УДК 342.72
DOI: 10.26565/2075-1834-2019-27-07

СЕКТОРАЛЬНИЙ ЗАХИСТ ІНФОРМАЦІЙНОГО ПРАЙВЕСІ В СПОЛУЧЕНИХ ШТАТАХ АМЕРИКИ

Серьогін В. О.,
доктор юридичних наук, професор,
професор кафедри конституційного
і муніципального права
юридичного факультету
Харківського національного
університету імені В.Н. Каразіна,
м. Харків, 61022, майдан Свободи 4,
e-mail: v.a.seryogin@karazin.ua
orcid: https://orcid.org/0000-0002-1973-9310

АНОТАЦІЯ: рівень наукового осмислення досвіду США щодо законодавчого захисту інформаційного прайвесі не відповідає сучасним технологічним, соціально-економічним та політико-правовим викликам, що виникли перед Україною. У статті надано комплексну характеристику чинного законодавства США щодо захисту інформаційного прайвесі у приватному секторі, виокремлено сутнісні риси, які відрізняють підходи американського законодавця в даній сфері від інших, передусім європейських, а також визначено перспективи розвитку американського законодавства з урахуванням новітніх загроз для недоторканності приватного життя, що виникають в умовах бурхливого розвитку інформаційно-комунікаційних технологій.

Відзначено, що американська система захисту інформаційного прайвесі переважно використовує так званий секторальний, або галузевий, підхід. Сутність цього підходу полягає в тому, що захист інформаційного прайвесі здійснюється тільки в рамках конкретного аспекту (контексту) збору або використання інформації і спрямований на заздалегідь певні сектори (галузі) суспільного життя або конкретні групи людей. Відповідно, федеральні закони класифіковані на кілька груп: 1) ті, що захищають прайвесі в сфері фінансів; 2) і, що захищають прайвесі в сфері освіти; 4) і, що захищають прайвесі в сфері охорони здоров'я; 5) ті, що захищають прайвесі дітей; 6) ті, що захищають прайвесі споживачів.

Стверджується, що федеральний секторальний підхід в США має адаптивний характер: Конгрес втручався, щоб регулювати інформаційне прайвесі, коли виникала нова проблема, і в основному це були нові технологічні розробки. Іншими словами, коли нова технологія загрожувала інформаційному прайвесі або, можливо, зростала з неприпустимою швидкістю, Конгрес надавав захист через призму певного сектора або категорії осіб, які найбільше постраждали від цієї нової технології. Досвід США дозволяє чітко розуміти, що захист інформаційного прайвесі і того, що слід вважати чутливим, може швидко змінюватися через зміну в способах збору, обробки та зберігання даних різними суб'єктами.

КЛЮЧОВІ СЛОВА: права людини, право на недоторканність приватного життя, прайвесі, інформаційне прайвесі, законодавство США.

СЕКТОРАЛЬНАЯ ЗАЩИТА ИНФОРМАЦИОННОГО ПРАЙВЕСИ В США

Серегин В. А.,
доктор юридических наук, профессор,
профессор кафедры конституционного
и муниципального права
юридического факультета
Харьковского национального университета
имени В. Н. Каразина,
г. Харьков, 61022, площадь Свободы 4,
e-mail: v.a.seryogin@karazin.ua,
orcid: https://orcid.org/0000-0002-1973-9310

АННОТАЦИЯ: уровень научного осмысления опыта США по законодательной защите информационного прайвеси не соответствует современным технологическим, социально-экономическим и политико-правовым вызовам, возникшим перед Украиной. В статье дана комплексная характеристика действующего законодательства США по защите информационного прайвеси в частном секторе, выделены сущностные черты, отличающие подходы американского законодателя в данной сфере от других, прежде всего европейских, а также определены перспективы развития американского законодательства с учетом новейших угроз для неприкосновенности частной жизни, возникающих в условиях бурного развития информационно-коммуникационных технологий.

Отмечено, что американская система защиты информационного прайвеси преимущественно использует так называемый секторальный, либо отраслевой, подход. Сущность этого подхода заключается в том, что защита информационного прайвеси осуществляется только в рамках конкретного аспекта (контекста) сбора или использования информации и направлена на заранее определенные сектора (отрасли) общественной жизни или

конкретные группы людей. Соответственно, федеральные законы классифицированы на несколько групп: 1) защищающие прайвеси в сфере финансов; 2) защищающие прайвеси в сфере образования; 4) защищающие прайвеси в сфере здравоохранения; 5) защищающие прайвеси детей; 6) защищающие прайвеси потребителей.

Утверждается, что федеральный секторальный подход в США имеет адаптивный характер: Конгресс вмешивался, чтобы регулировать информационное прайвеси, когда возникала новая проблема, и в основном это были новые технологические разработки. Другими словами, когда новая технология угрожала информационному прайвеси или, возможно, росла с недопустимой скоростью, Конгресс предоставлял защиту через призму определенного сектора или категории лиц, наиболее пострадавших от этой новой технологии. Опыт США позволяет четко понимать, что защита информационного прайвеси и того, что следует считать чувствительным, может быстро меняться из-за изменения в способах сбора, обработки и хранения данных различными субъектами.

КЛЮЧЕВЫЕ СЛОВА: права человека, право на неприкосновенность частной жизни, прайвеси, информационное прайвеси, законодательство США.

SECTORAL PROTECTION OF INFORMATION PRIVACY IN THE USA

Seryogin Vitalii,
Professor of Department of Constitutional
and Municipal Law Doctor of Science (Law),
Full Professor,
Kharkiv, 61022, 4 Svoboda Square,
e-mail: v.a.seryogin@karazin.ua,
orcid: https://orcid.org/0000-0002-1973-9310

ANNOTATION: the level of scientific understanding of the US experience in the legal protection of information privacy does not correspond to modern technological, socio-economic, and political and legal challenges that have arisen before Ukraine. The article provides a comprehensive description of the current US legislation on the protection of information privacy in the private sector, highlights the essential features that distinguish the approaches of the American legislator in this field from others, primarily European ones, and also identify prospects for the development of American legislation, taking into account the latest threats to privacy, arising in the conditions of rapid development of information and communication technologies.

The American system of information privacy protection primarily uses the so-called sectoral approach. The essence of this approach is that the protection of information privacy is carried out only within a specific aspect (context) of collecting or using information and is aimed at pre-defined sectors of public life or specific groups of people. Accordingly, federal laws are classified into several groups: 1) protecting privacy in the field of finance; 2) protecting privacy in the field of education; 4) protecting privacy in health care; 5) protecting children privacy; 6) protecting consumer privacy.

The federal sectoral approach in the United States is adaptive in nature: Congress intervened to regulate information privacy when new problems arose, and it was mainly new technological developments. In other words, when a new technology threatened the information privacy or perhaps grew at an unacceptable rate, Congress provided protection through the lens of a certain sector or category of people most affected by this new technology. The US experience makes it possible to clearly understand that the protection of information privacy and what should be considered sensitive can change rapidly due to changes in the way data is collected, processed and stored by various actors.

KEY WORDS: human rights, the right to privacy, privacy, information privacy, US law.

Постановка проблеми. Як відомо, США є «батьківщиною» прайвесі як у доктринальному, так і в політико-правовому плані. Протягом усього XX століття ця країна слугувала прикладом юридичного (передусім судового) захисту прайвесі в умовах ліберально-демократичного режиму і сьогодні залишається в авангарді захисту названого права від новітніх загроз, спричинених науково-технічним прогресом. То ж для України, котра перебуває тільки на початку тривалого шляху розбудови ефективного механізму захисту прав людини, досвід США, попри всі відмінності національних правових систем, є вельми повчальним і корисним. Втім рівень наукового осмислення цього досвіду не відповідає сучасним технологічним, соціально-економічним і політико-правовим викликам, що постали перед Україною.

Стан дослідження. Проблеми юридичного забезпечення права на недоторканність приватного життя вже були предметом наукових досліджень окремих вітчизняних авторів, зокрема Л.В. Ємчук [1], І.В. Михайленко [2], В.С. Сивухіна [3], однак питання забезпечення інформаційного прайвесі в США висвітлювалися в них лише побіжно й уривчасто. Окремі аспекти цієї проблеми були висвітлені й нами, зокрема в межах загальної характеристики конституційно-правового забезпечення прайвесі в США [4, с. 236-247], історії становлення концепції прайвесі в американській правовій теорії та практиці [5] та захисту медичного прайвесі [6]. Однак досі бракує наукових праць, котрі б комплексно висвітлювали сучасну нормативно-правову основу захисту прайвесі в США, передусім щодо інформаційного аспекту цього права.

З урахуванням вищевикладеного, **метою** цієї статті є надання комплексної характеристики чинного законодавства США щодо захисту інформаційного прайвесі у приватному секторі, виокремлення тих сутнісних рис, які відрізняють підходи американського законодавця в даній сфері від інших, передусім

європейських, а також визначення перспектив розвитку американського законодавства з урахуванням новітніх загроз для недоторканності приватного життя, що виникають в умовах бурхливого розвитку інформаційно-комунікаційних технологій. Досягнення поставленої мети забезпечується використанням історико-правового, порівняльно-правового та формально-юридичного методів дослідження.

Виклад основного матеріалу. Розпочинаючи висвітлення теми, варто відзначити, що в минулому Конгрес США доволі чуйно реагував на технологічні винаходи й діджиталізацію (поширення цифрових технологій на дедалі ширші сфери суспільного життя), котрі потенційно загрожували прайвесі. Так, починаючи з 1970-х років Конгрес відреагував на загрози недоторканності приватного життя, розробивши цілу серію федеральних законів, які оберігають прайвесі у тих секторах та аспектах, в яких персональні дані можуть мати більш чутливий характер, а тому потребують кращого захисту. Ці федеральні закони можуть бути класифіковані на декілька груп: 1) ті, що захищають прайвесі у сфері фінансів; 2) ті, що захищають прайвесі у сфері освіти; 4) ті, що захищають прайвесі у сфері охорони здоров'я; 5) ті, що захищають прайвесі дітей; 6) ті, що захищають прайвесі споживачів [7].

У підсумку американська система захисту інформаційного прайвесі здебільшого використовує так званий секторальний, або галузевий, підхід (англ. – sectoral approach). При цьому традиційне для американської правової літератури розуміння інформаційного прайвесі зводиться до захисту права особи здійснювати контроль за своїми персональними даними [8, с. 878-889; 9, с. 1202-1205; 10], хоча таке ототожнення є не зовсім коректним з теоретичної точки зору. На відміну від універсального підходу до захисту прайвесі, прийнятого в багатьох державах світу і наддержавних утвореннях, таких як Європейський Союз, секторальний підхід зазвичай передбачає захист інформаційного прайвесі тільки в межах конкретного аспекту (контексту) збирання чи використання інформації та спрямовується на заздалегідь визначені сектори (галузі) суспільного життя чи конкретні групи.

Водночас варто відзначити, що американська система захисту прайвесі не є повністю секторальною. Право на недоторканність приватного життя було розтлумачене Верховним Судом США як таке, що є «включеним» до Білля про права, особливо до Першої, Третьої, Четвертої та П'ятої поправок [10]. Крім того, окремі штати іноді захищають прайвесі в своїх конституціях чи просто приймають спеціальне законодавство про прайвесі. Наприклад, прайвесі може бути захищене конкретними законами про прайвесі, законами про необхідність сповіщення щодо порушень даних або законами про цивільні правопорушення [11, с. 145-156]. Як на рівні штатів, так і на федеральному рівні прайвесі також певною мірою захищене через визначення порядку використання відповідних засобів і каналів зв'язку, незалежно від потенційної чутливості (вразливості) даних. Система захисту інформаційного прайвесі може включати в себе, зокрема, встановлення правових меж для прослуховування телефонних розмов, порядку доступу до електронних повідомлень, що зберігаються, отримання даних з рукописних джерел тощо. До цієї системи також входить регулювання тих випадків, коли приватним суб'єктам доручається брати участь у проведенні урядових розслідувань чи сприяти їм. Наприклад, Закон про банківську таємницю 1970 року [12] зобов'язує банки та інші фінансові установи консолідувати фінансові дані та звіти, аби допомагати правоохоронним органам у проведенні фінансових розслідувань, а Закон про комунікаційну допомогу в правоохоронній діяльності 1994 року [13] вимагає від провайдерів телекомунікаційних мереж сприяти перехопленню компетентними органами окремих повідомлень та стеженню за спілкуванням абонентів за певних обставин.

В інших випадках недоторканність приватного життя забезпечується через поняття «захист громадськості від втручання уряду» в аспекті того, які саме дані має право збирати держава або як державні органи повинні обробляти отримані дані. Наприклад, Закон про зовнішню розвідку (FISA) 1978 року [14] внормовує питання щодо збирання інформації в процесі розвідувальної діяльності, Закон про захист прайвесі 1980 року [15] встановлює обмеження для уряду щодо незаконного пошуку і вилучення продукції друкованих та інших засобів масової інформації, Закон про захист електронних комунікацій (ECPA) 1986 року [16] регулює відносини щодо зберігання електронної інформації та електронного спостереження. Однак Закон PATRIOT 2001 р. [17] шляхом внесення змін до таких актів, як ECPA і FISA, послабив обмеження щодо збору даних правоохоронними органами за умов боротьби з тероризмом. У результаті, як зазначають американські дослідники К. Бамбергер і Д. Малліган, навіть за наявності нормативного забезпечення, прайвесі «на папері» може суттєво відрізнятися від прайвесі «в реальному житті» [18, с. 260].

Хоча всі вищеназвані форми захисту прайвесі й важливі, однак вони не включені до загальної оцінки захисту прайвесі, викладеної в цій статті. Конституційний захист виключений нами через те, що він не стосується практики приватного сектора [9, с. 879]. Натомість захист права на недоторканність приватного життя на рівні штатів виключений з нашого поля зору, оскільки він є непослідовним і застосовується по-різному залежно від того органу, котрий визначає правову політику штату. Нарешті, збір і зберігання даних в публічних цілях – на відміну від збору і зберігання даних приватними особами – суттєво відрізняється від обробки даних у приватному секторі, а відтак є темою окремого дослідження. Іншими словами, у цій статті основна увага приділяється секторальному захисту прайвесі, тобто

федеральному захисту недоторканності приватного життя, що застосовується в приватному секторі.

Аби краще зрозуміти секторальне прайвесі, ми повинні спочатку розглянути його, розкласти на частини та проаналізувати кожну з них. Таким чином, ми зосереджуємо увагу на секторальному прайвесі в рамках федеральних законів, які стосуються приватних осіб і поділяються на п'ять категорій: фінансове прайвесі, прайвесі у сфері освіти, прайвесі у сфері охорони здоров'я, дитяче прайвесі та прайвесі споживачів.

Перша категорія – це фінансове прайвесі, коли фінансова інформація піддається за певних обставин федеральному захисту.

Передусім слід відзначити, що з точки зору ліберально-демократичного підходу, що панує в США, фінансовий стан особи, у тому числі розмір її доходів і видатків, кредитна історія тощо, є невід'ємною складовою її приватного життя, а відтак підлягає втаємниченню і захисту від сторонніх очей, є вільним від правового регулювання. Однак у другій половині XX століття ситуація суттєво змінилася: стало зрозуміло, що для забезпечення фінансового прайвесі без державного регулювання вже не обійтися.

Першим федеральним законом, який врегулював приватне використання й поширення інформації, став Закон про чесну кредитну звітність (FCRA) 1970 року [19]. За загальним правилом, FCRA регулює порядок використання кредитних звітів. Він визначає порядок збору, ведення і поширення «звітів споживачів» і вимагає, щоб агентства зі звітності споживачів дотримувались певних процедур для забезпечення «максимально можливої акуратності». Це положення було законодавчо закріплене з міркувань забезпечення інформаційного прайвесі в аспекті видалення, вторинного використання і розкриття даних, зібраних кредитними бюро. По суті, FCRA покладає на агентства обов'язки щодо інформування споживачів і надає приватним особам певні права щодо контролю над особистими фінансовими записами, котрі зберігаються компаніями, що надають кредитні звіти, наприклад, право запитувати копію свого кредитного звіту.

Слід зауважити, що до FCRA було внесено чимало поправок. Зокрема, Закон про чесні й точні кредитні операції (FACTA) 2003 року, прийнятий з метою попередження крадіжок персональних даних і підвищення точності кредитних рейтингів, вимагає від агентств кредитної звітності надавати споживачам щорічний кредитний звіт [20].

Фінансові дані були додатково внормовані в 1978 році з прийняттям Закону про право на фінансове прайвесі (RFPA) [21]. RFPA встановлює обмеження на розкриття фінансових документів фінансовими установами органам державної влади без судового ордера чи повістки. За несанкціоноване розкриття даних, що становлять фінансове прайвесі споживача, фінансова установа чи будь-який інший державний орган, який отримав фінансові звіти внаслідок порушення закону, підлягає цивільно-правовій відповідальності.

Крім того, до нормативно-правової основи фінансового прайвесі у США можна також включити Закон про модернізацію фінансових послуг 1999 року, також відомий як Закон Гремм-Ліч-Блайлі (GLBA) [22]. Хоча GLBA не завжди має пряме відношення до фінансових даних, він, як правило, регулює обробку персональної інформації фінансовими установами, зокрема їх діяльність щодо збору, використання і розкриття фінансової інформації, котра дозволяє ідентифікувати особу. За деякими винятками, GLBA зобов'язує установи, котрі надають фінансові послуги, захищати дані про своїх клієнтів, повідомляти споживачів і запитувати їх попередню згоду на передачу таких даних третім особам, а також розкривати свої методи забезпечення прайвесі.

Друга категорія – це прайвесі у сфері освіти, що забезпечує додатковий правовий захист персональних даних студентів. Ключовим джерелом права у даній сфері є Закон про сімейні освітні права та прайвесі (FERPA) 1974 року [23]. FERPA захищає конфіденційність освітніх записів, регулюючи доступ до навчальних реєстрів, персональних даних студентів, а також іншої інформації, що зберігається в навчальних закладах, зокрема такої, як медичні записи, психологічні оцінки та додаткова інформація, безпосередньо пов'язана зі студентом. За деякими винятками, студент або його чи її батьки повинні надати згоду, перш ніж навчальний заклад зможе передати особисту інформацію третім особам. FERPA також надає батькам і студентам право на доступ до своїх файлів, аби вони мали змогу оскаржувати неправдиву чи шкідливу інформацію, що міститься в них.

Примітним є те, що сфера прайвесі в освіті на федеральному рівні досить обмежена. FERPA застосовується тільки до тих навчальних закладів та установ, які отримують федеральні бюджетні кошти від Міністерства освіти США. Незважаючи на обмежену сферу застосування, така форма законодавчого регулювання має досить чітке обґрунтування. FERPA прагне захистити конфіденційність певних записів, накопичених у навчальному закладі, котрі можуть вважатися частиною інформаційного прайвесі студентів. Це пов'язано з тим, що навчальні заклади в процесі виконання своїх функцій збирають інформацію про своїх студентів, яка може бути дуже чутливою.

Третя категорія – це прайвесі у сфері охорони здоров'я, де медична інформація заслуговує більш суворого захисту даних. Вперше на федеральному рівні визнання важливості даних про стан здоров'я було включено до Закону про свободу інформації (FOIA) 1966 року [24]. Цей закон виключає публічний

доступ до урядових записів для «кадрових и медичних карт і подібних файлів, розкриття яких являтиме собою явно необґрунтоване втручання в особисте прайвесі» та «записів чи інформації, що зібрані для правоохоронних цілей… котрі за розумним очікуванням являтимуть собою необґрунтоване втручання в особисте прайвесі».

Усвідомлюючи необхідність оцифрування медичної інформації та забезпечення акуратності при її передачі, Конгрес розвинув ідеї FOIA в нових законодавчих актах. Так, Закон про мобільність і підзвітність медичного страхування (HIPAA) 1996 року [25] регулює конфіденційність медичних записів, уповноважуючи Міністерство охорони здоров'я та соціальних служб (HHS) оприлюднити правила про те, як штати повинні захищати конфіденційність певної медичної інформації. На виконання цих вимог у 2003 році HHS прийняло Правила HIPAA щодо прайвесі [26] – стандарти конфіденційності ідентифікуючої особу медичної інформації, які набули чинності в квітні 2005 року. Ці стандарти стосуються використання і розкриття інформації про стан здоров'я фізичних осіб (так званої «захищеної інформації про здоров'я») усіма організаціями, що підпадають під дію HIPAA (так званими «суб'єктами, охопленими страхуванням») і вимагають від них виконання певних заходів щодо забезпечення конфіденційності та безпеки, а також інформування пацієнтів в разі, коли конфіденційність і безпека їхніх персональних даних перебувають під загрозою.

Законодавство про прайвесі у сфері охорони здоров'я було суттєво оновлено в 2008 році: мається на увазі Закон про недопущення дискримінації в галузі генетичної інформації (GINA) [27]. GINA регулює використання інформації щодо генетичної схильності до хвороб у межах групових планів охорони здоров'я та страхування здоров'я при прийнятті рішень про покриття чи встановлення страхових внесків. Він також обмежує використання генетичної інформації роботодавцями при прийнятті кадрових рішень щодо їхніх працівників.

Стосовно медичного страхування, частина I Закону GINA:

1) забороняє дискримінацію в плані страхових виплат чи внесків при груповому страхуванні на основі генетичної інформації;

2) забороняє використання генетичної інформації в якості підстави при визначенні права на участь у програмі медичного страхування чи при встановленні страхових виплат на ринках індивідуального і додаткового до програми Medicare (Medigap) страхування;

3) обмежує можливості організацій, котрі видають групові плани медичного страхування і страхові поліси, а також емітентів полісів Medigap, щодо збору генетичної інформації та в праві просити/вимагати від фізичних осіб проходження генетичного тестування.

Натомість частина II Закону GINA забороняє використання генетичної інформації в контексті трудових відносин і зайнятості, обмежує право роботодавців та інших осіб, які підпадають під дію цього закону, запитувати, вимагати чи набувати генетичну інформацію, і жорстко обмежує можливість розкриття цими особами генетичної інформації.

У зв'язку з необхідністю поліпшення правозастовчої практики та розширення прав пацієнтів, у тому числі щодо генетичного прайвесі, HIPAA був додатково переглянутий у 2009 році згідно із Законом про інформаційні технології у сфері охорони здоров'я для економічного та клінічного здоров'я (HITECH) [28]. Цей Закон розширив повноваження HHS, охопивши своїм регулюванням «ділових партнерів» та всі інші установи та організації, котрі отримують інформацію від організацій, на яких поширюються вимоги HIPAA. Він також додав положення про сповіщення пацієнта про порушення безпеки його медичних даних і значно збільшив штрафи за порушення HIPAA. Остаточну редакцію Правил HIPAA (так звані Правила омнібуса) було видано у 2013році [29].

Тож на сьогодні Правила HIPAA застосовуються до даних про здоров'я, якими володіють будь-які охоплені страхуванням суб'єкти та/або їхні ділові партнери. При цьому під даними про здоров'я розуміється будь-яка інформація, включаючи генетичну інформацію, як усна, так і зафіксована в будь-якій формі та на носієві будь-якого виду, яка:

1) створена чи отримана постачальником медичних послуг або медичного страхування, органом охорони здоров'я, роботодавцем, страхувальником життя, інститутом чи університетом або посередником при наданні медичних послуг;

2) стосується минулого, теперішнього чи майбутнього фізичного чи психічного здоров'я або стану фізичної особи; надання медичної допомоги фізичній особі; або минулих, поточних або майбутніх платежів за надання медичної допомоги фізичній особі [30].

Загалом правила HIPAA поділяються на Правила щодо прайвесі (Privacy Rule) та Правила щодо безпеки (Security Rule).

Правила HIPAA щодо прайвесі вимагають більш жорсткого захисту та позитивної згоди пацієнтів на певні види використання фінансових та медичних даних, наприклад, у маркетингу. Ці Правила стосуються виключно захищеної медичної інформації (англ. – protected health information або PHI), яка включає в себе будь-яку «індивідуально ідентифіковану інформацію про здоров'я», включаючи демографічні дані та інформацію, що стосується пацієнта, його медичного минулого та догляду, який він

отримує. Це вимагає, зокрема, анонімізації даних про стан здоров'я шляхом видалення різноманітних типів ідентифікаторів.

Натомість Правила щодо безпеки встановлюють стандарти для захисту PHI в електронній формі, яку організація, чиї послуги покриваються страховкою, створює, отримує, підтримує чи передає. Згідно з HIPAA організації, на які поширюється дія страховки, зобов'язані: призначити співробітника з питань прайвесі; розробити й запровадити політики конфіденційності; забезпечити доступ і використання тільки мінімально необхідної PHI; забезпечити, щоб розкриття PHI пацієнтів відбувалося тільки за їхньої згоди (за деякими винятками); надати пацієнтам набір прав і гарантій безпеки щодо їхньої PHI.

Четверта категорія – це прайвесі дітей. Конгрес визнав важливість захисту недоторканності приватного життя дітей в Інтернеті, прийнявши відповідний закон у 1998 році [31]. Варто відзначити, що Конгрес також прагнув врегулювати вплив на дітей з боку невідповідних матеріалів у Всесвітній Мережі шляхом ухвалення Закону про захист дітей в Інтернеті (Child Online Protection Act , COPA), але в кінцевому рахунку він не витримав обговорення, оскільки на думку багатьох конгресменів, накладав «неприпустимий тягар» на свободу висловлювань.

COPPA регулює використання персональних даних дітей в Інтернеті. Водночас цей закон доповнюється Правилами, виданими Федеральною торговельною комісією, і відомими як Правила COPPA [32]. Обидві форми регулювання застосовуються до постачальників онлайн-послуг (OSP), які орієнтовані на дітей віком до тринадцяти років або свідомо збирають у них персональні дані. Названі документи призначалися для заборони нечесних або обманних дій, спрямованих на отримання персональних даних від дітей і про дітей в Інтернеті, і Федеральна торговельна комісія забезпечує їх дотримання.

Нарешті, *п'ята категорія* – це прайвесі споживачів, адже в деяких випадках дані про споживача можуть сприйматись як високочутливі, відтак їм потрібен більш надійний захист. Одним із прикладів такого роду є захист персональних даних абонентів кабельного зв'язку за Законом про політику в галузі кабельного зв'язку 1984 року (CCPA) [33]. Цей Закон вимагає від кабельних компаній зберігати конфіденційність інформації про кабельних абонентів і вимагає від кабельних операторів інформувати своїх абонентів про збір і використання ідентифікуючої особу інформації, що має збиратися компанією, та про способи розкриття зазначеної інформації. Закон також встановлює конкретні цілі, заради яких оператор кабельного телебачення може розкривати чи використовувати персональні дані.

Іншим прикладом є Закон про захист приватності відео (VPPA) [34]. Ймовірно, VPPA було прийнято у відповідь на випадок з кандидатом на пост судді Верховного суду США Р. Борка, після того як журналісти спробували отримати список історії прокату відеокасет кандидата. VPPA регулює використання інформації про відеопрокат і, як правило, забороняє «постачальникам відеопослуг» розкривати особисту інформацію про своїх клієнтів третій стороні стосовно оренди чи продажу відеоматеріалів. По суті, це обмежує розкриття деякими організаціями форм перегляду відео. Однак у 2013 році до VPPA були внесені поправки у світлі нових послуг оренди відеоматералів, таких як Netflix, і в кінцевому рахунку його захист прайвесі був знижений.

Висновки.

Загалом, секторальний (галузевий) підхід до захисту прайвесі прагне захистити персональні дані в деяких контекстах. Аби зрозуміти, як технологічні інновації можуть поставити під сумнів ефективність такого підходу, його необхідно розбити на частини. Тільки на основі такого розподілу можна краще зрозуміти основні цінності та інтереси, які Конгрес прагнув захистити в рамках секторального підходу до забезпечення інформаційного прайвесі, та їхню актуальність для нових потенційних проблем.

У той час, як чутливість інформації, як правило, важко визначити, увага академічної спільноти сфокусована здебільшого на чотирьох факторах: ймовірність шкоди; можливість шкоди; наявність довірливих відносин; чи відображає ризик побоювання більшості [35, с. 1136]. По суті, обґрунтування законодавчого регулювання тих чи інших питань щодо захисту інформаційного прайвесі за допомогою «секторальних» законів свідчить про те, що Конгрес намагався визначити, які саме дані можуть стати чутливими у певних сферах чи в конкретному контексті; і, можливо, чи зросте ризик шкоди для прайвесі через певний контекст. Як було продемонстровано вище, Конгрес у цілому захищав інформаційне прайвесі за п'ятьма основними категоріями: фінансове прайвесі, прайвесі у сфері освіти, прайвесі у сфері охорони здоров'я, прайвесі дітей та прайвесі споживачів. Ці категорії потенційно представляють певний контекст. Наприклад, персональні дані дітей захищені в режимі онлайн, оскільки вони вважаються категорією осіб, які мають право на особливий догляд і допомогу, а Інтернет створює для них нові ризики. Так само фінансові транзакції, записи про освіту, дані про стан здоров'я та деякі типи даних про споживачів вважаються чутливими для забезпечення захисту, коли ймовірність збереження даних приватними суб'єктами вважається високою через контекст їх збору.

Можна з упевненістю припустити, що Конгрес ніколи прямо не заявляв, що інші типи інформаційного прайвесі не будуть захищені в майбутньому або що немає сенсу захищати ці види інформації поза їх сферою дії, як визначено законодавчими органами. Фактично, однак, існуюча правова

база є досить обмеженою за обсягом. Наприклад, фінансове прайвесі захищається тільки на федеральному рівні, коли відповідна інформація збирається заздалегідь визначеними приватними організаціями – всіма, хто певною мірою пов'язані з фінансовою сферою. Прайвесі у сфері охорони здоров'я захищене в контексті чутливості інформації, наприклад, медичних реєстрів, і психологічної оцінки, які зазвичай збираються захищеними установами – тому це стосується тільки їх. Прайвесі у сфері освіти захищається аналогічним чином, тобто тільки у сфері з високою вірогідністю отримання чутливих даних. Дані про дітей можуть стати чутливими через практику збору даних на веб-сайтах, але це все ще може бути застосовано тільки в Інтернеті – і також обмежене за обсягом. Нарешті, прайвесі споживачів вважається чутливою інформацією тільки у певному контексті в деяких сферах, наприклад, в реєстрах абонентів кабельного телебачення та реєстрах прокату і продажу відеоматеріалів, але не в інших випадках.

Звісно, чутливі дані, які Конгрес прагнув захистити в цілому, можуть збиратися в різних сферах і в інших контекстах, виключених з існуючої нормативно-правової бази. Відповідні дані були захищені тільки в межах певного контексту, котрий суб'єкти формування державної політики щодо інформаційного прайвесі даних прагнули захистити найбільше. По суті, можна стверджувати, що федеральний секторальний підхід у США має адаптивний характер: Конгрес втручався, аби регулювати інформаційне прайвесі, коли виникала нова проблем, і в основному це були нові технологічні розробки. Іншими словами, коли нова технологія загрожувала інформаційному прайвесі або, можливо, зростала з неприпустимою швидкістю, Конгрес надавав захист через призму певного сектора чи категорії осіб, які найбільше постраждали від цієї нової технології. Він визначав контекст, у якому приватне життя людей піддавалося найбільшому ризику, і безпосередньо регулював відповідні сектори.

Звісно, було б помилковим припускати, що захищена інформація стала чутливою тільки в цих секторах або що потенційна шкода для суб'єктів даних була ймовірною тільки в цих контекстах. Просто ризик у відповідних секторах і контекстах сприймався вище, ніж раніше. Ось чому чутливість даних у зв'язку з новими технологічними розробками має постійно залишатися на порядку денному політиків, у тому числі й вітчизняних. Досвід США дає змогу чітко розуміти, що захист інформаційного прайвесі й того, що слід вважати чутливим, може швидко змінюватися через зміни у способах збору, обробки і зберігання даних різноманітними суб'єктами. Іншими словами, треба знаходити правильний спосіб забезпечити баланс між корисністю певних даних про особу та інформаційним прайвесі суб'єктів цих даних.

ЛІТЕРАТУРА

1. Ємчук Л.В. Конституційно-правове регулювання особистого та сімейного життя людини і громадянина: автореф. дис…. канд.. юрид. наук: 12.00.02. Ужгород, 2015. 18 с.
2. Михайленко І.В. Право людини на недоторканність приватного життя: поняття, аспекти, механізм реалізації: Автореф. дис…. канд.. юрид. наук: 12.00.01. Харків, 2014. 20 с.
3. Сивухін В. С. Конституційне право людини і громадянина на невтручання в їх особисте і сімейне життя та його забезпечення органами внутрішніх справ України: дис… канд. юрид. наук: 12.00.02. Київ, 2007. 239 с.
4. Серьогін В.О. Право на недоторканність приватного життя (прайвесі) у конституційно-правовій теорії та практики: монографія. Харків: ФІНН, 2010. 608 с.
5. Серьогін В. О. Прайвесі як право «бути залишеним у спокої». *Право і безпека*. 2010. № 3 (35). С. 6-9.
6. Серьогін В. О. Медичне прайвесі: досвід США. *Від громадянського суспільства – до правової держави*: тези III Міжнар. наук.-практ. конф. (м. Харків, 24 квітня 2008 р.). Харків: Харків. нац. ун-т ім. В.Н. Каразіна, 2008. С. 207-209.
7. Feldman D., Haber E. Measuring and protecting privacy in the always-on era. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3404086.
8. Kang J. Information privacy in cyberspace transactions. *Stanford Law Review*. 1998. Vol. 50. P. 1193-1294.
9. Reidenberg J. R. Privacy wrongs in search of remedies. *Hastings Law Journal*. 2003. Vol. 54. P. 877-898.
10. Solove D. J. A brief history of information privacy law. Proskauer on privacy. PLI, 2016; GWU Law School Public Law Research Paper No. 215. URL: https://ssrn.com/abstract=914271.
11. Solove D. J., Schwartz P.M. Privacy law fundamentals. 4th edition. Portsmouth, NH: International Association of Privacy Professionals (IAPP), 2017. 318 p.
12. Bank Secrecy Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114 (1970).
13. Communications Assistance for Law Enforcement Act of 1994 (CALEA), Pub. L. No. 103-414, 108 Stat. 4279 (1994) (
14. Foreign Intelligence Surveillance Act (FISA) of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978).
15. Privacy Protection Act of 1980, Pub. L. No. 96-440, 94 Stat. 1879 (codified at 42 U.S.C. § 2000aa (2012).
16. Electronic Communications Privacy Act (ECPA) of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510–2522 (2012).
17. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered sections of U.S.C. (2012).
18. Bamberger K. A., Mulligan D. K. Privacy on the Books and on the Ground. *Stanford Law Review.* Vol. 63. 2011.

P. 247-315.
19. Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681.
20. Fair and Accurate Credit Transaction Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (2003).
21. Right to Financial Privacy Act (RFPA), 12 U.S.C. §§ 3401–22.
22. The Financial Services Modernization Act (Gramm-Leach-Bliley) Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 & 15 U.S.C.).
23. Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380, 88 Stat. 57 (1974) (codified as amended at 20 U.S.C. §1232g et seq. (2012)); 34 C.F.R. § 99 (2018).
24. Freedom of Information Act of 1966, Pub. L. No. 90-23, 81 Stat. 54 (1966); 5 U.S.C. § 552 (2012).
25. Health Insurance Portability and Accountability Act (HIPAA) of 1996, 29 U.S.C. § 1181.
26. HIPAA Privacy Rule, 45 C.F.R. (2018).
27. Genetic Information Nondiscrimination Act (GINA) of 2008, Pub. L. No. 110-233, Stat. 881 (2008).
28. Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009, Pub. L. No. 111-5, 123 Stat. 226 (2009) (codified as amended in scattered sections of 42 U.S.C.)
29. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach-Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566, 5566 (Jan. 25, 2013).
30. Храмцовская М. США: Изменения в правилах HIPAA защиты медицинских персональных данных и генетическая информация. URL: http://rusrim.blogspot.com/ 2013/02/hipaa.html.
31. Children's Online Privacy Protection Act (COPPA) of 1998, Pub. L. No. 105-277, Stat. 2681-736 (1998).
32. Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888 (Nov. 3, 1999) (codified at 16 C.F.R. § 312 (2018)).
33. Cable Communications Policy Act of 1984, Pub. L. No. 98-549, 98 Stat. 2779 (1984) (codified at 47 U.S.C. § 551 (2012)).
34. Video Privacy Protection Act Amendments Act of 2012, Pub. L. No. 112-258, 126 Stat. 2414 (2012) (codified at 18 U.S.C. §§ 2710–2711 (2012)).
35. Ohm P. Sensitive Information. *Southern California Law Review.* 2015. Vol. 88. P. 1125-1196.

REFERENCES

1. Єmchuk L.V. Konstitucijno-pravove reguljuvannja osobistogo ta simejnogo zhittja ljudini i gromadjanina: avtoref. dis…. kand.. jurid. nauk: 12.00.02. Uzhgorod, 2015. 18 s.
2. Mihajlenko I.V. Pravo ljudini na nedotorkannist' privatnogo zhittja: ponjattja, aspekti, mehanizm realizacii: Avtoref. dis…. kand.. jurid. nauk: 12.00.01. Harkiv, 2014. 20 s.
3. Sivuhin V. S. Konstitucijne pravo ljudini i gromadjanina na nevtruchannja v їh osobiste i simejne zhittja ta jogo zabezpechennja organami vnutrishnih sprav Ukraïni: dis… kand. jurid. nauk: 12.00.02. Kiïv, 2007. 239 s.
4. Ser'ogin V.O. Pravo na nedotorkannist' privatnogo zhittja (prajvesi) u konstitucijno-pravovij teorii ta praktiki: monografija. Harkiv: FINN, 2010. 608 s.
5. Ser'ogin V. O. Prajvesi jak pravo «buti zalishenim u spokoï». Pravo i bezpeka. 2010. № 3 (35). S. 6-9.
6. Ser'ogin V. O. Medichne prajvesi: dosvid SShA. Vid gromadjans'kogo suspil'stva – do pravovoï derzhavi: tezi III Mizhnar. nauk.-prakt. konf. (m. Harkiv, 24 kvitnja 2008 r.). Harkiv: Harkiv. nac. un-t im. V.N. Karazina, 2008.
7. S. 207-209.
8. Feldman D., Haber E. Measuring and protecting privacy in the always-on era. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3404086.
9. Kang J. Information privacy in cyberspace transactions. Stanford Law Review. 1998. Vol. 50. P. 1193-1294.
10. Reidenberg J. R. Privacy wrongs in search of remedies. Hastings Law Journal. 2003. Vol. 54. P. 877-898.
11. Solove D. J. A brief history of information privacy law. Proskauer on privacy. PLI, 2016; GWU Law School Public Law Research Paper No. 215. URL: https://ssrn.com/abstract=914271.
12. Solove D. J., Schwartz P.M. Privacy law fundamentals. 4th edition. Portsmouth, NH: International Association of Privacy Professionals (IAPP), 2017. 318 p.
13. Bank Secrecy Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114 (1970).
14. Communications Assistance for Law Enforcement Act of 1994 (CALEA), Pub. L. No. 103-414, 108 Stat. 4279 (1994) (Foreign Intelligence Surveillance Act (FISA) of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978).
15. Privacy Protection Act of 1980, Pub. L. No. 96-440, 94 Stat. 1879 (codified at 42 U.S.C. § 2000aa (2012).
16. Electronic Communications Privacy Act (ECPA) of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510–2522 (2012).
17. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered sections of U.S.C. (2012).
18. Bamberger K. A., Mulligan D. K. Privacy on the Books and on the Ground. Stanford Law Review. Vol. 63. 2011. P. 247-315.
19. Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681.
20. Fair and Accurate Credit Transaction Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (2003).
21. Right to Financial Privacy Act (RFPA), 12 U.S.C. §§ 3401–22.
22. The Financial Services Modernization Act (Gramm-Leach-Bliley) Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 & 15 U.S.C.).
23. Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380, 88 Stat. 57 (1974) (codified as amended at 20 U.S.C. §1232g et seq. (2012)); 34 C.F.R. § 99 (2018).

24. Freedom of Information Act of 1966, Pub. L. No. 90-23, 81 Stat. 54 (1966); 5 U.S.C. § 552 (2012).
25. Health Insurance Portability and Accountability Act (HIPAA) of 1996, 29 U.S.C. § 1181.
26. HIPAA Privacy Rule, 45 C.F.R. (2018).
27. Genetic Information Nondiscrimination Act (GINA) of 2008, Pub. L. No. 110-233, Stat. 881 (2008).
28. Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009, Pub. L. No. 111-5, 123 Stat. 226 (2009) (codified as amended in scattered sections of 42 U.S.C.)
29. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach-Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566, 5566 (Jan. 25, 2013).
30. Hramcovskaja M. SShA: Izmenenija v pravilah HIPAA zashhity medicinskih personal'nyh dannyh i geneticheskaja informacija. URL: http://rusrim.blogspot.com/ 2013/02/hipaa.html.
31. Children's Online Privacy Protection Act (COPPA) of 1998, Pub. L. No. 105-277, Stat. 2681-736 (1998).
32. Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888 (Nov. 3, 1999) (codified at 16 C.F.R. § 312 (2018)).
33. Cable Communications Policy Act of 1984, Pub. L. No. 98-549, 98 Stat. 2779 (1984) (codified at 47 U.S.C. § 551 (2012)).
34. Video Privacy Protection Act Amendments Act of 2012, Pub. L. No. 112-258, 126 Stat. 2414 (2012) (codified at 18 U.S.C. §§ 2710–2711 (2012)).
35. Ohm P. Sensitive Information. Southern California Law Review. 2015. Vol. 88. P. 1125-1196.