УДК 342.9
DOI https://doi.org/10.32782/klj/2025.2.39

Уртаєв О. І.,
адвокат, арбітражний керуючий,
аспірант кафедри теорії держави і права
Міжнародного гуманітарного університету

ВІДПОВІДАЛЬНІСТЬ ЗА ПРАВОПОРУШЕННЯ, ЩО ВИНИКАЮТЬ В СФЕРІ ІТ-ПРАВА

Анотація. У статті досліджено актуальні питання юридичної відповідальності за правопорушення, що виникають у сфері ІТ-права, з урахуванням сучасних викликів інформаційного суспільства та стрімкого розвитку цифрових технологій. З'ясовано, що відповідальність в сфері ІТ-права може інтегрувати норми як публічного, так і приватного права, що зумовлюється широким спектром і розгалуженістю можливих правопорушень у цій сфері та потребує визначення відповідного механізму юридичної відповідальності.

Встановлено, що в умовах цифровізації суспільних процесів порушення в сфері ІТ-права можуть набувати як приватноправового, так і публічно-правового характеру. У першому випадку йдеться про порушення цивільних інформаційних прав, договірних зобов'язань, неправомірне використання об'єктів інтелектуальної власності тощо, що тягне за собою майнову та немайнову відповідальність. У другому – про порушення законодавства щодо захисту персональних даних, кібербезпеки, інформаційної безпеки, що передбачає адміністративну, а в окремих випадках і кримінальну відповідальність.

Особливої уваги заслуговують виклики, пов'язані з кіберзлочинністю та неправомірною обробкою персональних даних, що в умовах воєнного стану набувають загрозливого характеру для національної безпеки України. Підкреслено потребу подальшого вдосконалення законодавства, зокрема – адаптації норм національного права до стандартів ЄС у сфері ІТ-правовідносин, посилення ефективності міжнародного співробітництва та створення умов для оперативного реагування на ІТ-правопорушення.

Зроблено висновок, що ефективна відповідальність у сфері ІТ-права потребує комплексного підходу, який має поєднувати превентивні, процедурні та санкційні механізми, а також потребує тісної взаємодії між державними органами, приватним сектором та громадянським суспільством та своєчасного реагування на порушення в сфері ІТ права. Своєчасне оновлення правової бази та підвищення цифрової обізнаності населення, що є ключовими чинниками формування дієвої системи відповідальності щодо використання інформаційно-телекомунікаційних технологій, які стрімко розвиваються.

Ключові слова: *ІТ-право, відповідальність, інформаційно-телекомунікаційні технології, кібератаки, захист персональних даних.*

Urtayev O. I. Liability for offenses arising in the field of IT law

Abstract. The article examines the current issues of legal liability for offenses arising in the field of IT law, taking into account the modern challenges of the information society and the rapid development of digital technologies. It is found that liability in the field of IT law can integrate the norms of both public and private law, which is due to the wide range and ramifications of possible offenses in this area and requires the definition of an appropriate mechanism of legal liability.

It is established that in the conditions of digitalization of social processes, violations in the field of IT law can acquire both private and public law nature. In the first case, we are talking about violations of civil information rights, contractual obligations, improper use of intellectual property objects, etc., which entails property and non-property liability. In the second, we are talking about violations of legislation on the protection of personal data, cybersecurity, information security, which provides for administrative, and in some cases criminal liability.

Particular attention is paid to the challenges associated with cybercrime and unlawful processing of personal data, which in conditions of martial law become threatening to the national security of Ukraine. The need for further improvement of legislation is emphasized, in particular, the adaptation of national law to EU standards in the field of IT legal relations, strengthening the effectiveness of international cooperation and creating conditions for a prompt response to IT offenses.

It is concluded that effective liability in the field of IT law requires a comprehensive approach that should combine preventive, procedural and sanction mechanisms, and also requires close interaction between state bodies, the private sector and civil society and timely response to violations in the field of IT law. Timely updating of the legal framework and increasing digital awareness of the population, which are key factors in

the formation of an effective system of liability for the use of information and telecommunications technologies, which are rapidly developing.

Key words: *IT law, liability, information and telecommunications technologies, cyberattacks, personal data protection.*

Уже понад двадцять років світ перебуває на етапі активного інформаційного розвитку. Інформаційні технології сьогодні стали ключовим фактором технічного та технологічного поступу майже в усіх сферах суспільного життя. Вони водночас виступають концентрованим відображенням загальних процесів інформаційної революції, яка розпочалася наприкінці XX і триває на початку XXI століття.

Очевидно, що IT-технології об'єднують не лише комунікаційні та технічні ресурси, а й матеріальні, фінансові, інтелектуальні, гуманітарні та політичні складові, сприяючи формуванню й ускладненню механізмів соціального регулювання. Глобалізація світової економіки була б неможливою без стрімкого розвитку IT-сфери. Останні роки стали періодом глибоких і швидкоплинних змін у сфері інформаційних технологій, які істотно впливають на трансформацію світової політики. IT-компанії сьогодні є провідниками інновацій та прикладами реалізації масштабних міжнародних проєктів.

У контексті інтеграційних процесів у світовій економіці, що супроводжуються вибуховим зростанням IT-індустрії, особливу вагу набувають питання нормативно-правової, управлінської та психологічної підготовки IT-фахівців, як для самих компаній, так і для наукових установ, що здійснюють їхню підготовку.

Правове регулювання IT-галузі в Україні вимагає розроблення комплексної нормативно-правової бази, яка б забезпечувала ефективне функціонування цієї сфери. Серед ключових питань залишаються: гарантування прав і свобод людини та громадянина, захист інтересів суспільства й держави у сфері IT-правовідносин, діяльність суб'єктів, що відповідають за інформаційну безпеку, протидія правопорушенням у цифровій сфері, правове врегулювання діяльності у віртуальному середовищі, захист прав споживачів під час онлайн-купівель, оформлення договірних відносин щодо інтелектуальної власності та її захист в Інтернеті, відповідальність за порушення умов використання цифрового контенту, правове регулювання трудових відносин в IT-секторі, а також адаптація національного законодавства до міжнародних стандартів у цій галузі.

Відповідно до звіту Digital 2024 Global Statshot, представленого Британською компанією DataReportal, станом на 2024 рік 5,75 мільярда людей користуються Інтернетом, що становить 70,3% від всього населення планети [1]. Дана статистика свідчить про стійку глобальну тенденцію до повсюдної цифровізації та поширення Інтернет-мережі. У контексті таких змін у сучасній юридичній науковій сфері сформувалося нове поняття – IT-право, як відповідь на потребу правового врегулювання відносин, що виникають у сфері інформаційних технологій.

Так, Р. Калюжний визначає IT-право як галузь, що знаходиться на межі публічного та приватного права, зазначаючи, що в межах складної, багаторівневої структури української правової системи IT-право виступає як міжгалузева комплексна правова наука, яка посідає своє місце у загальній системі національного права [2, с. 6]. Прихильники даної концепції визнання інформаційних технологій окремою комплексною галуззю права підкреслюють, що правові норми, які становлять її предмет, водночас належать до інших правових галузей, таких як конституційне, цивільне, адміністративне, кримінальне, сімейне право тощо [3, с. 4]. Наприклад, положення частини другої статті 34 Конституції України, яке гарантує кожному право вільно збирати, зберігати, використовувати та поширювати інформацію в усній, письмовій або іншій формі за власним вибором, є елементом інформаційно-правового регулювання, оскільки охоплює відносини, пов'язані з пошуком, отриманням, використанням та поширенням інформації [4]. Водночас дане положення є нормою конституційного права, оскільки гарантує основоположне право особи. В свою чергу, погляди на правову природу IT-права продовжують змі-

нюватися, прикладом цього є позиція вітчизняних науковців Є. Харитонова та О. Харитонової. З їх позиції, класифікація комплексного правового регулювання інформаційного суспільства як нової галузі права є методологічно невиправданою, оскільки з позицій нормативістського підходу ІТ-право, Інтернет-право та інформаційне право не можуть розглядатися як самостійні галузі. Натомість вони пропонують тлумачити ІТ-право як «концепт», який передбачає сукупність уявлень, знань, понять і асоціацій, що стосуються правового регулювання відносин, які виникають у процесі створення та застосування інформаційних технологій [5, с. 24].

В свою чергу, О. Сімсон акцентує увагу на тому, що ІТ-право не є штучно сформованим утворенням, а являє собою систему правового регулювання реальних суспільних відносин, що формуються та розвиваються в межах однієї з провідних галузей сучасної економіки – інформаційних технологій [6, с. 55].

У науковому дискурсі ІТ-право іноді розглядається як складова частина інформаційного права, а окремі дослідники навіть ототожнюють дані поняття. Проте, на нашу думку, така позиція є спірною, оскільки предметна сфера інформаційного права охоплює правовідносини, в яких об'єктом виступає інформація незалежно від форми її існування (наприклад: усна, письмова тощо). Натомість, як справедливо зазначають Т. В. Міхайліна та Я. В. Мазур, ІТ-право регулює специфічне коло відносин, що виникають у процесі створення, збереження, передачі та захисту інформації в електронній формі, яка обробляється з використанням інформаційних технологій у межах локальних та глобальних інформаційних систем. Сюди входять питання, пов'язані з розробкою й поширенням програмного забезпечення, інноваційних інформаційних технологій, баз даних, веденням Інтернет-бізнесу, укладанням і виконанням смарт-контрактів, здійсненням онлайн-розрахунків тощо. Норми, що регулюють ІТ-сферу, мають змішаний характер, поєднуючи елементи публічного та приватного права: з одного боку, домінує приватна ініціатива та договірне регулювання, що обумовлює наявність диспозитивних норм; з іншого – значна частина норм має імперативний характер і встановлює обов'язкові правила поведінки. Таким чином, ІТ-право поєднує диспозитивний та імперативний методи правового регулювання [7, с. 147].

Відтак, можна дійти до висновку, що ІТ-право включає в себе як публічно-правові, так і приватно правові аспекти, а до предмета правового регулювання ІТ-галузі належать: 1) надання та використання інформаційних послуг і продуктів (створення, отримання, обробка, зберігання баз даних); 2) результати інтелектуальної діяльності (твори літератури, мистецтва, музики тощо та діяльність щодо них); 3) документообіг, електронні договори, цінні папери, об'єкти нематеріального характеру (наприклад: персональні дані фізичних та юридичних осіб, що потребують належного контролю за їх обробкою, зберіганням та передачею та забезпеченням безпеки таких осіб); 4) матеріальні активи, пов'язані з функціонуванням інформаційного простору.

Так, порушення у сфері ІТ-права в межах приватноправових відносин слід розуміти як протиправну поведінку, що виражається в недотриманні або неналежному виконанні цивільно-правових інформаційних обов'язків чи у порушенні інформаційних прав, які закріплені в договірних положеннях та/або нормативно-правових актах, і яка спричиняє моральну та/або матеріальну шкоду, збитки чи інші витрати [8, с. 38]. Такі правопорушення можуть мати як майновий, так і немайновий характер, що зумовлює необхідність чіткого встановлення кола осіб, яким може бути завдано немайнової шкоди внаслідок інформаційного правопорушення. Згідно з правовою позицією, викладеною в роз'ясненнях Пленуму Верховного Суду України щодо судової практики розгляду справ про відшкодування моральної (немайнової) шкоди [9], така шкода може бути заподіяна як фізичним, так і юридичним особам. Для фізичних осіб йдеться про втрату немайнового характеру, що виникає внаслідок моральних або фізичних страждань, спричинених неправомірними діями чи бездіяльністю суб'єктів правопорушення у сфері ІТ-відносин. У випадку з юридичними особами йдеться про втрати

немайнового характеру, пов'язані з посяганням на ділову репутацію, фірмове найменування, товарний знак, комерційне найменування, розголошенням комерційної таємниці, а також іншими діями, які знижують престиж або підривають довіру до діяльності юридичної особи [8, с. 39].

Однією з визначальних характеристик зобов'язань, що виникають із відшкодування шкоди, заподіяної в результаті ІТ-правопорушення, є їхня відновлювально-компенсаційна природа, що передбачає прагнення повернути особу до стану, в якому та перебувала до моменту вчинення правопорушення. У разі, якщо фактичне відновлення попереднього стану є неможливим, передбачено компенсування всіх завданих збитків у майновій формі з урахуванням характеру порушення та його наслідків у сфері інформаційних правовідносин.

У публічно-правовому аспекті відповідальність у сфері ІТ-права набуває особливої актуальності в контексті порушення режиму захисту персональних даних, оскільки всі інформаційно-комунікаційні системи тією чи іншою мірою пов'язані з їх обробкою, зокрема у межах функціонування державних реєстрів, розробниками яких виступають приватні юридичні особи. В умовах воєнного стану питання безпеки персональних даних в цифровому середовищі набуває принципово нового значення, адже безпосередньо перетинається із проблематикою кібербезпеки держави загалом та захисту її громадян зокрема. В свою чергу, Пашинський В. Й. та Цьоменко А. В. зазначають, що однією з ключових проблем у веденні державних інформаційних реєстрів є потреба у формуванні спеціального порядку їх заповнення та чіткої системи верифікації доступу до таких даних, особливо у випадках, що стосуються персональної інформації військовослужбовців. Зокрема, мова йде про представників силових структур – Збройних Сил України, Національної гвардії України, Служби безпеки України, Національної поліції, Державної прикордонної служби України та інших військових формувань. Незаконне отримання доступу агресором до персональних даних цієї категорії осіб становить реальну загрозу не лише національній безпеці, але й фундаментальним правам самих військовослужбовців та членів їхніх родин. Ілюстрацією таких загроз є випадок, коли прокремлівська хакерська група RaHDIt здійснила публікацію персональних даних 700 співробітників Служби безпеки України, доповнивши їх інформацією про військовослужбовців Збройних Сил України: ПІБ, дата народження, посада, звання, адреса проживання, контактні дані, паспортні реквізити, електронна пошта, облікові записи в соціальних мережах тощо – часто з додаванням фотозображень. Подібна інформація може бути використана ворожою стороною з метою порушення прав осіб, що належать до особливо вразливих категорій, зокрема для психологічного тиску, залякування, завдання моральної або навіть фізичної шкоди [10].

Одним із важливих інструментів адміністративно-правового захисту персональних даних у межах ІТ-права є система превентивних заходів, спрямованих на запобігання порушенням законодавства у сфері захисту персональних даних, яку, згідно зі ст. 4 відповідного законодавства, повинні впроваджувати володільці персональних даних, розпорядники таких даних та Уповноважений Верховної Ради України з прав людини [11]. До суб'єктів, що можуть виступати володільцями або розпорядниками персональних даних, належать юридичні особи всіх форм власності, органи державної влади, органи місцевого самоврядування, а також фізичні особи-підприємці, які здійснюють обробку даних на підставі законодавства. Якщо персональні дані належать органу державної влади або органу місцевого самоврядування, то їх розпорядником може бути лише державне або комунальне підприємство, що перебуває у сфері управління відповідного органу. При цьому обробка персональних даних розпорядником можлива лише в межах мети, обсягу та способу, визначених письмовим договором з володільцем даних.

У межах ІТ-права особлива увага також приділяється і превентивним заходам, які поділяються на дві категорії: ті, що вживаються самими володільцями або розпорядниками даних, та ті, які реалізуються посадо-

вими особами Уповноваженого. Відповідальні структурні підрозділи або окремі уповноважені особи в межах підприємств чи установ забезпечують захист персональних даних від випадкової втрати, знищення, несанкціонованої обробки чи доступу. Вони також зобов'язані інформувати та консультувати суб'єктів обробки даних щодо дотримання вимог законодавства, а також здійснювати комунікацію з Уповноваженим з метою запобігання та усунення правопорушень у сфері захисту персональних даних.

Невід'ємною складовою адміністративно-правового захисту персональних даних в ІТ-сфері є притягнення до адміністративної відповідальності у випадках порушення вимог законодавства. Згідно зі ст. 188-39 КУпАП, правопорушеннями у даній сфері визнаються: неподання або несвоєчасне подання інформації Уповноваженому щодо обробки персональних даних або зміни у відомостях, що підлягають повідомленню згідно з законом; подання неповної або недостовірної інформації; невиконання приписів Уповноваженого або посадових осіб його секретаріату щодо усунення порушень; повторні порушення, вчинені протягом одного року після застосування адміністративного стягнення; недотримання вимог щодо порядку захисту персональних даних, що призвело до несанкціонованого доступу або порушення прав суб'єкта персональних даних; а також повторне порушення, передбачене частиною четвертою цієї статті, за яке вже було застосовано відповідне стягнення [12].

Попри численні позитивні наслідки стрімкого розвитку інформаційно-телекомунікаційних технологій, сучасне суспільство та держава стикаються з об'єктивними ризиками, серед яких особливої ваги набуває кіберзлочинність як правове явище в межах ІТ-права. Одним із ключових нормативно-правових актів, що спрямований на превенцію злочинності у сфері інформаційних технологій, є Закон України «Про основні засади забезпечення кібербезпеки України», відповідно до положень якого, кіберзлочин (комп'ютерний злочин) визначається як суспільно небезпечне, винне діяння, вчинене у кіберпросторі або з його використанням, кримінальна відповідальність за яке передбачена Кримінальним кодексом України та/або міжнародними договорами, сторонами яких є Україна. Основною метою таких дій зазвичай є несанкціоноване втручання в інформаційні системи, крадіжка або знищення даних, порушення цілісності інформаційної інфраструктури [13].

В умовах повномасштабної війни кіберзлочини набувають нових форм і функцій, серед яких – дестабілізація державних процесів, викрадення конфіденційної інформації, виведення з ладу систем критичної інфраструктури та завдання шкоди економіці. Зазначені загрози конкретизовано в Стратегії кібербезпеки України, що була затверджена Указом Президента України № 446/2021. Також, Розділ XVI Кримінального кодексу України містить визначення кримінальних правопорушень у сфері використання електронно-обчислювальних машин, комп'ютерних систем і мереж, а також мереж електрозв'язку [14]. Хоча окремі елементи превенції закріплено також у Конституції України та Кримінальному процесуальному кодексі України, дані положення мають переважно декларативний характер та вимагають подальшого системного вдосконалення.

Особливістю кіберзлочинності є її транснаціональна природа, оскільки такі правопорушення можуть вчинюватися особами, що перебувають за і межами національної юрисдикції. У зв'язку з цим міжнародне співробітництво у сфері ІТ-права є надзвичайно важливим. Європейський Союз, крім базових актів, прийняв низку спеціалізованих документів, серед яких Директива щодо боротьби із сексуальною експлуатацією дітей в Інтернеті та дитячою порнографією (2011 рік), а також Пропозиція щодо тимчасового регулювання обробки персональних та інших даних з метою протидії сексуальному насильству над дітьми (2020 рік). У межах Європолу створено Європейський центр з кіберзлочинності, який акумулює експертизу держав-членів ЄС для підтримки розслідувань у галузі ІТ-злочинів. Водночас, попри ратифікацію Україною низки міжнародних договорів у сфері боротьби з кіберзлочинністю, механізми реалізації міжнародного співробітництва залишаються надмірно бюрократизова-

ними, що ускладнює оперативне реагування на кіберзлочини [15, с. 18].

Після початку російського повномасштабного вторгнення на територію України було зафіксовано стрімке зростання кількості кримінальних правопорушень у сфері інформаційних технологій. Країна-агресор активно використовує ІТ-інструменти для поширення дезінформації, маніпулювання громадською думкою, ведення інформаційної війни. У відповідь на зазначені виклики на державному рівні здійснено ряд комплексних зміни у сфері кримінального та кримінального процесуального законодавства стосовно кібербезпеки. Зокрема, були прийняті нормативно-правові акти, які суттєво посилили правові механізми притягнення до відповідальності осіб, що вчиняють злочини у сфері ІТ, зокрема, Закон «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» з питань підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам, а також Закон «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» [16; 17]. Зазначені законодавчі ініціативи безпосередньо спрямовані на розширення повноважень правоохоронних органів у частині виявлення, документування та розслідування кіберзлочинів, а також на посилення кримінальної відповідальності за діяння, вчинені у сфері інформаційних технологій.

Таким чином, відповідальність у сфері ІТ-права має розгалужений та багаторівневий характер, що зумовлено стрімким поширенням інформаційно-телекомунікаційних технологій у всі сфери суспільного життя. Ефективне функціонування механізму такої відповідальності потребує комплексного підходу, який має охоплювати превентивні, процедурні та санкційні інструменти, а також передбачати тісну взаємодію між органами державної влади, приватним сектором та громадянським суспільством. Необхідним також є своєчасне реагування на правопорушення у сфері ІТ, з урахуванням їх динамічного та транснаціонального характеру, а ключовими умовами формування ефективної системи відповідальності за порушення у сфері інформаційно-телекомунікаційних технологій має виступати постійне та системне оновлення правової бази, що пов’язано з постійним розвитком технологій і потребою належного нормативного регулювання з боку держави, а також перманентне підвищення рівня цифрової правової культури серед населення задля запобігання можливих порушень у сфері цифрових технологій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Digital 2024 October Global Statshot Report. DATAREPORTAL. URL: https://datareportal.com/reports/digital-2024-october-global-statshot.

2. Калюжний Р. Предмет та методи інформаційного права. Правова інформатика. 2008. № 3. С. 5-9.

3. Бачинський Т., Радейко Р. Основи ІТ-права: навч. посіб. 3-тє вид., допов. і перероб. К. Юрінком Інтер. 2019. 244 с.

4. Конституція України від 28 червня 1996 р. Відомості Верховної Ради України. 1996. № 30. Ст. 141.

5. Харитонов Є. О., Харитонова О. І. Сутність ІТ-права: пошук парадигми. Право України. 2018. № 1. С. 18-29.

6. Сімсон О. ІТ-право з позицій теорії та практики, підходи до вивчення і викладання. Право України. 2018. № 1. С. 51-62.

7. Міхайліна Т. В., Мазур Я. В. ІТ-Право у системі права: дискусійні моменти сучасності. Науковий вісник Ужгородського Національного Університету, 2024. Серія Право. Випуск 84. Ч. 3. С. 144-151.

8. Тихомиров О.О. Цивільно-правова відповідальність за інформаційні правопорушення: загальнотеоретичні аспекти. Порівняльно-аналітичне право. № 1. 2015. С. 37-40.

9. Про судову практику в справах про відшкодування моральної (немайнової) шкоди : Постанова Пленуму Верховного Суду України № 4 від 31.03.1995 р. URL: http://zakon5.rada.gov.ua/laws/show/v0004700-95.

10. Пашинський В.Й., Цьоменко А.В. Забезпечення захисту персональних даних громадян органами публічної влади в умовах війни. Вісник Київського національного університету імені Тараса Шевченка. Серія Військові науки. № 4 (52), 2022. Київ, С. 50-53. DOI: https://doi.org/10.17721/1728- 2217.2022.52.50-53

11. Про захист персональних даних : Закон України від 1 черв. 2010 р. № 2297-VI. Відомості Верховної Ради України. 2010. № 34. Ст. 481.

12. Кодекс України про адміністративні правопорушення від 7 груд. 1984 р. № 8073-X. Відомості Верховної Ради УРСР. 1984. Додаток до № 51. Ст. 1122.

13. Про основні засади забезпечення кібербезпеки України: закон України від 5 жовтня 2017 року № 2163-VIII https://zakon.rada.gov.ua/laws/show/2163-19.

14. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III URL: https://zakon.rada.gov.ua/go/2341-14.

15. Сащенко М.І. Проблемні аспекти запобігання кіберзлочинності в Україні. «Young Scientist». 2022. № 1 (101). С. 17–20.

16. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану від 24.02.2022 № 2149-IX. URL: https:// zakon.rada.gov.ua/laws/show/2149-20#Text.

17. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану : Закон України від 24 берез. 2022 № 2149- IX: URL: https:// zakon.rada.gov.ua/laws/show/2149-20#Text.