

ДІЯЛЬНІСТЬ ДЕРЖАВНИХ ОРГАНІВ ЩОДО ЗАБЕЗПЕЧЕННЯ ПРАВА ОСОБИ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ

ACTIVITIES OF GOVERNMENT BODIES TO ENSURE THE PERSON'S RIGHT TO INFORMATION SECURITY

Глющик О.М., к.ю.н., доцент,
доцент кафедри адміністративно-правових дисциплін
Львівський державний університет внутрішніх справ

Дідик Н.І., к.ю.н., доцент,
доцент кафедри адміністративного права та адміністративного процесу
Львівський державний університет внутрішніх справ

Стаття присвячена дослідженню із застосуванням комплексного системного аналізу, використанням еволюційного підходу однієї з актуальних теоретико-правових проблем інформаційного й адміністративного права – діяльності державних органів щодо забезпечення права особи на інформаційну безпеку. Агресія Росії щодо України здійснюється не тільки у сфері військового протистояння, але й в інформаційній сфері, тому питання підвищення ефективності забезпечення інформаційної безпеки особи, захист інформаційних прав і права особи на інформаційну безпеку в умовах розвитку цифрових інформаційних технологій є актуальним. Проведено аналіз чинної нормативно-правової бази системи забезпечення інформаційної безпеки України, структури органів державної влади, які беруть участь у зазначеній діяльності з реалізації державної інформаційної політики. Розглянуто напрями діяльності у сфері права особи на інформаційну безпеку Верховної Ради України, Президента України, Кабінету Міністрів України, Міністерства цифрової трансформації України, Служби безпеки України, Державної спеціальної служби спеціального зв'язку та захисту інформації України, Міністерства культури та інформаційної політики і інших центральних органів виконавчої влади щодо розробки й удосконалення нормативно-правової бази та практичної реалізації заходів, спрямованих на забезпечення права людини на інформаційну безпеку. Державні органи з метою забезпечення безпеки можуть взаємодіяти з громадськими об'єднаннями, міжнародними організаціями та громадянами.

У системі органів державної влади найбільшою компетенцією у сфері забезпечення права особи на інформаційну безпеку володіють Міністерство культури та інформаційної політики, Центр стратегічних комунікацій і інформаційної безпеки, Державна служба спеціального зв'язку та захисту інформації України.

Ключові слова: права людини, інформаційна безпека, органи державної влади, забезпечення інформаційної безпеки.

The article is devoted to the study using a comprehensive systems analysis using an evolutionary approach, one of the current theoretical and legal issues of information and administrative law – the activities of government agencies to ensure the right of the individual to information security. Russia's aggression against Ukraine is carried out not only in the field of military confrontation but also in the information sphere, so the issue of improving the effectiveness of information security, protection of information rights and the right to information security in the development of digital information technology is relevant. The analysis of the current regulatory framework of the information security system of Ukraine, the structure of public authorities involved in these activities for the implementation of state information policy. Areas of activity in the field of the right to information security of the Verkhovna Rada of Ukraine, the President of Ukraine, the Cabinet of Ministers of Ukraine, the Ministry of Digital Transformation of Ukraine, the Security Service of Ukraine, the State Special Service for Special Communications and Information Protection of Ukraine, the Ministry of Culture and Information Policy and other central executive bodies on the development and improvement of the regulatory framework and the practical implementation of measures aimed at ensuring the human right to information security. Public authorities can interact with public associations, international organizations and citizens to ensure security.

In the system of public authorities, the Ministry of Culture and Information Policy and the Center for Strategic Communications and Information Security of the State Service for Special Communications and Information Protection of Ukraine have the greatest competence in ensuring the right of a person to information security.

Key words: human rights, information security, public authorities, information provision.

Держава виступає основним суб'єктом забезпечення права особи на інформаційну безпеку. Ця обставина зумовлена наявністю в компетенції відповідних прав і повноважень, спеціальних інститутів, органів і служб, що займаються забезпеченням інформаційної безпеки.

Важливе значення для дослідження діяльності державних органів щодо забезпечення права особи на інформаційну безпеку мали праці В.Б. Авер'янова, В.М. Бевзенка, А.І. Берлача, Ю.П. Битяка, П.В. Діхтєвського, І.С. Гриценка, Р.А. Калужного, О.В. Карасса, Л.С. Кисіль, А.А. Козловського, В.К. Колпакова, О.В. Кузьменко, В.І. Курила, Є.В. Курінного, Р.С. Мельника, В.Я. Настюка, О.І. Остапенка, А.О. Селіванова, О.І. Харитонової, В.В. Цветкова, Я.М. Шевченко, Ю.С. Шемчушенка та інших.

На думку О.Є. Малишка та С.С. Єсімова, політика інформаційної безпеки як суспільне явище має комплексний характер, включаючи внутрішньо- та зовнішньополітичні, економічні, технологічні, військові та інші елементи, тому вимагає комплексного підходу. Діяльність органів державної влади має спрямовуватися на виконання конкретних завдань у цій сфері й об'єднуватися

єдиною метою – створити належні умов для реалізації забезпечення інформаційної безпеки України [1, с. 50].

Доктрина інформаційної безпеки України виділяє як сили забезпечення інформаційної безпеки державні органи, підрозділи та посадових осіб державних органів, органів місцевого самоврядування і юридичних осіб, що вповноважені на вирішення завдань забезпечення інформаційної безпеки.

Одним із завдань державних органів щодо здійснення діяльності в цьому напрямі є забезпечення захисту прав та законних інтересів фізичних і юридичних осіб в інформаційній сфері. Діяльність держави щодо забезпечення права особи на інформаційну безпеку включає правові та організаційно-технічні напрями.

До правових напрямів можна зарахувати запобігання загроз, здійснюваних у вигляді несанкціонованих і неправомірних впливів на інформацію. Це забезпечується правовими заходами: закріпленням за державними органами, посадовими особами правових можливостей на розпорядження інформацією про приватне життя особи у встановлених законом випадках; встановленням право-

вого режиму поводження з персональними даними громадян; наданням громадянину права повідомляти факти про приватне життя у встановлених законом випадках; визначенням правил користування та відкриття особистої інформації, порядку ознайомлення громадян із документами, що стосуються їх особисто; встановленням заходів юридичної відповідальності за вторгнення у приватне життя у вигляді неправомірного використання документів та інформації органами державної влади та управління, фізичними та юридичними особами.

До організаційно-технічних заходів належать розробка та використання інженерно-технічних засобів, впровадження обмежувальних заходів на доступ до об'єктів, пов'язаних зі збереженням інформаційних ресурсів, розробка програмно-апаратних засобів захисту інформації тощо.

Верховна Рада України є органом законодавчого забезпечення інформаційної безпеки. У Законі України «Про національну безпеку України» визначено завдання державних органів щодо розробки нормативного забезпечення інформаційної безпеки – Стратегії інформаційної безпеки [2].

До складу Верховної Ради України входить Комітет із питань гуманітарної та інформаційної політики, метою діяльності якого, зокрема, є державна політика у сфері інформації та інформаційної безпеки (крім питань, що належать до сфери національної безпеки та оборони). Значний вплив на інформаційну безпеку в контексті зменшення негативного інформаційного впливу Росії в умовах збройної агресії справило прийняття Закону України «Про внесення змін до деяких законів України щодо забезпечення прозорості власності провайдерів програмної послуги багатоканальних цифрових ефірних телемереж із загальнонаціональним покриттям» [3].

Зазначені зміни містять заходи, спрямовані на протидію використанню на території держави інформаційних систем, що дозволяють користувачам отримати доступ до тих сайтів в Інтернеті, які були визнані невідповідними законодавству України.

Значний внесок у забезпечення інформаційної безпеки робить Президент України, який є гарантом прав і свобод людини та громадянина. Президент України у сфері забезпечення безпеки визначає основні напрями державної політики у сфері забезпечення безпеки, зокрема інформаційної.

Серед стратегічних напрямів України на перспективу зазначені вдосконалення нормативної бази відповідно до вимог Європейського Союзу в контексті реалізації Угоди про асоціацію України та ЄС, цифровізації національної економіки, розвиток кібербезпеки, формування цифрових платформ, сумісних з європейським інформаційним простором, впровадження мереж п'ятого покоління та технологій зв'язку, Інтернету речей [4, с. 2025].

Ці заходи є актуальними щодо питань забезпечення права особи на інформаційну безпеку, оскільки передбачають вдосконалення способів захисту персональних даних від несанкціонованих впливів, розширюють можливості особи використовувати переваги інформаційного суспільства.

До повноважень Президента України належать затвердження стратегічних та концептуальних документів щодо сфери забезпечення права особи на інформаційну безпеку, видання указів та розпоряджень у цій сфері.

Президент очолює Раду національної безпеки і оборони України, в складі якої функціонує Служба з питань інформаційної безпеки та кібербезпеки. Служба здійснює аналіз інформації про стан інформаційної безпеки України та підготовку пропозицій щодо вдосконалення діяльності органів публічної влади в розглянутій сфері, прогнозування, виявлення та оцінку загроз інформаційній безпеці та їх джерел, підготовку пропозицій та рекомендацій щодо запобігання виявленим та недопущенню прогнозованих загроз у сфері інформаційної безпеки [5].

У проєктах законів про внесення змін у Закон України «Про санкції» передбачається надання повноважень Раді

національної безпеки і оборони України у сфері застосування санкцій щодо фізичних і юридичних осіб, які завдають шкоду національній безпеці та її складникам, у тому числі інформаційному [6].

Повноваження Кабінету Міністрів України у сфері забезпечення права особи на інформаційну безпеку полягають у розробці цільових програм, виділенні фінансових коштів на реалізацію, координації діяльності органів виконавчої влади та місцевих органів виконавчої влади, прийнятті постанов та розпоряджень та контролі за виконанням, здійсненні заходів із запобігання загроз інформаційній безпеці та організаційному забезпеченню цієї діяльності.

Великі повноваження у сфері забезпечення інформаційної безпеки мають органи виконавчої влади України, а саме: Служба безпеки, Міністерство внутрішніх справ (далі – МВС), Державна служба з технічного та експортного контролю, Державна служба спеціального зв'язку та захисту інформації (далі – Держспецзв'язок), Міністерство цифрової трансформації.

У Законі «Про Службу безпеки України» забезпечення інформаційної безпеки регулюється окремою статтею. Повноваження Служби безпеки у сфері інформаційної безпеки здійснюються в процесі формування та реалізації державної і науково-технічної політики в зазначеній сфері щодо використання інженерно-технічних та криптографічних засобів захисту державної таємниці [7].

Держава гарантує дотримання прав і свобод людини та громадянина під час здійснення діяльності органами Служби безпеки. Отримані в процесі її діяльності відомості про приватне життя, що зачіпають честь і гідність громадянина чи здатні зашкодити законним інтересам, Служба безпеки не має права надавати інформацію без добровільної згоди громадянина, крім випадків, передбачених законами.

Згідно з Положеннями про Міністерство внутрішніх справ України, воно в межах повноважень забезпечує захист прав та свобод людини та громадянина в інформаційній сфері, захист відомостей, що становлять державну та іншу таємницю, що охороняється законом у системі МВС України, організацію попередження, виявлення, припинення, розкриття та розслідування кримінальних правопорушень, попередження та припинення адміністративних правопорушень, що вчиняються в інформаційній сфері [8].

У вирішенні питань забезпечення права особи на інформаційну безпеку беруть участь усі структурні підрозділи Міністерства внутрішніх справ у межах компетенції. Додатково для реалізації цих завдань створено спеціальні підрозділи, Департамент кіберполіції Національної поліції України.

Серед повноважень кіберполіції – припинення протиправних дій в інформаційно-комунікаційних мережах, включаючи мережу Інтернет, боротьба з кримінальними правопорушеннями у сфері комп'ютерної інформації, протидія міжнародним злочинам у сфері інформаційних технологій, міжнародне співробітництво у сфері боротьби з правопорушеннями, що скоєні з використанням інформаційних технологій.

МВС України здійснює підготовку спеціалістів у галузі забезпечення інформаційної безпеки. У Харківському державному університеті внутрішніх справ функціонує факультет кібербезпеки, ведеться підготовка поліцейських у сфері інформаційних технологій у правоохоронній сфері і в інших університетах зі специфічними умовами навчання.

Технічними питаннями забезпечення інформаційної безпеки займається Державна служба з технічного та експортного контролю України.

Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язок) здійснює забезпечення криптографічними й інженерно-технічними методами безпеки інформаційно-комунікаційних систем,

мереж зв'язку спеціального призначення, забезпечує передачу шифрованої інформації в Україну та установи, що перебувають за її межами.

Міністерство цифрової трансформації України функціонує з 18 вересня 2019 року і є головним органом, що забезпечує формування і реалізацію державної політики у сферах цифровізації, цифрового розвитку, цифрової економіки, цифрових інновацій та технологій, електронного урядування та електронної демократії, розвитку інформаційного суспільства, інформатизації, розвитку цифрових навичок і цифрових прав громадян, відкритих даних, розвитку національних електронних інформаційних ресурсів, розвитку інфраструктури широкопasmового доступу до Інтернету та телекомунікацій, електронної комерції та бізнесу, електронних довірчих послуг і електронної ідентифікації, розвитку та функціонування правового режиму Дія Сіті [9].

Основний вектор діяльності міністерства спрямований на цифровий розвиток, переведення більшості адміністративних послуг в електронну форму, регулювання цифрової економіки, вироблення та реалізацію державної політики, нормативно-правове регулювання у сфері обробки персональних даних, інформаційних технологій (включаючи використання інформаційних технологій під час формування державних інформаційних ресурсів та забезпечення доступу до них), формування єдиного інтерфейсу та стандарту роботи електронних сервісів для дистанційного отримання адміністративних послуг громадянами, функції розвитку національної IT-інфраструктури. Діяльність міністерства зв'язана із забезпеченням інформаційних прав людини та інформаційної безпеки.

Координатором реалізації державної політики у сфері права людини на інформаційну безпеку виступає Міністерство культури та інформаційної політики України [10]. Міністерство забезпечує координацію діяльності державних і місцевих органів, громадських організацій у сфері інформаційної безпеки. При Міністерстві створено Центр стратегічних комунікацій та інформаційної безпеки, який почав діяти у березні 2021 року. Робота Центру сфокусована на протидії зовнішнім загрозам, об'єднанні зусиль держави та громадських організацій у боротьбі з дезінформацією, оперативному реагуванні на фейки, а також на промоцію українських наративів; він здійснює контроль у сфері функціонування засобів масової інформації, зокрема електронних.

У 2017 році було прийнято рішення про блокування сайтів, які публікують інформацію, що спрямована на пропаганду війни, розпалювання національної, расової чи релігійної ненависті та ворожнечі, спонукає дітей до здійснення дій, що становлять загрозу життю та здоров'ю, в тому числі до заподіяння шкоди своєму здоров'ю, самогубству, посягає на територіальну цілісність та суверенітет України.

У разі порушення Закону України «Про внесення змін до деяких законодавчих актів України щодо імплементації Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства (Ланцаротської конвенції)», якщо власник сайту не вживатиме необхідних заходів для видалення забороненої інформації, доступ до нього буде заблоковано. Ці заходи є цілком виправданими та сприяють забезпеченню права особи на інформаційну безпеку, оскільки спрямовані на захист від негативного впливу забороненої інформації [11].

Особлива увага приділяється питанням безпеки дітей і громадян у мережі Інтернет. У зв'язку з цим пропонується внесення змін до законодавства, а саме розширення повноважень Держспецзв'язку щодо блокування сайтів у разі встановлення даних про використання мережі Інтернет із метою схилення до самогубства або скоєння іншого правопорушення.

Діяльність із забезпечення права особи на інформаційну безпеку здійснюють місцеві органи влади в межах

повноважень. Вони розробляють та приймають правові акти у сфері забезпечення інформаційної безпеки в межах предметів відання, забезпечують дотримання законодавства України у сфері забезпечення інформаційної безпеки на території підвідомчих суб'єктів.

Крім виконавчої та законодавчої влади, в питаннях забезпечення інформаційної безпеки бере активну участь судовою владою шляхом реалізації правосуддя в разі протидії загрозам інформаційної безпеки особи. Ця діяльність є невід'ємною складовою частиною забезпечення інформаційної безпеки, оскільки дає змогу реалізувати конституційне право на об'єктивний розгляд обставин, пов'язаних із реалізацією інформаційних прав.

Судовий захист у формі правосуддя – це найвищий рівень юридичного забезпечення прав і свободи громадян. Захисна функція суду у сфері забезпечення права особи на інформаційну безпеку полягає в попередженні порушень права особи на інформаційну безпеку, відновленні порушених прав, свобод та законних інтересів громадян, відшкодуванні збитків та моральної шкоди, заподіяної громадянину, вирішенні питання про відповідальність за порушення прав громадянина у сфері інформації.

Органи судової влади беруть участь у забезпеченні права особи на інформаційну безпеку шляхом здійснення правосуддя в справах щодо відновлення або підтвердження порушеного права, перевірки законності і обґрунтованості індивідуальних правових актів та дій посадових осіб, державних органів із метою забезпечення права особи на інформаційну безпеку.

До цього напрямку діяльності судових органів варто зарахувати тлумачення норм законодавства, за допомогою чого забезпечується державно-правова оцінка відповідних сфер соціальної дійсності, розвиток змісту самих норм законодавства без зміни тексту відповідних статей.

Розгляд Конституційним Судом України питань щодо конституційності положень нормативно-правових актів, що стосуються забезпечення права особи на інформаційну безпеку та вироблення на основі розгляду конкретних справ рекомендацій законодавцю щодо вдосконалення правового забезпечення зазначеної сфери, є важливим напрямом забезпечення права особи на інформаційну безпеку [12]. Система правосуддя має в розпорядженні комплекс заходів, спрямованих на захист права особи на інформаційну безпеку.

Система правосуддя зацікавлена в забезпеченні інформаційної безпеки, оскільки активно використовує в діяльності сучасні інформаційні технології.

Нині в стадії розвитку знаходиться електронне правосуддя, під яким розуміється сукупність різних автоматизованих інформаційних систем, що становлять кошти для публікації судових актів, ведення електронної справи та доступу сторін до матеріалів такої справи.

Забезпечення інформаційної безпеки особи здійснюється не лише органами законодавчої, виконавчої та судової влади. Забезпечення права особи на інформаційну безпеку знаходить своє відображення в діяльності Уповноваженого Верховної Ради України з прав людини.

Уповноважений Верховної Ради України з прав людини бере активну участь у забезпеченні інформаційної безпеки громадян. У щорічній доповіді Уповноваженого за 2020 рік проблему прав людини в контексті забезпечення інформаційної безпеки відображено у розділах 1 «Особисті права і свободи» та 2 «Громадянські та політичні права» [13].

Підкреслено значення превентивних заходів забезпечення інформаційної безпеки. Однак в доповіді за 2020 рік цей напрям не розглядається комплексно, а знаходить відображення як аспект під час розгляду інших прав. Наприклад, у процесі розгляду права на свободу совісті та віросповідання зазначається, що значна частина звернень стосується електронної ідентифікації особи, обліку та обробки персональних даних віруючих.

Громадянські права, до яких належать права на особисту та сімейну таємницю, особисту свободу та недоторканність, посідають третє місце в рейтингу, випереджаючи економічні та політичні права. Зростає кількість порушень прав, серед яких зазначаються звернення щодо порушення свободи інформації. У структурі політичних прав виділяються звернення щодо реалізації свободи слова.

У щорічній доповіді відображено порушення у сфері обороту персональних даних у мережі Інтернет. В Інтернеті з'явилися сайти, що маскують під відомі бренди, які здійснюють збір персональних даних із метою подальшого використання як бази даних для розсилки «спаму». Сайти здійснювали збирання персональних даних без відповідних відомостей, що визначають політику конфіденційності.

Для Інтернет-ресурсів, які здійснюють збирання та обробку персональних даних із порушеннями встановлених вимог, доцільно встановити процедуру блокування з попереднім повідомленням, аналогічну процедурі блокування сайтів за поширення протиправного контенту. Це пояснюється тим, що персональні дані громадян становлять певну цінність і можуть бути використані в різних протиправних цілях.

Кодекс України про адміністративні правопорушення у ст. 188-39 «Порушення законодавства у сфері захисту персональних даних» передбачає штрафні санкції за невиконання власниками Інтернет-ресурсів обов'язків з опублікування або забезпечення іншим чином необмеженого доступу до політики конфіденційності або до відомостей про вимоги до захисту персональних даних, що реалізуються. Чинні заходи адміністративної відповідальності є досить ефективними, оскільки забезпечують зниження кількості порушень у сфері обігу персональних даних.

На думку І.М. Павлюк і В.В. Калічка, законодавство України містить чітке визначення терміна «персональні дані», а Конституційний Суд України, даючи офіційне тлумачення ст. 32 Конституції в рішенні, наводить конкретний перелік інформації, що може становити персональні дані. Водночас законодавством впроваджено дієвий механізм захисту порушених прав у сфері захисту персональних даних [14].

Тривалий час питання безпеки залишалися прерогативою держави, однак Закон України «Про національну безпеку України» визначив серед принципів забезпечення безпеки взаємодію державних органів із громадськими об'єднаннями, міжнародними організаціями та громадянами. Ця діяльність не обмежується державним рівнем.

Недержавна система поки що перебуває в стадії формування, основною перешкодою для її розвитку є відсутність єдиного методичного та організаційного центру. Національна стратегія сприяння розвитку громадянського суспільства на 2021–2026 роки передбачає, що в умовах розвитку громадянського суспільства становлення недержавної системи забезпечення інформаційної безпеки набуває актуальності [15]. Взаємодія державної та недержавної

системи забезпечення права особи на інформаційну безпеку сприятиме дотриманню балансу між потребою громадян у вільному обміні інформацією та обмеженнями, пов'язаними з необхідністю забезпечення національної безпеки, зокрема в інформаційній сфері.

Розглянувши діяльність державних органів у сфері забезпечення права особи на інформаційну безпеку, доцільно зазначити, що реалізація гарантій прав та свобод громадян в інформаційній сфері, захисту національних інтересів України передбачає суттєве посилення ролі держави в регулюванні суспільних відносин, наявність відкритої державної політики в цій галузі.

Державна політика, що проводиться у сфері забезпечення інформаційної безпеки, має бути прозорою та слідувати певному курсу забезпечення інформаційної безпеки. Характер цієї політики визначає пріоритети державних, громадських чи особистих інтересів, місце та повноваження суб'єктів забезпечення інформаційної безпеки особи.

У проєкті Стратегії інформаційної безпеки – 2025 держава має виконувати два набори інформаційних зобов'язань відповідно до системи інформаційної безпеки особи: 1) зобов'язання у сфері інформаційно-правової безпеки (забезпечувати доступ до інформації, що запитується; збирати та надавати інформацію, що має інтерес для суспільства; підтримувати розвиток інформаційного сектора); 2) зобов'язання у сфері інформаційно-психологічної безпеки, спрямовані на недопущення поширення морально небезпечної інформації [16]. Ця позиція є обґрунтованою, оскільки захист від інформаційно-психологічних впливів займає особливе місце через збільшення можливостей впливу інформації на психіку людини.

Діяльність із забезпечення права особи на інформаційну безпеку характерна для багатьох органів державної влади України. Державні органи здатні здійснювати цю діяльність найбільш ефективно, оскільки мають необхідний інструментарій. Необхідно зазначити роль недержавної системи – громадських об'єднань, професійних спілок, громадських фондів – у забезпеченні права особи на інформаційну безпеку.

Доцільно зробити висновки. Діяльність із забезпечення права особи на інформаційну безпеку передбачає реалізацію органами державної влади різних рівнів певних повноважень. Відповідно до Закону «Про національну безпеку України» державні органи з метою забезпечення безпеки можуть взаємодіяти з громадськими об'єднаннями, міжнародними організаціями та громадянами.

У системі органів державної влади найбільшою компетенцією у сфері забезпечення права особи на інформаційну безпеку володіють Міністерство культури і інформаційної політики, Державна служба спеціального зв'язку і захисту інформації України. До повноважень Держспецзв'язку доцільно додати можливість блокування Інтернет-ресурсів, що займаються збиранням та обробкою персональних даних із порушенням вимог законодавства України.

ЛІТЕРАТУРА

1. Малашко О.Є., Єсімов С.С. Зміст державної діяльності із забезпечення інформаційної безпеки. *Міжнародний науковий журнал «Інтернаука»*. 2020. № 15 (95). Т. 1. С. 46–54.
2. Про Національну безпеку України : Закон України від 21 червня 2018 р. № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>
3. Про внесення змін до деяких законів України щодо забезпечення прозорості власності провайдерів програмної послуги багатоканальних цифрових ефірних телемереж із загальнонаціональним покриттям : Закон України від 3 жовтня 2019 р. № 158-IX. URL: <https://zakon.rada.gov.ua/laws/show/158-20>
4. Сопільник Л., Скриньковський Р., Ковалів М., Заяць Р. Розвиток цифрової економіки в контексті забезпечення інформаційної безпеки в Україні. *Траєкторія Науки = Path of Science*. 2020. Vol. 6. № 5. S. 2023–2032.
5. Апарат Ради національної безпеки і оборони України. URL: <https://www.mbo.gov.ua/ua/Aparat-Rady-natsionalnoi-bezpeky-i-oboronyUkrainy>
6. Проєкт Закону «Про внесення змін до Закону України від 05.11.2021 р. № 6286 «Про санкції» щодо уточнення підстав застосування». URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=73157
7. Про Службу безпеки України : Закон України від 22 березня 1992 р. № 2229-XII. URL: <https://zakon.rada.gov.ua/laws/show/2229-12>
8. Про затвердження Положення про Міністерство внутрішніх справ України : Постанова Кабінету Міністрів України від 28 жовтня 2015 р. № 878. URL: <https://zakon.rada.gov.ua/laws/show/878-2015-%D0%BF#Text>

9. Питання Міністерства цифрової трансформації : Постанова Кабінету Міністрів України від 18.09.2019 р. № 878. URL: <https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text>
10. Деякі питання діяльності Міністерства культури та інформаційної політики : Постанова Кабінету Міністрів України від 16.10.2019 р. № 885. URL: <https://zakon.rada.gov.ua/laws/show/885-2019-%D0%BF#Text>
11. Про внесення змін до деяких законодавчих актів України щодо імплементації Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства (Ланцаротської конвенції) : Закон України від 18 лютого 2021 р. № 1256-IX. URL: <https://zakon.rada.gov.ua/laws/show/1256-20#n84>
12. Право на інформацію. Конституційний Суд України. URL: <https://ccu.gov.ua/storinka-knygy/431-pravo-na-informaciyu>
13. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини «Про стан додержання прав і свобод людини і громадянина в Україні» 2020 рік. Київ : *Верховна Рада України*, 2021. 355 с.
14. Павлюк І., Калічак В. Чи реально притягти до відповідальності за порушення захисту персональних даних в Україні? *Юридична газета*. 24 березня 2021 р. URL: <https://yur-gazeta.com/dumka-eksperta/chi-realno-prityagti-do-vidpovidalnosti-za-porushennya-zahistu-personalnih-danih-v-ukrayini.html>
15. Про Національну стратегію сприяння розвитку громадянського суспільства в Україні на 2021–2026 роки : Указ Президента України від 27 вересня 2021 р. 487/2021. URL <https://zakon.rada.gov.ua/laws/show/487/2021#Text>
16. Стратегія інформаційної безпеки – 2025: що зміниться у сфері цифрових прав. 22 вересня 2021 р. URL: <https://dslua.org/publications/strategiia-informatsiynoi-bezpeky-2025-shcho-zminytsia-u-sferi-tsyfrovykh-prav/>