[https://doi.org/10.52058/2708-7530-2021-7\(13\)-180-190](https://doi.org/10.52058/2708-7530-2021-7(13)-180-190)

УДК: 342.7[351/354.073.533](100)

Білоусов Олександр Сергійович доктор політичних наук, доцент, професор кафедри міжнародних відносин та права Одеського національного політехнічного університету, проспект Шевченко, 1, м. Одеса, 65044, тел.: (067) 484-97-34, e-mail: o.s.bilousov@onu.ua, <https://orcid.org/0000-0003-2535-5505>

МІЖНАРОДНА ПРАКТИКА ПРАВОВОГО ЗАХИСТУ ПРИВАТНОЇ ТА ПУБЛІЧНОЇ ІНФОРМАЦІЇ

Анотація. У статті досліджено сучасну міжнародну практику правового захисту приватної та публічної інформації. Зокрема, здійснено огляд чинного законодавства Європейського Союзу щодо регулювання приватної та публічної інформації. Досліджено законодавчі новації країн-членів ЄС передбачені «Загальним положенням про захист даних (GDPR)» та «Директивою про захист даних для сектору поліції та договірною правосуддя».

Зокрема, удосконалення категоріального апарату, критеріїв згоди на збір даних, систему органів, що здійснюють контроль у сфері обігу даних та розмір штрафних санкцій у випадку їх порушення.

Здійснено огляд чинного законодавства Японії, зокрема Закону про захист особистої інформації, та деяких положень Закону про спам, в частині, що стосується комерційного обігу персональних даних.

Визначено галузеві особливості застосування законодавства у сфері захисту персональних даних в Японії, в тому числі, на прикладі, застосування промислового стандарту якості JIS Q 15001: 2017.

Узагальнено основні підходи до захисту персональної інформації, на прикладі ЄС, США та Японії.

Досліджено систему адміністративних органів покликаних забезпечити контроль та захист обігу персональної інформації в досліджуваних країнах.

Розглянуто систему адміністративних та кримінальних санкцій, що накладаються у цих країнах при порушенні законодавства у сфері захисту персональних даних.

Виокремлено кращий міжнародний досвід правового захисту приватної та публічної інформації та розглянуто можливість його апробації у вітчизняну практику.

В процесі дослідження виявлено загальні тенденції до посилення контролю за використанням приватної та публічної інформації, поширюваної в Інтернеті, а також докладання зусиль з боку урядів країн, щодо підвищення рівня її захисту. Особливо використання приватної інформації в комерційних цілях.

Запропоновано власні підходи до формування політики конфіденційності та захисту публічної та приватної інформації.

Ключові слова: приватна інформація, публічна інформація, правовий захист інформації, кібербезпека, міжнародна практика.

Bilousov Oleksandr Serhiiovych Doctor of Political Sciences, Associate Professor, Professor of the Department of International Relations and Law of Odessa National Polytechnic University, Shevchenko Avenue, 1, Odessa, 65044, tel.: (067) 484-97-34, e-mail: o.s.bilousov@opu.ua, <https://orcid.org/0000-0003-2535-5505>

INTERNATIONAL PRACTICE OF LEGAL PROTECTION OF PRIVATE AND PUBLIC INFORMATION

Abstract. The article examines modern international practice of legal protection of private and public information. In particular, the current legislation of the European Union on the regulation of private and public information was reviewed. The legislative innovations of the EU member states provided for by the General Data Protection Regulation (GDPR) and the Data Protection Directive for the Police and Contractual Justice Sector have been studied.

In particular, the improvement of the categorical apparatus, the criteria for consent to data collection, the system of bodies exercising control in the field of data circulation and the amount of penalties in case of violation.

The current legislation of Japan, in particular the Personal Information Protection Act, and some provisions of the Spam Act have been reviewed in the part concerning the commercial circulation of personal data.

The branch features of application of the legislation in the field of protection of personal data in Japan are defined, including on an example of application of the industrial quality standard JIS Q 15001: 2017.

The main approaches to the protection of personal information are summarized, on the example of the EU, USA and Japan.

The system of administrative bodies designed to ensure control and protection of personal information in the studied countries has been studied.

The system of administrative and criminal sanctions imposed in these countries for violation of legislation in the field of personal data protection is considered.

The best international experience of legal protection of private and public information is singled out and the possibility of its approbation in domestic practice is considered.

The study identified a general trend towards stronger control over the use of private and public information disseminated on the Internet, as well as efforts by governments to increase its protection. Especially the use of private information for commercial purposes.

Own approaches to the formation of privacy policy and protection of public and private information are proposed.

Keywords: private information, public information, legal protection of information, cybersecurity, international practice.

Постановка проблеми. З розвитком е-технологій сучасний світ переживає чергову революцію, на цей раз інформаційну.

На сьогодні значно зросли швидкість поширення інформації, та її обсяги, що потребує від споживачів інформації не лише особливих навиків, щодо її пошуку, обробки, та аналізу, а й знань в галузі персональної кібербезпеки та її правового захисту.

Останнім часом виникають конфлікти, щодо незаконного використання приватної інформації користувачів Інтернет-мережі, зламу персональних сторінок в соціальних мережах та ін., у зв'язку з чим почастишали судові позови та розслідування, щодо виявлених фактів.

При цьому, не менш вразливою сферою, що потребує правового захисту є захист інформаційних баз даних органів публічної влади від незаконного інформаційного впливу, незаконного розповсюдження, копіювання і підміни даних, протиправного збору персональних даних, втручання кібер-злочинців в діяльність світової банківської системи, використання «DDoS-атак» з метою промислового шпигунства і т.д., все вищевикладене змушує світову спільноту розробляти активні заходи щодо попередження та протидії даним тенденціям.

У зв'язку з чим міжнародне гуманітарне право поступово напрацьовує цілу низку нормативних документів покликаних захистити від інформаційних загроз та незаконного поширення приватної інформації про особу власне населення.

Одним із флагманів, щодо правового захисту інформації є країни члени Європейського Союзу, де робота в цьому напрямку розпочалася, ще у 2016 році з здійснення масштабної реформи по захисту даних.

Наразі законодавство України, щодо регулювання та захисту приватної та публічної інформації, поки що перебуває на шляху свого становлення, хоча й орієнтується при цьому на найкращі зразки світової юридичної практики.

Разом з тим, вітчизняне законодавство з захисту даних потребує значного удосконалення, особливо в частині розробки реальних механізмів правового захисту приватної та публічної інформації, що й актуалізує тему нашого дослідження.

Аналіз наукових досліджень та публікацій. Цілком логічним є те, що питання правового захисту публічної та приватної інформації викликають значний науковий інтерес. Так, проблемам адміністративно-правового захисту інформації з обмеженим доступом присвячена стаття вітчизняного науковця, доктора юридичних наук Белєвцева В. В., механізми забезпечення захисту права на доступ до публічної інформації в адміністративному судочинстві досліджує Семяніста С. Л., основам правового захисту персональних даних присвячена публікація Головченко В., співвідношення понять «конференційна інформація», «персональна інформація» та «інформація про особу» визначає Буртник Х.

Дана проблема є предметом численних досліджень світової наукової спільноти, зокрема, Мілда Макена і Елені Коста, які розглядають проблему згоди на обробку персональних даних дітей в країнах-членах ЄС, Соня Лівінгстон, Джон Карр і Жасміну Бірн вивчають питання пов'язані з правами дітей в Інтернеті, Ефрен Діас Діас, аналізує новий «Загальний Регламент Європейського Союзу про захист даних і правові наслідки для установ», Пітер Коу, досліджує

феномен соціальних мереж в контексті їх перетину зі свободою слова і кримінальним законодавством та ін.

Метою статті є аналіз міжнародної практики правового захисту приватної та публічної інформації, на прикладі країн Європейського Союзу, Сполучених штатів Америки та Японії, з огляду перспектив її адаптації на вітчизняній арені.

Виклад основного матеріалу. У 2017-2021 р. р. по світу прокотилася ціла хвиля кібер-злочинів, мішенню для яких стали не тільки звичайні користувачі ПК, а цілі держави, згадаємо хоча б «WanaCrypt0r 2.0» (2017 г.), під вплив яких потрапили комп'ютерні системи Великобританії, В'єтнаму, Німеччини, Іспанії, Італії, Індонезії, Казахстану, Португалії, Туреччини, України, Філіппін і Японії. Або ж вірус «Petya» (2016 г.) і його нова версія, яка знищувала повністю всі дані на ПК, яка виникла в 2017 році і отримала назву «NotPetya».

Набув широкого розголосу і інцидент, який стався у 2018 році пов'язаний з забезпеченням конфіденційності персональних даних користувачів соціальної мережі «Фейсбук», компанією «Cambridge Analytica», в ході передвиборчої агітації кандидата на пост Президента США Дональда Трампа, наслідком якої став допит генерального директора компанії «Facebook» Марка Цукерберга в Конгресі США. [4]

Вже не один рік триває міждержавний конфлікт між США та Росією, де Росію звинувачують у втручанні у виборчий процес США, за допомогою Інтернет-технологій.

Подібні звинувачення США висуває і до уряду Китаю, інкримінуючи йому підтримку приватних фірм по організації кібератак, з метою шпигунства.

В Україні, також, час від часу, спалахують інформаційні приводи пов'язані з незаконним використанням персональних даних. Наприклад, поширення персональних даних користувачів з порталу «Дія», що є надавачем державних послуг, та започаткований в рамках проекту «Держава в смартфоні» [5].

Досліджувана проблема актуалізується ще й тим, що з розвитком інформаційних технологій, в тому числі, поширенням соціальних мереж, відбувається постійний обмін особистою інформацією, доступ до якої можуть отримати не тільки інтернет-провайдери, але і інші суб'єкти при автоматичному зборі даних, чи в разі злому персональних ПК, або зі сторінок в соціальних мережах.

До того ж, в умовах тотального карантину та пришвидшення темпів диджиталізації, у всьому світі значно зросла потреба в е-послугах, їх правому регулюванні, забезпеченні рівномірного доступу до послуг, розширені е-трафіку, удосконаленні логістичного ланцюга доставки послуг до споживача, та виявила цілу низку проблем пов'язану з зростанням шахрайства в Інтернеті, в тому числі з незаконним використанням персональних даних.

Варто зазначити, що більшість провідних країн світу мають власну законодавчу базу покликану забезпечити захист персональних даних інтернет-користувачів, при цьому самі підходи, як у виборі інструментів захисту, так і обсягу прав користувачів, інтернет-провайдерів, та приватних компаній різняться. Так, країни-члени ЄС прирівнюють захист персональних даних до фундаментальних прав людини.

Наприклад, в Японії, гарантується право на конфіденційність, тобто визнається право на недоторканість особистого життя та право не розголошувати власну особисту інформацію, без поважної на це причини, та як наслідок, право контролювати власну особисту інформацію, з чого витікає, що сторонні особи, які мають доступ до особистої інформації інших осіб не повинні порушувати їх особисті права.

В Японії до 2020 року існував різний підхід до правового регулювання особистої інформації та особистої інформації, що знаходиться в адміністративних органах. У квітні 2020 року ця країна стала на шлях уніфікації та застосування єдиного підходу до використання будь-яких персональних даних.[7]

Також, в Японії з 2002 року діє «Закон по боротьбі зі спамом», відповідно до якого маркетингові

електронні листи можуть надсилатися лише тим споживачам, які погодились на їх отримання та самостійно надали їх відправителю власну електронну пошту в письмовій формі.

Закон вимагає надати можливість одержувачеві подібної кореспонденції права відмовитися від неї.

В Японії комерційне придбання маркетингового списку є законним, при цьому продавець повинен отримати згоду осіб, дані яких містяться у даному списку. Продавець даних протягом трьох років повинен вести облік інформації пов'язаної з наданням персональних даних, а покупець даних має бути поінформований про ім'я та адресу продавця, або його представника, а також інформацію про те, яким чином продавець отримав відповідні дані.

Вперше так званий Закон про конфіденційність було прийнято в Сполучених Штатах Америки ще у 1974 році. Закон був орієнтований в першу чергу на захист публічних даних, що зберігаються урядовими установами США, оскільки Конгрес Сполучених Штатів Америки був стурбований потенційними зловживаннями персональними даними.

США не має окремого закону про конфіденційність, як не має єдиного центрального органу з питань захисту відповідних даних.

Наразі в США застосовується так званий «секторальний підхід», який полягає у наявності значної кількості нормативно-правових актів, які надають дуже обмежений спектр механізмів захисту персональних даних в залежності від їх спрямування, наприклад, даних про стан здоров'я людини, даних про дітей та ін.

Наприклад, ще з 1998 року в США діє Закон про захист конфіденційності дітей в мережі Інтернет (COPPA), якій містить чіткі правила для операторів онлайн-послуг, націлених на дитячу аудиторію, що здійснюють збір та зберігання фактичної інформації, і містить персональні дані дитини.

Оскільки при підготовці GDPR розробники частково користувалися досвідом впровадження COPPA, досвід США, може бути корисним в дебатах в країнах-членах ЄС, щодо нових проблем захисту даних, пов'язаних зі згодою дітей на використання персональних даних.

При цьому, за відсутності єдиного федерального закону, щодо конфіденційності даних, кожен з 50 штатів, за бажанням, може прийняти власний, як це було зроблено у випадку із Законом про повідомлення про порушення даних. Так, 35 штатів і Пуерто-Ріко мають власне законодавство, щодо правового регулювання розпорядження даними; 25 штатів мають власний Закон про конфіденційність; 10 штатів мають власний Закон про захист прав споживачів [8].

Наприклад, Закон про захист прав споживачів штату Каліфорнія (ССРА), прийнятий у 2018 році мав на меті поширити захист конфіденційності споживачів в т. ч. і на користувачів Інтернету.

Він застосовується до підприємств, постачальників послуг, які обслуговують підприємства та третіх сторін (які можуть бути приватними особами або організаціями).

ССРА містить положення, відповідно до якого комерційні підприємства штату Каліфорнія повинні негайно реагувати на запити приватних осіб, щодо того, які персональні дані про них збираються та поширюються.

Також, приватні компанії повинні видаляти дані про споживача за його запитом.

Комерційні фірми не мають права продавати інформацію про споживачів (користувачів), без чіткого та помітного їх інформування за допомогою веб-повідомлення, при цьому користувачам мережі Інтернет в обов'язковому порядку надається можливість відмовитися від обробки та поширення їх даних [9].

Таким чином, сьогодні провідні держави світу переглядають та удосконалюють власне законодавство, щодо захисту баз даних. Так, основу нормативно-правового регулювання Європейських країн у сфері правового захисту приватної та публічної інформації становлять: Регламент Європейського Парламенту і Ради (ЄС) «Про захист фізичних осіб при обробці персональних даних» від 27.04.2016 р., 216/679, а також про скасування Директиви 95/46/ЄС (Загальний регламент про захист персональних даних) (далі – Регламент 679) [2]; Конвенція Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» від 28.01.1981 р., зі змінами 1999 р.; Додатковий протокол до конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних від 08.11.2001 р. [3]; Директива 95/66/ЄС «Про обробку персональних даних і захист прав осіб у телекомунікаційному просторі», 1997 р.[1] та ін.

Зокрема, в 2016 році в ЄС було проведено масштабну реформу у сфері захисту даних, а саме було розроблено і затверджено постанову Європейського союзу 2016/679, яка регламентує «Загальний стан речей про захист даних (GDPR)» (дата вступу в дію 25.05.2018 р.) [2] та «Директиву про захист даних для сектора поліції та кримінального правосуддя» (Директива про поліцію) [3].

В «Загальному регламенті про захист персональних даних (далі – GDPR) було розширено категоріальний апарат поняття персональних даних, наприклад, введено поняття: «право на забуття», поняття «псевдоанонімізації»,

«трансграничної передачі даних» та ін. Також, GDPR було конкретизовано критерії, що вважати згодою користувача.

Він же покладає на компанії зобов'язання повідомляти органи із захисту даних (DPAs) про їхню діяльність з обробки даних.

До цього часу на компанії, що здійснюють обробку даних покладалася лише обов'язок записати таку обробку, а дані в DPA надавалися лише за запитом.

Малі та середні підприємства або організації звільнені від цієї вимоги, за винятком чітко регламентованих ситуацій.

З введенням GDPR значно підвищується ефективність правового захисту, зокрема громадяни мають можливість ініціювати колективні претензії за місцем проживання.

При цьому з впровадженням DPAs був значно збільшений розмір штрафних санкцій і заходів по контролю за використанням даних.

Так, при невиконанні закону на компанію накладається штраф до 20 000 000 EUR або до 4% від річного обороту компанії за попередній фінансовий рік, в залежності від того, яка сума є більшою [2].

До моменту запровадження GDPR правозастосування законодавства щодо захисту даних в країнах Європейського Союзу було слабким. Так, з 2010 по 2017 рік у федеральних землях Берліна, Баварії та Гамбурга менше 20 підприємств щорічно підпадали під штрафні санкції за порушення закону про захист даних. Середній розмір штрафу в Берліні склав менше 1800 євро (Баварія: - 3100 євро; Гамбург: - 10000 євро. [6]

Наразі GDPR запроваджено єдиний набір правил який буде застосовуватися до всіх країн-членів ЄС. Держави-члени ЄС створюють незалежний наглядовий орган (SA) для розгляду і розслідування скарг, застосування санкцій за адміністративними правопорушеннями у сфері захисту даних і т.п. (там же).

Діяльність SA в державах-членах ЄС націлена на координацію і взаємодію з іншими SA в рамках співдружності, надання взаємодопомоги та організацію спільних операцій.

У разі, якщо бізнес компанія має більше одного офісу на території країн-членів ЄС, у неї буде один SA, як «провідний орган», заснований за місцем знаходження її «головної установи», де відбуваються основні види обробки даних.

При цьому, ведучий орган буде виступати в якості «універсального магазину» для контролю всієї оброблюваної діяльності цієї компанії у всіх країнах ЄС (статті 46-55 ВВП) [2].

Європейська рада із захисту даних (EDPB) координуватиме SA. EDPB замінить робочу групу із захисту даних (стаття 29) [там же].

Відповідно «Директива про захист даних для сектора поліції та кримінального правосуддя» (далі - Директива) прагне полегшити обмін інформацією, щодо захисту персональних даних та кримінальних правопорушеннях пов'язаних з нею в правоохоронних органах [3].

Також, були встановлені критерії обміну інформацією між національною поліцією та судовими органами, з метою полегшити процеси їх взаємодії, і в кінцевому підсумку, підвищити ефективність їх роботи.

Директива, також уточнює завдання і повноваження DPA, зокрема DPA може накласти тимчасову або постійну заборону на незаконну обробку даних.

До компетенції DPA віднесено також розгляд скарг, поданих контрольованими суб'єктами що, безумовно, потребує від DPA додаткових ресурсів.

Отже, політика щодо забезпечення конфіденційності персональних даних країн-членів Європейського Союзу спрямована в першу чергу на посилення заходів їх захисту та контролю з боку органів влади, а також збільшення штрафних санкцій при її порушенні.

Практика застосування нового законодавства ЄС щодо забезпечення конфіденційності персональних даних має додатковий позитивний ефект, який можна окреслити гаслом «купує європейське».

В США на федеральному рівні повноваженнями з захисту баз даних наділена Федеральна торговельна комісія (FTC).

Саме FTC здатна накласти заборону на недобросовісну та таку, що вводить в оману споживачів торговельну практику, в т.ч. і в мережі Інтернет.

У випадку виявлення відповідних фактів FTC проводить власне розслідування та накладає заборону на використання подібної інформації.

Але, як показує досвід, вже згаданої нами компанії Cambridge Analytica, це жодним чином не заважає подібним компаніям використовувати персональні дані користувачів для розробки недобросовісної реклами, здатної вплинути на вибір користувачів.

В Японії органом, що здійснює контроль та застосування Закону «Про захист персональної інформації» (APPI) є Комітет по захисту особистої інформації (PPC). PPC створено в 2016 році. Крім контролю за дотриманням чинного законодавства Японії в галузі захисту даних, до його компетенції входить і розробка рекомендацій по його застосуванню[7].

До того ж, крім PPC, деякі міністерства Японії розробили власні рекомендації та принципи, що регулюють питання захисту даних, наприклад, керівні принципи по телекомунікації та керівні принципи мовлення видані Міністерством внутрішніх справ та зв'язку Японії, керівні принципи поширення генетичної інформації видані Міністерством економіки, торгівлі та промисловості, керівні принципи поширення фінансової інформації розроблені Агентством з фінансових послуг [там же].

В приватному бізнесі Японії застосовується, так звана «Система знаків конфіденційності» (або «знак конфіденційності») (JIS Q 15001: 2017), яка є промисловим стандартом якості та розроблена японським центром розвитку обробки інформації. Не зважаючи на те, що JIS Q 15001: 2017 не є законом, її застосування продемонструвало досить високий рівень ефективності, а її вимоги, іноді є навіть більш жорсткими ніж вимоги APPI [там же].

Японія, як і ЄС з 2020 року значно збільшила розмір штрафів, за порушення законодавства, у сфері захисту персональних даних.

На сьогодні максимальне покарання передбачене за порушення норм чинного законодавства по боротьбі зі спамом в Японії становить один рік

позбавлення волі, або штраф у розмірі 1 000 000 юанів для фізичних осіб та штраф у розмірі 30 000 000 юанів для юридичних осіб [там же].

За порушення Закону «Про захист персональної інформації» (APPI) максимальне покарання становить один рік позбавлення волі, або ж штраф у розмірі до 1 000 000 юанів для фізичних осіб, та 100 000 000 юанів для юридичних осіб (ст. 83, 87 APPI) [там же].

Висновки. Таким чином, результати аналізу міжнародної практики правозастосування та правового регулювання захисту приватної та публічної інформації в Інтернет-мережі на прикладі країн-членів ЄС, США та Японії, дозволили нам зробити висновок про загальні тенденції до посилення контролю за використанням приватної та публічної інформації, поширюваної в Інтернеті, а також докладання значних зусиль з боку урядів цих країн, щодо підвищення рівня її захисту.

Особливо, це стосується використання приватної інформації в комерційних цілях.

Загальною тенденцією є також підвищення рівня відповідальності набувачів інформації та суворості санкцій, у випадку порушення ними національного законодавства щодо збору, використання та поширення персональних даних.

Також, виявлено тенденцію до впровадження у міжнародну практику права на видалення (США, Японія), яке має стати основоположним принципом законодавства про конфіденційність, з його подальшим розвитком, а саме реалізацією права на «забуття» (ЄС).

На нашу думку, виходячи з міжнародного досвіду захисту персональної та публічної інформації будь-який законодавчий акт, що регулює питання конфіденційності персональних даних має містити наступні права, а саме право доступу, право на видалення, право на виправлення, право інформування (або право на пояснення), право на мобільність та ін.

З метою посилення захисту персональних даних та підвищення рівня безпеки Інтернет-користувачів, їх обробка має бути обмежена конкретними перерахованими цілями, містити чітку згоду користувача на їх обробку та використання даних.

Доцільним вбачається впровадження обов'язку своєчасного інформування користувачів про те, кому, з якою метою та в якому обсязі їхні дані передаються третім особам.

Запровадження практики загального публічного повідомлення користувачів у випадку виявлення правопорушень, як самою компанією, так і по відношенню до неї (у випадку несанкціонованого зламу бази даних).

Крім, того персональні дані, що належать до категорії чутливих даних (sensitive data), мають мати посилений режим захисту та підвищений рівень відповідальності у випадку їх незаконного використання.

В державах зацікавлених у підвищенні рівня кібербезпеки їх громадян на центральному та регіональному рівнях мають бути створені незалежні комісії (агенції, тощо), наділені відповідними повноваженнями та ресурсами, метою діяльності яких є моніторинг, проведення розслідувань та застосування санкцій у випадках виявлення правопорушень у сфері захисту даних.

Перспективним напрямком подальшого дослідження нам видається порівняння чинного законодавства України у сфері захисту даних із законодавством провідних країн, з метою його коригування та удосконалення.

Література:

1. Про обробку персональних даних і захист прав осіб у телекомунікаційному секторі : Директива 97/66/ЄС Європейського Парламенту і Ради від 15.12.97 р. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/994_243
2. Regulation (EU)2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4 May 2016. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (дата звернення 20.04.2021)
3. Directive (EU)2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, 4 May 2016. URL: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=uriserv%3AOJ.L_. 2016. 119. 01.0089.01.ENG (дата звернення 20.04.2021)
4. Facebook запізнився із захистом особистих даних – Цукерберг. URL: <https://www.ukrinform.ua/rubric-technology/2787837-facebook-zapiznivsa-iz-zahistom-osobistih-danih-cukerberg.html> (дата звернення 20.04.2021)
5. Додаток «Дія» звинуватили у «зливі» персональних даних українців. Влада заперечує. URL: <https://www.bbc.com/ukrainian/news-52636988> (дата звернення 20.04.2021)
6. Мартин, Н., Мэйтт, К. (2019). How Data Protection Regulation Affects Startup Innovation. URL: <https://link.springer.com/article/10.1007/s10796-019-09974-2> (last accessed: 25. 04. 2021).
7. Data Protection 2021 / Laws and Regulations / Japan / ICLG. URL: <https://iclg.com/practice-areas/data-protection-laws-and-regulations/japan> (last accessed: 25.04. 2021).
8. United States Data Protection Laws: State-Level Approaches to Privacy Protection. URL: <https://blog.netwrix.com/2019/08/27/data-privacy-laws-by-state-the-u-s-approach-to-privacy-protection/> (last accessed: 25. 05.2021).
9. Complete Guide to Privacy Laws in the. URL:<https://www.varonis.com/blog/us-privacy-laws/>(last accessed: 25. 05.2021).

References:

1. Pro obrobku personalnykh danykh i zakhyst prav osib u telekomunikatsiinomu sektori : Dyrektyva 97/66/IeS Yevropeiskoho Parlamentu i Rady vid 15.12.97 r. [On the processing of personal data and the protection of the rights of individuals in the telecommunications sector: Directive 97/66 / EC of the European Parliament and of the Council of 15.12.97]. zakon.rada.gov.ua. Retrieved from http://zakon4.rada.gov.ua/laws/show/994_243 [in Ukrainian]
2. Regulation (EU)2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4 May 2016. Retrieved from <https://eur-lex.europa.eu/eli/reg/2016/679/oj> [in English].
3. Directive (EU)2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, 4 May 2016. Retrieved from https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=uriserv%3AOJ.L_. 2016. 119. 01.0089.01.ENG [in English].

4. Facebook zapiznyvsia iz zakhystom osobystykh danykh – Tsukerberh. [Facebook is late with the protection of personal data - Zuckerberg.] [www.ukrinform.ua](https://www.ukrinform.ua/rubric-technology/2787837-facebook-zapiznivsa-iz-zahistom-osobistih-danih-cukerberg.html). Retrieved from. <https://www.ukrinform.ua/rubric-technology/2787837-facebook-zapiznivsa-iz-zahistom-osobistih-danih-cukerberg.html> [in Ukrainian].

5. Dodatok «Diia» zvyuvatyly u «zlyvi» personalnykh danykh ukrainsiv. Vlada zaperechuie. [The «Action2 application was accused of «showing» the personal data of Ukrainians.]. www.ukrinform.ua. Retrieved from <https://www.bbc.com/ukrainian/news-52636988> [in Ukrainian].

6. Мартин, Н., Мэтт, К. (2019). How Data Protection Regulation Affects Startup Innovation. Retrieved from <https://link.springer.com/article/10.1007/s10796-019-09974-2> [in English].

7. Data Protection 2021 / Laws and Regulations / Japan / ICLG. Retrieved from <https://iclg.com/practice-areas/data-protection-laws-and-regulations/japan> [in English].

8. United States Data Protection Laws: State-Level Approaches to Privacy Protection. Retrieved from <https://blog.netwrix.com/2019/08/27/data-privacy-laws-by-state-the-u-s-approach-to-privacy-protection/> [in English].

9. Complete Guide to Privacy Laws in the. Retrieved from <https://www.varonis.com/blog/us-privacy-laws/> [in English].