персональних даних пояснюється тим, що якщо витік належним чином і своєчасно не буде усунуто, то це може привести до заподіяння фізичним особам майнової та моральної шкоди, зокрема такої, як втрата контролю над персональними даними або обмеження їх прав, дискримінація, крадіжка ідентифікаційних даних або шахрайство з персональними даними, фінансові втрати, несанкціонована скасування використання псевдонімів, приниження репутації, порушення конфіденційності персональних даних, захищених професійною таємницею, будь-які інші істотні економічні або соціальні втрати для відповідних фізичних осіб.

При цьому види порушень захисту персональних даних можна пояснити таким чином:

- знищення, коли персональні дані більше не існують або не існують у формі, придатній для використання;

- пошкодження, коли персональні дані було змінено, перевернуто чи частково втрачено;

- втрата, коли персональні дані все ще існують, але власник втратив контроль або доступ до них, або персональні дані більше не знаходяться в його володінні;

- несанкціоноване розкриття або доступ, коли розкриття або доступ до персональних даних здійснюється особою, яка не уповноважена на це [11].

Зауважимо, що цей перелік видів порушень захисту персональних даних не може вважатися вичерпним. Усі порушення захисту персональних даних можна поділити на три типи:

- порушення конфіденційності – несанкціоноване або випадкове розкриття чи доступ до персональних даних;

- порушення цілісності – несанкціонована або випадкова зміна, перевернення персональних даних;

- порушення доступності – несанкціоноване або випадкове знищення чи втрата персональних даних.

При цьому необхідно зазначити, що (відповідно до конкретних обставин) порушення захисту персональних даних може одночасно об'єднувати порушення конфіденційності, цілісності та доступності (або будь-яку комбінацію) [11]. Прикладом такого поєднання різних порушень є реєстрація фейкових сторінок у соціальних мережах із використанням персональних даних фізичної особи.

У літературі вказується, що вперше поняття «фейк» стало використовуватися стосовно соціальних мереж, тому воно має два значення. Фейк – це фальшива сторінка сайту або фальшивий сайт, який створений для крадіжки персональних даних, зокрема паролів, які в подальшому будуть використовуватися для розсилки спаму. Друге значення слова пов'язане з підробленим акаунтом, який створюється на будь-якому сайті, де є реєстрація. Фейковий акаунт – це анкета неіснуючої людини або людини без її відома з використанням знову ж її персональних даних. У соціальних мережах досить розповсюджені випадки неправомірної реєстрації акаунта, тобто під іменем особи, але без її відома та без отримання її згоди на це як пересічних фізичних осіб, так і фізичних осіб публічного права [12, с. 288–289]. Прикладом такого порушення є справа бразильського півзахисника донецького футбольного клубу «Шахтар» Жадсона, який подав до суду на соціальну мережу orkut, створену компанією Google, за підроблений профіль в orkut, що нібито належить футболістові. Так, у соціальній мережі orkut є профіль користувача на ім'я Жадсон Родригес. У розділі «про себе» вказано, що профіль належить футболістові «Шахтаря». Сфера інтересів користувача обмежується футболем. Користувач досить активний у соціальній

мережі (у нього 135 друзів). Крім того, він регулярно оновлює розділ «фотографії». Також у соціальній мережі *orkut* є співтовариство, присвячене Жадсону [13].

Щодо інших підстав захисту права на персональні дані, зокрема невизнання та оспорення, то в літературі наводяться такі приклади. Прикладом невизнання права на персональні дані може слугувати ситуація, коли заклад охорони здоров'я може відмовити громадянину у наданні доступу до його медичної карки, не визнаючи його права на доступ до власних персональних даних [6, с. 209]. Право на персональні дані може бути оспорене, наприклад, власником персональних даних, який не надає особі копії певних документів стосовно її родичів із мотивів того, що такі документи не стосуються самої особи або містять конфіденційну інформацію про сторонніх осіб [6, с. 209]. Ураховуючи те, що право на персональні дані є особистим немайновим, яке належить кожній фізичній особі та є невід'ємним, зазначимо, що невизнання чи оспорення не може стосуватися права на персональні дані в цілому. Беручи до уваги охарактеризований вище взаємозв'язок права на персональні дані з іншими особистими немайновими правами, слід допустити можливість невизнання та (або) оспорення інших особистих немайнових прав, інформація про які відображається в персональних даних фізичної особи (право на ім'я, індивідуальність, особисті папери, зображення тощо). Крім того, оспорення може стосуватися самого факту належності персональних даних тій чи іншій фізичній особі, тобто наявності відомостей, які допускають пряму чи опосередковану ідентифікацію фізичної особи.

Сьогодні в науковій літературі достатньо широко обговорюється питання про розширення переліку підстав захисту суб'єктивних цивільних прав. Ґрунтуючись на аналізі чинного законодавства, Р.О. Стефанчук доходить висновку, що підставами цивільно-правового захисту можуть стати ще дві обставини, зокрема зловживання правом (ст. 12, 13 ЦК України), про що ми вже говорили вище, а також наявність небезпеки (ст. 282 ЦК України) та створення загрози життю, здоров'ю, майну фізичної особи або майну юридичної особи (ст. 1163-1165 ЦК України) [120, с. 181]. Твердження про розширення переліку підстав захисту отримувє своє підтвердження і на рівні законодавства про захист персональних даних. Так, п. 7 ч. 2 ст. 8 Закону України «Про захист персональних даних» установлює право суб'єкта персональних даних на захист від випадкової втрати, знищення, пошкодження. А ч. 1 ст. 24 Закону України «Про захист персональних даних» закріплює кореспондуючий обов'язок власників, розпорядників персональних даних та третіх осіб забезпечення захисту цих даних від випадкової втрати або знищення. Ідеться про покладання на власників, розпорядників персональних даних та третіх осіб ризику випадкової втрати, знищення, пошкодження та визнання такого ризику підставою захисту прав суб'єкта персональних даних.

Стосовно цього варто зауважити, що категорія «ризик» не має однозначного розуміння в теорії цивільного права. Одні автори (прихильники теорії «суб'єктивного ризику») вважають, що ризик – це психічне ставлення суб'єктів до результатів власних дій або до поведінки інших осіб, а також до можливого результату об'єктивного випадку і випадкових неможливих дій, які виражають в усвідомленому припущенні негативні, зокрема не відшкодовані майнові наслідки [14, с. 77]. Крім того, в літературі ризик розглядається об'єктивною категорією, тобто можливістю втрати майнові або особисті немайнові блага [15, с. 145], а також можливою небезпекою [16, с.33], не стільки можливою, скільки ймовірною шкодою [17, с.47]. Також можна виділити концепцію двохаспектного ризику, яка ґрунту-

ється на тезі про взаємодію двох концепцій і визначення суб'єктивного ризику поряд із об'єктивним збірною категорією, що поєднує в собі суб'єктивні й об'єктивні елементи [18, с. 81]. Екстраполюючи останню концепцію на предмет нашого дослідження, зазначимо, що ризик випадкової втрати, знищення, пошкодження персональних даних, слід розглядати об'єктивною категорією в розумінні змісту обов'язку забезпечення захисту персональних даних; суб'єктивною категорією в значенні підстави для захисту прав суб'єкта персональних даних.

Необхідність захисту персональних даних від будь-якого несанкціонованого, зокрема випадкового, доступу підтверджується також практикою ЄСПЛ. Для прикладу можна навести справу *I v. Finland* [19]. До Європейського суду звернулася особа, що була хворою на СНІД. Вона проходила лікування у лікарні, де і працювала. У певний момент інформація про діагноз заявниці стала відомою широкому загалу працівників лікарні. Вона звернулася за захистом своїх прав до суду. Їй було відмовлено в задоволенні скарг. Суди визнали, що інформацію було незаконно поширено кимось із працівників лікарні. Однак інформація щодо того, хто міг це зробити, зокрема щодо того, хто переглядав дані заявниці, не зберігалася лікарнею.

У цій справі ЄСПЛ установив, що відсутні твердження стосовно будь-якого навмисного розголошення медичних даних заявниці, що могло б бути втручанням у її право на повагу до приватного життя. Крім того, заявниця не заперечує факту збирання та збереження її медичної інформації. Її скарга стосується неспроможності лікарні гарантувати захист даних заявниці від несанкціонованого доступу, тобто порушення позитивного зобов'язання держави щодо забезпечення поваги до її приватного життя за допомогою впровадження системи правил і гарантій щодо захисту даних. У цьому контексті ЄСПЛ дійшов правового висновку, що для гарантування захисту персональних даних потрібен практичний і ефективний механізм, який би виключив саму можливість будь-якого несанкціонованого доступу.

Покладання на власників, розпорядників персональних даних та третіх осіб ризику випадкової втрати або знищення персональних даних має ще одне значення, зокрема розподіл обов'язку доказування. У цій же справі *I v. Finland* [19] ЄСПЛ установив, що заявниця прогнала цивільну справу через те, що не змогла довести причинно-наслідкового зв'язку між недоліками в правилах безпеки доступу та поширенням інформації про стан її здоров'я. Проте перенесення такого тягаря доказування на заявницю свідчить про ігнорування відомих на той момент недоліків у системі ведення документації в лікарні.

Висновки. Отже, підставами захисту прав суб'єкта персональних даних є посягання на права суб'єкта персональних даних, які охоплюють порушення, зокрема безпеки оброблення персональних даних, що призвело до випадкового чи незаконного знищення, втрати, пошкодження, несанкціонованого розкриття або доступу до персональних даних та спричинило порушення конфіденційності, цілісності та доступності таких даних; невизнання, заперечення в цілому або в певній частині прав суб'єкта персональних даних, внаслідок якого він позбавлений можливості реалізувати свої права; оспорення наявності чи відсутності прав суб'єкта персональних даних, приналежності таких прав певній особі, а також самого факту належності персональних даних тій чи іншій фізичній особі; невизнання та (або) оспорення інших особистих немайнових прав, інформація про які відображається в персональних даних фізичної особи (таких як право на ім'я, індивідуальність, особисті папери, зображення тощо); ризик випадкової втрати, знищення, пошкодження персональних даних.

Список використаної літератури:

1. Цивільний кодекс України від 16 січня 2003 року № 435-IV. URL: <http://zakon5.rada.gov.ua/laws/show/435-15>.
2. Богданов Е.В., Богданов Д.Е., Богданова Е.Е. Развитие гражданского права России. Тенденции, перспективы, проблемы: монография. Москва: ЮНИТИ-ДАНА: Закон и право, 2014. 335 с.
3. Стефанчук Р.О. Захист честі, гідності та репутації в цивільному праві: Монографія. Київ: Науковий світ, 2001. 303 с.
4. Цивільний кодекс України: Науково-практичний коментар (пояснення, тлумачення, рекомендації з використанням позицій вищих судових інстанцій, Міністерства юстиції, науковців, фахівців). Т. 1: Загальні положення / за ред. проф. І.В. Спасибо-Фатєєвої. Харків: ФО-П Колісник А.А., 2010. 320 с.
5. Радкевич О.П. Цивільно-правова охорона і захист персональної інформації в мережі Інтернет: автореф. дис. ... канд. юрид. наук : 12.00.03; Нац. акад. внутр. справ України. Київ: [б. в.], 2014. 20 с.
6. Романюк І.І. Законодавчі та теоретичні підходи до визначення поняття персональних даних та відмежування його від суміжних понять. Актуальні питання публічного та приватного права. 2014. № 1. С. 82–90.
7. Белоусов О.М. Ілюзія дотримання законодавства про захист персональних даних у цифровому середовищі. Юридична Газета. 2013 р. № 14. С. 37.
8. Кодекс України про адміністративні правопорушення від 07.12.1984 № 8073-X URL: <http://zakon3.rada.gov.ua/laws/show/80731-10>.
9. Кримінальний кодекс України від 5 квітня 2001 року № 2341-III. URL: <http://zakon3.rada.gov.ua/laws/show/2341-14>.
10. Чанишев Р.І. Міжнародні стандарти захисту персональних даних працівника і законодавство України. Актуальні проблеми держави і права. 2011. Вип. 57. С. 275–281.
11. Graef I. Putting the right to data portability into a competition law perspective. Law. The Journal of the Higher School of Economics, Annual Review. 2013. P. 53–63.
12. Кулініч О.О. Теоретичні проблеми реалізації та захисту права фізичної особи на власне зображення: дис. ... д-ра юрид. наук : 12.00.03; Нац. ун-т «Одес. юрид. акад.». Одеса: [б. в.], 2017. 488 с.
13. Ухвала Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ у справі № 6-40349св13 від 02 квітня 2014 року. URL: <http://www.reyestr.court.gov.ua/Review/38119227>.
14. Ойгензихт В.А. Проблемы риска в гражданском праве. Душанбе, 1972. 158 с.
15. Красавчиков О.А. Возмещение вреда причиненного источником повышенной опасности. Москва, 1966. С. 164.
16. Малейн Н.С. Вина необходимое условие имущественной ответственности. Сов. государство и право. 1971. № 2. С. 33–36.
17. Мезрин Б.Н. О юридической природе риска в советском гражданском праве. Гражданское право и способы его защиты. Свердловск, 1974. С. 47.
18. Майданик Р.А. Аномалії в цивільному праві України: Навч.-практ. посібник. Київ: Юстініан, 2007. 912 с.
19. Case of Hatton and others v. The United Kingdom, App. No. 36022/97. URL: <http://hudoc.echr.coe.int/eng/?i=001-61188>.

ІНФОРМАЦІЯ ПРО АВТОРА

Белова Юлія Дмитрівна – аспірант кафедри цивільного права та процесу Хмельницького університету управління та права

INFORMATION ABOUT THE AUTHOR

Bielova Yuliia Dmytrivna – Postgraduate Student at the Department of Civil Law and Process of the Khmelnytsky University of Management and Law

jbyelova84@gmail.com