УДК 342.9 (477)
DOI https://doi.org/10.32782/2408-9257-2024-4-11

Серебро М. В.,
докторант
Ужгородського національного університету

ПРОТИДІЯ ПРАВОПОРУШЕННЯМ У СФЕРІ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ: ЗАРУБІЖНИЙ ДОСВІД

COMBATING OFFENSES IN THE SPHERE OF USE OF INFORMATION TECHNOLOGIES: FOREIGN EXPERIENCE

Наукова публікація присвячена дослідженню зарубіжного досвіду протидії правопорушенням у сфері використання інформаційних технологій.

Зазначається, що у більшості цивілізованих зарубіжних країн встановлено відповідальність за «сталкінг», який визначається як свідоме, здійснюване із протиправним умислом переслідування та спричинення занепокоєння іншій людині. Враховуючи досліджений позитивний досвід, наголошено на необхідності внесення змін до національного законодавства щодо встановлення відповідальності за сталкінг, включаючи відповідальність за кібер-сталкінг – переслідування та спричинення занепокоєння іншій людині із використанням Інтернет (соціальних мереж та месенджерів, електронної пошти та інших засобів електронної комунікації).

Окремо проаналізовано позитивний досвід зарубіжних країн у сфері протидії правопорушенням, які вчиняються із використанням соціальних мереж та месенджерів.

Підкреслено необхідність запозичення позитивного європейського досвіду у сфері захисту персональних даних, зокрема, в частині прийняття в Загального регламенту про захист даних (General Data Protection Regulation, GDPR), який розширює повноваження органів публічної адміністрації у сфері правового регулювання діяльності соціальних мереж та месенджерів, а саме, дозволяє видаляти незаконний контент і змушує адміністраторів платформ докладати зусилля для боротьби з небезпечним контентом. Відповідні зміни необхідно внести в національне законодавство з метою адаптації національних стандартів у сфері захисту персональних даних до права ЄС, а також ефективної протидії поширенню забороненого законом контенту в соціальних мережах та месенджерах. Також доцільним вбачається посилення відповідальності за порушення недоторканості приватного життя (ст. 182 Кримінального кодексу України), а також порушення законодавства про захист персональних даних (ст. 188-39 Кодексу України про адміністративні правопорушення).

Ключові слова: *зарубіжний досвід, правопорушення, інформаційні технології, цифровий контент, сталкінг, соціальні мережі, месенджери, персональні данні, протидія, захист.*

The scientific publication is devoted to the study of foreign experience in combating offenses in the field of information technology use.

It is noted that in most civilized foreign countries, liability for «stalking» is established, which is defined as a deliberate, unlawful pursuit of another person, what causing concern. Taking into account the positive experience studied, it is emphasized the need to make changes to the national legislation on establishing liability for stalking, including liability for cyber-stalking – harassing and causing concern to another person using the Internet (social networks and messengers, e-mail and other means of electronic communication).

The positive experience of foreign countries in the field of combating crimes committed with the use of social networks and messengers is separately analyzed.

The need to borrow positive European experience in the field of personal data protection is emphasized, in particular, in the part of the adoption of the General Data Protection Regulation (GDPR), which expands the powers of public administration bodies in the field of legal regulation of the activities of social networks and messengers, namely , allows illegal content to be removed and forces platform administrators to make efforts to combat dangerous content. Corresponding changes must be made to national legislation in order to adapt national standards in the field of personal data protection to EU law, as well as to effectively counter the spread of content prohibited by law in social networks and messengers. It is also considered appropriate to increase liability for violation of privacy (Article 182 of the Criminal Code of Ukraine), as well as violation of the legislation on the protection of personal data (Articles 188-39 of the Code of Ukraine on Administrative Offenses).

Key words: *foreign experience, crimes, information technologies, digital content, stalking, social networks, messengers, personal data, protection.*

Актуальність теми. Правопорушення у сфері використання інформаційних технологій набувають все більшого поширення у зв'язку із загальною тенденцією щодо цифровізації суспільних відносин, збільшенням кількості користувачів Інтернет у геометричній прогресії, появою великої кількості різноманітних соціальних мереж та месенджерів, які часто використовуються із протиправною метою.

До найбільш поширених правопорушень у сфері використання інформаційних технологій відноситься, у тому числі, кібер-сталкінг, тобто протиправне переслідування особи із використанням Інтернет та інших засобів електронних комунікацій, а також порушення законодавства у сфері захисту персональних даних, зокрема права людини на недоторканість приватного життя.

Країни Європейського Союзу та США вживають різноманітні правові засоби протидії та запобігання вказаним правопорушенням, які заслуговують на увагу та визначення можливості і доцільності їх імплементації в національне законодавство та юридичну практику.

Вищевикладеним обґрунтовується актуальність, а також теоретична та практична значимість дослідження зарубіжного досвіду протидії правопорушенням у сфері використання інформаційних технологій.

Різні аспекти правового регулювання використання та розвитку інформаційних технологій завжди були в центрі уваги науковців. Із останніх наукових праць слід виділити роботи Д. Біленької [1], О. Берназюка [2], Т. Ковальової та О. Гунбіної [3], О. Комарова [4], А. Краковської та М. Бабик [5], А. Омельченка [6], Р. Стефанчука [7], І. Тищенкової [8].

Проте, зарубіжний досвід протидії правопорушенням у сфері використання інформаційних технологій ще не був предметом окремого наукового аналізу, що актуалізує підготовку даної публікації.

Постановка завдання. Метою наукової публікації є дослідження зарубіжного досвіду протидії правопорушенням у сфері використання інформаційних технологій.

Методологія даної публікації включає філософські (закони та прийоми діалектики: єдності та боротьби протилежностей, переходу кількісних змін у якісні, прийом «заперечення заперечення», принципи об'єктивності та історизму), загальнонаукові (системний та структурно-функціональний методи, прийоми логіки: аналіз, синтез, дедукція та індукція) та спеціально-юридичні методи дослідження (формально-юридичний метод як похідний від аксіоматичного методу дослідження, метод юридичного моделювання). Враховуючи тему дослідження, більшою мірою використовується методологія порівняльного правознавства. Крім того, в процесі дослідження використовуються такі загальновідомі наукові підходи як цивілізаційний, антропоцентричний, телеологічний та синергетичний.

Результати дослідження. У сфері використання інформаційних технологій вчиняється значна кількість правопорушень, більша частина яких вже всебічно описана науковцями та відображена в офіційній статистиці. Проте, із розвитком суспільних відносин та продовженням процесу їх цифровізації з'являються нові способи вчинення протиправних діянь, які потребують оперативної реакції органів публічної адміністрації та правового врегулювання.

Так, однією із найбільш актуальних проблем у сфері використання інформаційних технологій, яка знайшла своє правове врегулювання у багатьох зарубіжних країнах, є проблема сталкінгу.

Вперше поняття «сталкінг» з'явилось на законодавчому рівні як правопорушення, за яке передбачена кримінальна відповідальність, наприкінці двадцятого століття у США (штат Каліфорнія). Відповідно до положень Кримінального кодексу штату, «сталкінг» визначено як свідоме, здійснюване із злим умислом переслідування та спричинення занепокоєння іншій людині. Підставами для схвалення цього закону стало вбивство після тривалого переслідування у 1989 році актриси Ребекі Шефер, яку три роки поспіль домагався її шанувальник, який згодом проник до будинку та застрелив її [9].

Таким чином, в основу складу вказаного правопорушення було покладено не сам факт вбивства, а саме переслідування особи, що спричиняє їй занепокоєння.

Протягом двох років подібні закони з'явилися ще у 30 штатах. У 1996 році Конгрес США прийняв федеральний закон проти пере-

слідування як частину Закону про насильство щодо жінок (VAWA)17, відповідно до якого перетинання меж штату з метою переслідування певної особи, якщо така поведінка викликає страх та серйозні загрозливі побоювання щодо можливих тілесних ушкоджень або смерті жертви, переслідування її найближчих членів родини, є федеральним злочином (18 USC § 2261A) [9].

Таким чином, в правовому полі США з'явився новий склад правопорушення, яке згодом набуло поширення і в цифровому просторі, адже переслідування певної особи із використанням інформаційних технологій стало достатньо поширеним явищем, чому сприяли доступність та простота інформаційного впливу на іншу особу в Інтернет.

Враховуючи євроінтеграційні прагнення України, на особливу увагу заслуговує досвід правової регламентації протидії сталкінгу в Європейському Союзі.

Так, у Німеччині шляхом внесення змін до кримінального закону у березні 2007 року запроваджено відповідальність за сталкінг. Відповідно до диспозиції статті 238 Кримінального кодексу Німеччини будь-яка особа, яка без згоди (несанкціоновано) та навмисно переслідує іншу особу таким чином, що це може мати значний негативний вплив на її спосіб і стиль життя шляхом повторного вчинення такої дії, карається позбавленням волі на строк до трьох років або штрафом [9].

Отже, для притягнення порушника до відповідальності за сталкінг у Німеччині достатньо повторного вчинення такої дії, яка кваліфікується як навмисне переслідування іншої особи без її згоди, що може мати значний негативний вплив на її спосіб і стиль життя. Відповідно, це може бути повторний лист, надісланий на електронну пошту чи повторне повідомлення у месенджері, що може викликати вказані наслідки.

Законодавство Італії у сфері покарання за акти «сталкінгу» представлено Законом «Про невідкладні заходи щодо громадської безпеки та боротьби з сексуальним насильством, а також щодо актів переслідування» від 23 квітня 2009 року № 3821, яким внесені зміни до статті 612 Кримінального кодексу Італійської Республіки такого змісту: «Якщо будь-хто шляхом неодноразових (повторних) дій погрожує чи переслідує жертву таким чином, щоб викликати в неї стійкий і серйозний стан занепокоєння, тривоги чи страху або викликати обґрунтований страх за своє життя та особисту безпеку або близького родича, або особи, пов'язаної з нею емоційними стосунками, або примусу змінити свої життєві звички, карається позбавленням волі». За вчинення цього виду злочину до винуватої особи може бути застосоване покарання у вигляді позбавлення волі від шести місяців до чотирьох років. Покарання посилюється, якщо злочин вчинено одним із подружжя, що розлучилося, або особою, яка мала психічно-емоційні стосунки з ображеною особою; покарання збільшується вдвічі, якщо діяння вчинено на шкоду неповнолітній особі, вагітній жінці або особі з інвалідністю, або з використанням зброї [9].

Позитивним прикладом для національних законодавців є встановлення кваліфікуючих ознак сталкінгу (та, відповідно, посиленої відповідальності), які передбачає італійське законодавство – вчинення правопорушення одним із подружжя, що розлучилося, або особою, яка мала психічно-емоційні стосунки з особою, яка переслідується, а також вчинення відповідного діяння на шкоду неповнолітній особі, вагітній жінці або особі з інвалідністю, або з використанням зброї.

У Франції «сталкінг» є кримінальним проступком, який визначається як синдром нав'язливого переслідування та відноситься до категорії «delit», а не «crime». Відповідно до статті L. 222-33-2 Кримінального кодексу Франції переслідування особи через неодноразові коментарі чи поведінку з метою погіршення умов її праці, що може порушити її права та гідність, зашкодити фізичному або психічному здоров'ю чи поставити під загрозу її професійне майбутнє, карається позбавленням волі на строк до двох років та штрафом у розмірі 30 тис. євро [9].

Також позитивним прикладом є встановлення кваліфікуючих ознак сталкінгу у французькому законодавстві. Так, переслідування одним із подружжя свого колишнього партнера шляхом здійснення коментарів чи девіантною поведінкою, вторгненням у фізичний простір жертви, метою чи наслідком яких є погіршення

умов життя жертви, що призвело до погіршення її фізичного або психічного здоров'я, карається позбавленням волі на три роки та штрафом у розмірі 45 тис. євро. Якщо за наслідками протиправних дій жертва отримала повну втрату працездатності (понад вісім днів), покарання передбачає строк п'ять років позбавлення волі та штраф у розмірі 75 тис. євро.

Крім того, французьким законодавством передбачено, що покарання збільшується до десяти років позбавлення волі та штрафу у розмірі 150 тис. євро у випадку, якщо переслідування призвело до доведення до самогубства або спроби самогубства жертви.

Також статтею L. 222-33-2-2 Кримінального кодексу Франції передбачено, що переслідування особи через неодноразові коментарі у соціальних мережах чи девіантну поведінку, метою чи наслідком якої є погіршення умов її способу життя, призвело до зміни (погіршення) стану її фізичного чи психічного здоров'я, або у випадку, якщо протиправні діяння призвели до часткової втрати працездатності жертви (до восьми днів) – карається позбавленням волі на один рік і штрафом у розмірі 15 000 євро [9].

Таким чином, окремою частиною вказаної статті Кримінального кодексу Франції передбачено відповідальність за кібер-сталкінг, що також доцільно врахувати під час прийняття відповідного національного закону.

На особливу увагу в контексті євроінтеграції заслуговує досвід протидії сталкінгу у пострадянських країнах, які вже є повноправними членами ЄС.

Так, в Естонії кримінальна відповідальність за переслідування передбачена ст. 157-3 «Нав'язливе переслідування» Кримінального кодексу Естонської Республіки, відповідно до якої прагнення до повторного або тривалого контакту з особою, стеження за особою чи втручання у приватне життя особи проти її волі іншим способом, якщо метою або наслідком таких дій є залякування, приниження або інше суттєве занепокоєння особи, карається штрафом або позбавленням волі строком до одного року. Положення статті 157-3 КК Естонії застосовуються не лише до випадків фізичного переслідування, але і до переслідувань, що здійснюються через Інтернет чи з використанням цифрових технологій.

Також у кримінальному законодавстві Естонії передбачено такий окремий вид кримінального правопорушення як приватне спостереження, що вчиняється з метою переслідування, тобто незаконне слідкування за особою, що здійснюється з метою збору даних про таку особу задля переслідування – карається штрафом або позбавленням волі на строк до трьох років (стаття 137 КК Естонії) [9].

Таким чином, вказані положення Кримінального кодексу Естонської Республіки поширюються і на випадки кібер-сталкінгу (переслідувань оосби, що здійснюються за допомогою Інтернет або з використанням інших цифрових технологій).

Відповідно до статті 132-1 Кримінального кодексу Латвійської Республіки переслідування – це повторне або тривале стеження, слідкування за особою, вчинення погроз щодо особи або небажане спілкування з особою, якщо така особа мала підстави побоюватися за свою безпеку чи безпеку своїх близьких – карається позбавленням волі на строк до одного року або тимчасовим позбавленням волі, або пробаційним наглядом, або громадськими роботами, або штрафом. Ті самі дії, якщо вони вчинені щодо особи, з якою особа, що вчинила кримінальне правопорушення, перебуває в першому або другому ступені споріднення або щодо одного з подружжя чи колишнього з подружжя, або щодо особи, з якою особа, що вчинила кримінальне правопорушення, перебуває чи перебувала у постійних інтимних стосунках, або щодо особи, з якою особа, що вчинила кримінальне правопорушення, має спільне (нероздільне) майно – карається позбавленням волі на строк до трьох років або тимчасовим позбавленням волі, або пробаційним наглядом, або громадськими роботами, або штрафом [9].

Для України позитивним прикладом, що заслуговує на імплементацію в національне законодавство, є формулювання вищевказаних кваліфікуючих ознак сталкінгу у латвійському Кримінальному кодексі.

Згідно зі статтею 148-1 Кримінального кодексу Литовської Республіки незаконне переслідування особи, тобто систематичне переслідування потерпілого всупереч його чітко вираженої волі без законних на те підстав, внаслідок якого потерпілий був змушений змінити

місце проживання, місце роботи чи навчальний заклад або іншим чином зазнав негативного впливу на своє суспільне життя або емоційний стан – карається громадськими роботами або штрафом, або обмеженням волі, або арештом. Особа несе відповідальність за переслідування лише за наявності заяви потерпілого чи заяви його законного представника, вимоги прокурора або у разі початку досудового розслідування після виявлення ознак домашнього насильства [9].

Не менш важливим для України є досвід протидії сталкінгу та кібер-сталкінгу у Великобританії та Ірландії, адже в країнах загального права під законодавче врегулювання підпадають найбільш чутливі питання (проблеми).

Так, у Великобританії питання запобігання та протидії сталкінгу регулюються спеціальними законами: «Про захист від переслідування» 1997 року, «Про захист свобод» 2012 року та «Про захист від сталкінгу» 2019 року, якими визначено засади, підстави та умови захисту осіб від ризиків, пов'язаних із переслідуванням та суміжними діяннями. Під сталкінгом розуміється злочинна агресивна поведінка, спрямована на переслідування певної особи. Законодавчо встановлено, що акти сталкінгу включають такі дії: стеження за людиною; намагання контактувати або спроба зв'язатися з особою будь-яким способом; публікація будь-якої приватної інформації чи іншого компрометуючого матеріалу про певну особу або яка нібито походить від особи; постійний моніторинг використання особою мережі Інтернет, електронної пошти чи будь-якої іншої форми електронного зв'язку; перебування в будь-якому місці (державному чи приватному) з метою організації випадкової зустрічі з жертвою; навмисне посягання на будь-яке майно, що знаходиться у володінні або користуванні особи (жертви); спостереження або шпигування за особою (жертвою) [9].

Таким чином, в законодавстві Великобританії найбільш повно описані всі можливі способи вчинення сталкінгу як протиправного переслідування особи.

Для кваліфікації девіантної поведінки як сталкінгу у Великобританії достатньо двох інцидентів за умови, що правопорушнику відомо про небажаність його дій: це можуть бути два телефонних дзвінки незнайомій людині (жертві), два подарунки, два випадки переслідування тощо. Правопорушник, винуватий у вчиненні сталкінгу, позбавляється волі на строк, що не перевищує 51 тиждень або до нього застосовується штраф чи обидва покарання одночасно.

Переслідування, пов'язане із погрозою насильства, що має наслідком постійне перебування жертви у тривожному стані або стані занепокоєння, страждань, які здійснюють суттєвий негативний вплив на повсякденну діяльність особи, є за англійським законодавством обтяжуючими обставинами. У таких випадках порушник карається позбавленням волі на строк не більше п'яти років або штрафом чи поєднанням цих двох видів покарань. Якщо ж під час судового розгляду за пред'явленим обвинуваченням присяжні визнають особу-порушника невинуватою, то вони можуть, з огляду на фактично заподіяну шкоду, визнати цю особу винуватою у вчиненні іншого правопорушення (заподіяння тілесних ушкоджень, замах на життя жертви, сексуальні домагання тощо) [9].

Закон Великобританії «Про захист від сталкінгу» регламентує питання видачі захисного ордеру або тимчасового наказу про захист від переслідування, наслідки їх невиконання тощо (тобто процедурні питання).

В Ірландії 9 лютого 2021 року набув чинності Закон «Про переслідування, шкідливу комунікацію та пов'язані правопорушення», відомий як «Закон Коко» (названий на честь Ніколь Фокс, яка покінчила життя самогубством у 2018 році після серії знущань та публікацій її інтимних зображень в мережі Інтернет). Результатом прийняття цього закону стала криміналізація таких діянь: розповсюдження або публікація інтимних зображень без згоди постраждалої особи та з умислом завдати їй моральної чи матеріальної шкоди (карається позбавленням волі до семи років або штрафом); фото-, відеозйомка, розповсюдження або публікація інтимних зображень без згоди особи, навіть якщо немає конкретного наміру порушника завдати моральної чи матеріальної шкоди потерпілому (карається штрафом у розмірі п'ять тисяч євро та/або позбавленням волі на дванадцять місяців); одноразове надсилання погрозливого або грубо образливого

повідомлення, якщо особа, яка надсилає повідомлення, має намір завдати шкоди особі, яка є одержувачем такого повідомлення (карається позбавленням волі на два роки та/або штрафом) [9].

Крім того, у 2023 році в Ірландії набрав чинності закон «Про кримінальне правосуддя», яким значно посилено відповідальність за вчинення актів сталкінгу та запроваджено нові види кримінально карних діянь. Особа вважається винуватою у переслідуванні якщо: без законних повноважень або розумного виправдання постійно своїми діями навмисно чи необережно втручається у спокій та приватне життя іншої людини, або дії особи призводять до спричинення шкоди, викликають тривогу або занепокоєння; особа на постійній основі стежить або шпигує за іншою особою; фізично чіпляється до певної особи; розголошує приватну інформацію про особу; втручається у власність людини (включно з домашніми тваринами); здійснила пошкодження майна; намагається контактувати з особою без її згоди; використовує без згоди особи електронні комунікаційні або інформаційні системи з метою спостереження за нею; порушує вимоги ордеру суду, в якому встановлено заборони щодо спілкування та наближення до постраждалої особи, перебування або наближення до місць її проживання, навчання чи роботи [9].

У випадку, якщо переслідування не потягло за собою настання тяжких наслідків, то покарання передбачає засудження у спрощеному порядку та позбавлення волі на строк, що не перевищує дванадцяти місяців та штраф. За наявності обтяжуючих обставин або тяжких наслідків, спричинених переслідуванням, передбачено покарання у виді позбавлення волі на строк до десяти років та штрафу. Також вказаним законом збільшено максимальне покарання за переслідування із заподіянням шкоди у випадках домашнього або сексуального насильства до десяти років позбавлення волі [9].

Об'єктивна сторона цього виду кримінального правопорушення за ірландським законодавством також включає домагання, тобто будь-яку агресивну поведінку, яка провокує втручання у приватне життя людини та викликає тривогу, страждання, занепокоєння, страх чи образу. За умисну публікацію або трансляцію матеріалів, зображення (фотографії) жертви у соціальних мережах або в мережі Інтернет з метою її висміювання, дискредитації або приниження гідності та заподіяння моральної шкоди передбачено покарання у виді позбавлення волі на строк не більше трьох років і штрафу [9].

Таким чином, відповідальність за сталкінг та кібер-сталкінг в країнах Європи є достатньо суворою, що необхідно врахувати під час доопрацювання та прийняття аналогічного національного закону.

На розвиток положень щодо відповідальності за «сталкінг» Європейською Комісією прийнята Директива щодо протидії насильству над жінками та домашньому насильству № 2022/0066, якою пропонується криміналізувати кіберпереслідування (англ. cyber stalking) як сучасну форму психологічного насильства, що часто вчиняється проти членів сім'ї або осіб, які живуть в одному будинку, яке може вчинятися колишніми партнерами або знайомими [9].

Відповідно до ст. 8 вказаної Директиви кримінально караним кіберпереслідуванням є така умисна поведінка: вчинення погроз або залякування особи, що має постійний характер, шляхом використання інформаційних та комунікаційних технологій, що призвело до страху особи за власну безпеку або за безпеку осіб, які перебувають у неї на утриманні; постійний нагляд за особою без її згоди або законного дозволу, що здійснюється шляхом інформаційних та комунікаційних технологій з метою відстеження та контролю за пересуванням та діями такої особи; створення матеріалу, що містить персональні дані особи, без її згоди, доступного для невизначеної кількості кінцевих користувачів, шляхом використання інформаційних та комунікаційних технологій з метою підбурювання таких кінцевих споживачів завдати особі фізичної чи значної психічної шкоди [9].

Відсутність законодавчого регулювання поняття «сталкінгу» та «кібер-сталкінгу» в Україні обумовлює актуальність законодавчого врегулювання даного питання.

Наразі до Верховної Ради України подано проект Закону України «Про внесення змін

до Кримінального процесуального кодексу України та Закону України «Про запобігання та протидію домашньому насильству» щодо встановлення відповідальності за злочинне переслідування (сталкінг)», які розроблено у зв'язку з необхідністю удосконалення організаційно-правових засад щодо встановлення відповідальності за злочинне переслідування (сталкінг та кібер-сталкінг) та врахування положень Цивільного процесуального кодексу України у кримінальному судочинстві в частині застосування обмежувальних заходів щодо осіб, які вчинили домашнє насильство.

Автори законопроекту наголошують на тому, що українське суспільство повинне зрозуміти, що сталкінг – це не просто «новомодний» закордонний термін, а серйозна проблема, яка може нести за собою трагічні наслідки. Наприклад, за даними найбільш раннього дослідження в США за 1998 рік, три чверті постраждалих жінок, яких переслідували, піддавалися в подальшому фізичному насильству. Від того часу ситуація суттєво не змінилась, сталкінг досі залишається серйозною проблемою [9].

Таким чином, якнайскоріше внесення змін до Кримінального процесуального кодексу України та Закону України «Про запобігання та протидію домашньому насильству» щодо встановлення відповідальності за протиправне переслідування (сталкінг та кібер-сталкінг) має забезпечити наближення національних стандартів захисту прав і свобод людини до відповідних європейських норм та принципів у сфері правового регулювання вказаних суспільних відносин.

На увагу заслуговує також позитивний досвід зарубіжних країн у сфері протидії правопорушенням, які вчиняються із використанням соціальних мереж та месенджерів.

Так, французька прокуратура розслідує справу засновника Telegram Павла Дурова за 12 статтями, що передбачають відповідальність за співучасть у кіберзлочинах; незаконне надання криптографічних послуг та інструментів для забезпечення конфіденційності; відмову передавати інформацію, необхідну для проведення розслідувань, за запитом правоохоронних органів; співучасть у зберіганні порнографічного контенту з неповнолітніми; співучасть у шахрайстві; відмивання грошей, отриманих злочинним шляхом; співучасть у розповсюдженні наркотиків тощо [10; 11].

Реагуючи на зазначене розслідування адміністрація Telegram офіційно зобов'язалася передавати IP-адреси та номери телефонів правопорушників відповідним правоохоронним органам у відповідь на законні запити. Проте, як зазначають представники українського парламенту, Telegram буде передавати дані про порушників європейським спецслужбам, але не українським [12; 13].

Водночас за рішенням РНБО працівникам національних органів публічної адміністрації, а також військовослужбовцям взагалі заборонили користуватися Telegram. Так, РНБО було прийнято рішення щодо заборони встановлення та використання Telegram на службових пристроях працівників органів державної влади, військовослужбовців, працівників сектору безпеки і оборони, а також підприємств – операторів критичної інфраструктури [14].

Обґрунтовуючи необхідність прийняття вказаного рішення, представники Служби безпеки України та Генерального Штабу Збройних Сил України зазначили, що месенджер «Telegram» активно використовується ворогом (представниками російської федерації) для здійснення кібератак, розповсюдження фішингу та шкідливого програмного забезпечення (вірусів), встановлення геолокації користувачів, корегування ракетних ударів тощо [14].

Таким чином, РНБО своєчасно прийняла важливе рішення для протидії кіберзагрозам та правопорушенням у сфері використання інформаційних технологій.

Щодо загальноєвропейського досвіду у даній сфері суспільних відносин, слід зазначити, що у Європейському Союзі ще у 2016 році було прийнято Загальний регламент про захист даних (General Data Protection Regulation, GDPR). Цей загальноєвропейський нормативний акт дозволяє органам публічної адміністрації видаляти незаконний контент та змушує адміністраторів онлайн платформ докладати зусилля для боротьби з небезпечним контентом [15].

Загальний регламент захисту даних (GDPR) накладає зобов'язання на організації (адміністрацію інтернет-платформ) незалежно від їх місцезнаходження, якщо вони збирають дані,

пов'язані з громадянами держав-членів ЄС. Отже, вимоги GDPR поширюються і на резидентів України, якщо їх діяльність (зокрема, збір персональних даних) торкається прав і свобод громадян держав-членів ЄС.

Загальний регламент захисту даних (GDPR) набув чинності 25 травня 2018 року. Він передбачає стягнення значних за розміром штрафних санкцій з осіб, які будуть порушувати стандарти конфіденційності та безпеки, причому штрафи сягатимуть десятків мільйонів євро. За допомогою GDPR Європа демонструє свою чітку позицію щодо необхідності дотримання конфіденційності та безпеки даних у той час, коли все більше людей довіряють свої особисті дані онлайн платформам, хмарним сервісам (службам), а вищевказані порушення є щоденним явищем [15].

Враховуючи євроінтеграційні прагнення України, аналогічний закон має бути прийнятий і Верховною Радою України з метою ефективної протидії правопорушенням у сфері забезпечення конфіденційності персональної інформації користувачів Інтернет та безпеки даних в цілому.

Висновки. Проведене дослідження зарубіжного досвіду протидії правопорушенням у сфері використання інформаційних технологій дозволяє сформулювати висновок про необхідність запозичення позитивного європейського досвіду у сфері захисту персональних даних, зокрема, в частині прийняття Загального регламенту про захист даних (General Data Protection Regulation, GDPR), який розширює повноваження органів публічної адміністрації у сфері захисту персональних даних, а також у сфері правового регулювання діяльності соціальних мереж та месенджерів.

Відповідні зміни необхідно внести в національне законодавство з метою адаптації національних стандартів у сфері захисту персональних даних до права ЄС, а також ефективній протидії поширенню забороненого законом контенту в соціальних мережах та месенджерах. Також доцільним вбачається посилення відповідальності за порушення недоторканості приватного життя (ст. 182 КК України), а також порушення законодавства про захист персональних даних (ст. 188-39 Кодексу України про адміністративні правопорушення).

Проведене дослідження також актуалізує питання прийняття Закону України «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про запобігання та протидію домашньому насильству» щодо встановлення відповідальності за злочинне переслідування (сталкінг)».

Необхідність узагальнення позитивного зарубіжного досвіду у сфері протидії іншим правопорушенням у сфері використання інформаційних технологій обумовлює перспективність подальшого дослідження даної теми.

ЛІТЕРАТУРА:

1. Біленська Д.О. Адміністративно-правове регулювання інформаційних відносин в Україні: автореф. дис. ... канд. юрид. наук: 12.00.07 «адміністративне право і процес; фінансове право; інформаційне право»; Нац. юрид. ун-т ім. Ярослава Мудрого. Харків, 2016. 20 с.

2. Берназюк О.О. Цифрові технології у праві: сучасний погляд у майбутнє: монографія. Ужгород: Гельветика, 2020. 525 с.

3. Ковальова Т.В., Гунбіна О.В. Правові проблеми надання адміністративних послуг з використанням інтернет-технологій. *Наукові перспективи. Серія «Право».* 2021. № 9 (15). С. 260-271. URL: http://perspectives.pp.ua/index.php/np/article/download/483/486.

4. Комаров О.В. Адміністративно-правовий статус суб'єктів здійснення цифрової трансформації регіону. *Юридична наука.* 2020. № 12 (114). С. 122-128.

5. Краковська А.Є., Бабик М.К. Цифровізація адміністративних послуг в Україні: проблеми та перспективи розвитку. *Науковий вісник Ужгородського Національного Університету. Серія ПРАВО.* 2022. Випуск 70. С. 329-334.

6. Омельченко А.В. Суспільні відносини у сфері цифровізації як предмет правового регулювання. *Юридична Україна.* 26.12.2023. DOI 10.37749/2308-9639-2023-10(250)-5

7. Стефанчук Р. Інформаційні технології та право: quo vadis? *Право України.* 2018. № 1. С. 30-50.

8. Тищенкова І.О. Адміністративні процедури надання електронних публічних послуг публічною адміністрацією в Україні. *Форум права.* Юридичний форум. 2017. № 2. С. 124-129.

9. Проект Закону про внесення змін до Кримінального процесуального кодексу України та Закону України «Про запобігання та протидію домашньому насильству» щодо встановлення відповідальності за злочинне переслідування (сталкінг). Картка законопроекту. Пояснювальна записка. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/44972 (дата звернення: 05.10.2024).

10. Артемчук О. Французька прокуратура розслідує справу засновника Telegram Дурова за 12 статтями. *Економічна правда.* 26.08.2024. URL: https://www.epravda.com.ua/news/2024/08/26/718504/ (дата звернення: 01.09.2024).

11. Communiqué de presse. La Procureure de la Lepublique. Paris, le 26 août 2024. URL: https://www.tribunal-de-paris.justice.fr/sites/default/files/2024-08/2024-08-26 – CP TELEGRAM .pdf (дата звернення: 01.09.2024).

12. Du Rove's Channel. Paul Du Rove, edited Sep 23 at 16:09. URL: https://t.me/durov/345 (дата звернення: 24.09.2024).

13. Telegram буде передавати дані про порушників європейським спецслужбам, але не українським, – нардепка. Антикор. 23.09.2024. URL: https://antikor.com.ua/articles/725683-telegram_budet_peredavatj_dannye_o_narushiteljah_evropejskim_spetssluhbam_no_ne_ukrainskim_-_nardep (дата звернення: 24.09.2024).

14. Працівникам державних органів та військовослужбовцям заборонили користуватися Telegram – РНБО. Судово-юридична газета. Публікації. 20.09.2024. URL: https://sud.ua/uk/news/publication/311056-rabotnikam-gosudarstvennykh-organov-i-voennosluzhaschim-zapretili-polzovatsya-telegram-snbo (дата звернення: 21.09.2024).

15. What is GDPR, the EU's new data protection law? GDPR.EU. URL: https://gdpr.eu/what-is-gdpr/ (дата звернення: 01.09.2024).