DOI: 10.31359/2079-6242-2022-45-149
УДК 343.41:343.9

Є. В. Полях, аспірантка відділу кримінологічних досліджень Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України

КРИМІНОЛОГІЧНА ДЕТЕРМІНАЦІЯ ПОРУШЕННЯ НЕДОТОРКАННОСТІ ПРИВАТНОГО ЖИТТЯ

Постановка проблеми. Будь-яка система, у тому числі й соціальна, має схильність до розвитку, який, у свою чергу, відбувається під впливом великої кількості чинників, що можуть як стимулювати прогресивно орієнтовані зміни, так і стримувати появу останніх, нерідко призводячи до регресу. Такими чинниками виступають детермінанти, а, власне, процес обумовлення одного явища іншим має назву «детермінація». Під детермінацією (від лат. «*determinio*» – визначаю[1]) розуміють підпорядкований об'єктивним законам природи і суспільного розвитку складний процес породження, зумовлення, взаємних трансформацій і динамічних змін явищ, процесів, подій та станів оточуючої дійсності. У процесі детермінації відбувається безперервне відтворення й оновлення різних форм життя, типів відносин, класів явищ і процесів[2].

Теорія детермінації заснована на концепції детермінізму – філософському підході до причинно-наслідкових зв'язків, а фундаментом теорії виступає вчення про універсальний зв'язок у світі, який проявляється у діалектичних формах взаємозалежності та взаємодії[3]. Розгалуженням загальної концепції детермінізму є соціальний детермінізм[4]. У межах теорії соціальної детермінації пояснюється процес спричинення та обумовлення соціальних явищ та процесів, а також розкриваються їх взаємні зв'язки.

Різновидом соціальної детермінації є кримінологічна детермінація[5]. Детермінація злочинності розкриває відношення, взаємозв'язок та взаємодію між явищами, процесами, станами, подіями суспільного життя, що породжують та зумовлюють злочинність[6]. У свою чергу, вчення про детермінацію злочинності є методологічною основою наукового обґрунтування заходів запобігання злочинності, адже система протидії злочинності повинна спрямовуватися на явища та процеси суспільного життя, які причинно зумовлюють її функціонування та розвиток[7]. Таким чином, при дослідженні злочинності вбачається практична значимість установлення криміногенних факторів, тобто чинників, що спричинюють та зумовлюють злочинність, а також знаходяться у різноманітних взаємозв'язках з нею. Зазначене є актуальним для дослідження й окремих різновидів злочинності, зокрема кримінальних правопорушень проти приватності особи.

Аналіз останніх досліджень і публікацій. Слід констатувати, що єдиними науковцями на теренах України, які досліджували кримінологічні фактори порушення недоторканності приватного життя, є В. Д. Басай та І. Б. Король. У 2015 р. вийшла спільна стаття названих дослідників під назвою «Кримінологічні фактори (загрози) порушен-

[1] Закалюк А П *Курс сучасної української кримінології: теорія і практика:* у 3 кн. Кн. 1: *Теоретичні засади та історія української кримінологічної науки* (Видавничий Дім «Ін Юре», 2007) 424

[2] Головкін Б М 'Причинність у системі детермінації злочинності' (2014) 1 Теорія і практика правознавства: електрон. наук. фах. вид. <https://dspace.nlu.edu.ua/bitstream/123456789/6358/1/Golovkin.pdf> (дата звернення: 18.01.2023) 1

[3] Закалюк А П *Курс сучасної української кримінології: теорія і практика:* у 3 кн. Кн. 1: *Теоретичні засади та історія української кримінологічної науки* (Видавничий Дім «Ін Юре», 2007) 424

[4] 'Causal Determinism' (2016) Jan 21 Stanford Encyclopedia of Philosophy Archive <https://plato.stanford.edu/archives/spr2016/entries/determinism-causal> (Last accessed: 18.01.2023)

[5] Кузнецова Н Ф *Проблемы криминологической детерминации* (М.: МГУ, 1984) 208

[6] Головкін Б М 'Про детермінацію злочинності' (2020) 1 Часопис Київського університету права 274–280

[7] Новіков О В 'Недоліки й прорахунки політики держави в епоху постіндустріальної економіки як детермінуючий комплекс злочинності у сфері інтелектуальної власності' (2014) 4 Юридичний вісник 338–342

ня права на недоторканність приватного життя»[1], яка стала основою для відповідного підрозділу дисертації І. Б. Король «Охорона недоторканності приватного життя: кримінально-правові та кримінологічні аспекти» (2015)[2].

У зазначених роботах вчені визначили кримінологічні фактори порушення недоторканності приватного життя, які умовно поділили на усталені та новітні загрози приватності. До усталених загроз приватності вони віднесли: відсутність прозорості в діяльності органів державної влади та правоохоронних органів; недостатню контрольованість діяльності спеціальних правоохоронних структур і використання ними спеціальних засобів негласного зняття, фіксування та передачі інформації; відсутність загальної культури та традицій поваги до приватності, а також соціальних і правових норм поведінки у зв'язку з необхідністю дотримання права на недоторканність приватного життя; низький рівень правової культури службових осіб, які мають доступ до відомостей про приватне життя особи; відсутність корпоративної відповідальності за розголошення особистих даних; недостатній рівень професіоналізму і правової культури працівників засобів масової інформації, а також недосконаліть правових механізмів захисту приватності у співвідношенні з правом на інформацію[3]. Ці кримінологічні фактори, на думку науковців, виникають внаслідок специфічного ставлення до проблем приватності на пострадянському просторі, а також через низький рівень розвитку інститутів демократичного суспільства і правової держави (недоліки судової системи, брак професіоналізму та майже повна відсутність відповідальності засобів масової інформації, бездіяльність чи низька активність інститутів громадянського суспільства)[4].

До новітніх же загроз приватності вчені віднесли: появу та використання нових технологій для збирання, зберігання, поширення і використання персональної інформації; посилення політики держав щодо обмеження права на недоторканність приватного життя у зв'язку з новими загрозами громадській безпеці, поширенням тероризму і радикалізму; появу нових суб'єктів посягань на приватність – комерційних компаній і корпорацій, які втручаються у приватне життя в інтересах бізнесу та отримання прибутку; появу нових форм посягань на недоторканність приватного життя з боку засобів масової інформації[5]. Новітні загрози приватності зумовлені стрімким розвитком сучасних технологій, переходом до інформаційного суспільства та вільного інформаційного простору. Їх особливістю є те, що, зважаючи на різноманітність їх проявів та стрімкий розвиток, вони не враховані і не можуть бути повною мірою враховані законодавцем під час конструювання правових норм[6].

У цей самий час, незважаючи на очевидну цінність напрацювань вказаних дослідників, вважаємо, що такий поділ є неповним та непрактичним з погляду на необхідність систематизації заходів запобігання порушенням недоторканності приватного життя.

Отже, **метою статті є** встановлення криміногенних чинників, що зумовлюють сучасні порушення недоторканності приватного життя.

Виклад основного матеріалу. Почнемо з того, що згрупуємо зазначені криміногенні чинники у такий спосіб: чинники, що пов'язані із цифровізацією суспільних відносин; чинники, що пов'язані з недостатнім захистом інформації; чинники, що пов'язані з роботою правоохоронних органів, а також соціально-економічні, соціально-політичні (правові), соціально-культурні та віктимологічні чинники.

Визначальну роль у детермінаційному комплексі порушень приватності відіграють *чинники, пов'язані із цифровізацією суспільних відносин.* Упродовж другої половини XX ст. в економічно розвинених країнах поступово був здійснений перехід від індустріального суспільства до такої історичної фази еволюційного розвитку, як «постіндустріальна ера», або «вік інформації»[7]. За сво-

[1] Басай В Д, Король І Б 'Кримінологічні фактори (загрози) порушення права на недоторканність приватного життя' (2015) 3 Частина 2 Право і суспільство 174–180

[2] Король І Б 'Охорона недоторканності приватного життя: кримінально- правові та кримінологічні аспекти' (автореф. дис. канд. юрид. наук, Львів, 2015) 22

[3] Король І Б 'Охорона недоторканності приватного життя: кримінально- правові та кримінологічні аспекти' (автореф. дис. канд. юрид. наук, Львів, 2015) 13

[4] Басай В Д, Король І Б 'Кримінологічні фактори (загрози) порушення права на недоторканність приватного життя' (2015) 3 Частина 2 Право і суспільство 174–180 (с.177)

[5] Король І Б 'Охорона недоторканності приватного життя: кримінально- правові та кримінологічні аспекти' (автореф. дис. канд. юрид. наук, Львів, 2015) 13

[6] Басай В Д, Король І Б 'Кримінологічні фактори (загрози) порушення права на недоторканність приватного життя' (2015) 3 Частина 2 Право і суспільство 174–180

[7] Головко А Я 'Постіндустріальна трансформація світового господарства в контексті формування концепції соціальної відповідальності ТНК' (2013) 9 Ефективна економіка: електрон.

єю природою цифрові технології не існують у вакуумі, адже вони можуть бути як потужним інструментом просування людського прогресу, що значною мірою сприяє заохоченню та захисту прав людини, так й нести дуже серйозні ризики для людської гідності, автономії та недоторканності приватного життя, а разом із тим й для здійснення прав людини в цілому, якщо вони застосовуються без ефективних гарантій. Оцінюючи реальні та потенційні ризики, потрібно розуміти, що всі сучасні девайси міцно пов'язані з Інтернетом і оновлюються ззовні, отже, й управляються вони так само ззовні. Технології, які потребують великого обсягу даних та «живляться» ними (наприклад, додатки штучного інтелекту, що покликані навчитися приймати самостійні рішення без будь-якого втручання людини), сприяють створенню цифрового середовища, в якому як держави, так і комерційні підприємства мають все більше можливостей відстежувати, аналізувати, прогнозувати і навіть маніпулювати поведінкою людей. Таким чином, можна зробити висновок, що персональні дані особи у кінцевому підсумку просто не належать їй. Тому є справедливим висловлювання *(мовою оригіналу)*, що «privacy as we knew it in the past is no longer feasible… How we conventionally think of privacy is dead»[1]. Про це говорить й буквальне тлумачення нормативно-правових актів ЄС та США. Такий підхід є адекватним у наш час з точки зору важливості збору та обробки personal data для розвитку новітніх технологій, тоді як обмеження їх в обігу чи видалення взагалі гальмує такий процес.

У зв'язку з вищевказаним сьогодні доцільно вести мову про те, що такі потужні можливості призвели до цілковитої комерціалізації персональних даних. Отже, ще однією групою чинників, що порушують privacy, є *соціально-економічні.* Як стверджує М. Карчевський, у сучасних умовах до легального економічного обігу активно залучаються так звані «нетрадиційні» види майна[2], серед яких чільне місце посідають персональні дані, які, як зазначає Л. Детерманн, є новою нафтою цифрової економіки[3]. Оскільки такі види майна мають здатність приносити високі доходи з найнижчими ризиками, на них відповідним чином реагує й кримінальне середовище[4]. Як результат – поява все нових і нових видів злочинних посягань, які передбачають використання сучасних інформаційних технологій, оскільки стрімке поширення останніх робить неможливим повне, об'єктивне, своєчасне осмислення кримінальних нововведень у кіберпросторі.

Сьогодні більшість постачальників послуг (включаючи роздрібні онлайн-магазини) намагаються збирати інформацію про поведінку своїх потенційних користувачів/клієнтів (так звані «поведінкові дані») і використовувати останні для збільшення своїх продажів, пропонуючи персоналізовані послуги або навіть впливаючи на поведінковий маркетинг споживачів товарів і послуг. Це може принести користь обом сторонам, оскільки люди можуть насолоджуватися доступом до різноманітних онлайн-сервісів, новинних сайтів, електронної пошти, соціальних мереж, відео, музики тощо без прямої оплати грошима, однак багато людей можуть навіть не знати, що вони платять своїми персональними даними, які збираються та використовуються лише тому, що вони сліпо прийняли політику конфіденційності, умови надання послуг або cookie, які пропонують ці вебсайти. До того ж, такі дані можна використовувати не лише для прибутку з продажу, реклами тощо, їх можна продати як окремий об'єкт за чималі кошти. Ю. Когут із посиланням на М. Побокіна визначає, що «за дослідженнями IBM Security та Ponemon Institute, середня ціна навіть порівняно невеликого витоку інформації (від 2 500 до 100 тис. облікових записів) складає 3,87 млн дол., а великі витоки обходяться, як мінімум, у 40 млн дол.[5]. Отже, персональні дані, інші відомості про приватне життя стали джерелом формування капіталу.

журн. <http://www.economy.nayka.com.ua/?op=1&z=2330> (дата звернення: 15.01.2023)

[1] AFP and Prigg M, 'Harward professors warn 'privacy is dead' (2015) Jan 25 The Sunday Times 2 (Sri Lanka) Page 5 <https://www.pressreader.com/sri-lanka/sunday-times-sri-lanka/20150125/282153584681118> (Last accessed: 18.01.2023)

[2] Карчевский Н В '«Киберпреступление» или преступление в сфере использования информационних технологий?' *Кібербезпека в Україні: правові та організаційні питання:* матеріали Всеукр. наук.-практ. конф. (м. Одеса, 21 жовт. 2016 р.) 10–14

[3] Determann L, 'No One Owns Data': articles (2018) Vol. 70:1 Hastings Law Journal Pages 1–44. <https://www.researchgate.net/publication/323617530_No_One_Owns_Data> (Last accessed: 18.01.2023)

[4] Бегма А П, Ховпун О С 'Розслідування злочинів в ІТ-сфері' (2021) 28 Наукові праці Національного університету «Одеська юридична академія» (Одеса: Видавничий дім «Гельветика») 12–19

[5] Когут Ю І *Кібербезпека та ризики цифрової трансформації компаній: практичний посібник* (Консалтингова компанія «СІДКОН», 2022) 372

Політична еліта в багатьох країнах оцінила зазначені вище ризики доволі пізно, тому не менш важливими є *соціально-політичні (правові) чинники* порушень недоторканності приватного життя. Вони пов'язані із недоліками функціонування як політичної, так і правової систем суспільства, що проявляється у нехтуванні суспільними інтересами та вимогами у ході прийняття політичних рішень, нестабільності та недосконалості законодавства, що неспроможне забезпечувати правове регулювання та ефективний захист суспільних відносин, а також призводить до виникнення криміногенних детермінант, які, в свою чергу, породжують злочинність.

Українське суспільство є активним користувачем усіх технічних благ, які передбачають обробку персональних даних (онлайн-торгівлі, онлайн-банкінгу та інших онлайн-послуг, у тому числі державних). Через таке суттєве збільшення активності обробки даних у мережі Інтернету українське середовище privacy дуже змінилося, а тому чинний Закон України «Про захист персональних даних», у якому відбито норми Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних 1981 року, та інші нормативно-правові акти у сфері захисту personal data є застарілими і, як наслідок, недієвими. Україна не ратифікувала так звану Конвенцію 108+, оскільки це вимагає відповідності її вимогам. Стосовно імплементації положень GDPR (General Data Protection Regulation), що спрямовані на гармонізацію захисту основних прав і свобод фізичних осіб щодо діяльності з переробки і на забезпечення вільного потоку персональних даних між державами-членами ЄС, то влітку 2021 р. у Верховній Раді України був зареєстрований законопроект № 5628 «Про захист персональних даних», покликаний підвищити рівень захисту приватного життя українців та привести законодавство України у відповідність до міжнародних стандартів. Однак законодавці не підтримали його під час голосування[1]. Наразі оновлений проект Закону № 8153 від 25 жовтня 2022 р. зареєстровано знову, а комітети встигли оприлюднити свої висновки. Мета – ратифікувати вищевказані європейські акти та оновити законодавство України згідно з вимогами теперішнього часу, зробити його відповідним до технологій обробки персональних даних, які існують сьогодні[2]. Однак затримка у вирішенні цього питання, а також в оновленні інших нормативно-правових актів аналізованої сфери не лише гальмує розвиток країни на шляху євроінтеграції, а й створює сприятливі умови для подальших порушень захисту персональних даних та privacy в цілому.

Як справедливо зазначає І. Король, ще одним фактором порушень privacy є «посилення політики держав щодо обмеження права на недоторканність приватного життя у зв'язку з новими загрозами громадській безпеці, поширенням тероризму і радикалізму»[3], оскільки держави світу, в тому числі й Україна, повинні якимось чином реагувати на підвищені загрози національній безпеці, й одним із шляхів політики вбачають саме розширення повноважень органів публічної влади щодо доступу до personal data, їх збирання й опрацювання. Н. Уханова констатує, що обмеження прав людини, включаючи й право на privacy, є наслідком зменшення ролі демократичних цінностей у правовому режимі та підвищення необхідності забезпечення нацбезпеки задля збереження порядку управління, що існує в державі[4].

Звісно, будь-яка система не позбавлена слабких сторін захисту, а цифровізація має ще й іншу сторону – кіберзлочини, тобто «суспільно небезпечні винні діяння у кіберпросторі та/або з його використанням»[5], а тому доцільно вести мову про *чинники, що пов'язані з недостатнім захистом інформації.* Як слушно зазначає І. Король, «для збирання інформації використовуються спеціальні комп'ютерні програми-шпигуни, які непомітно для користувача збирають інформацію, задану за певними критеріями»[6], так звані «невідомі keyloggers» – шкідливе шпигунське програмне забезпечення, яке використовується для збору персональних даних, наприклад, паролів або фінансових даних, які потім відправляються третім особам для використання

[1] Проект Закону про захист персональних даних: від 07.06.2021 № 5628. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72160 (дата звернення: 16.01.2023)

[2] Проект Закону про захист персональних даних: від 25.10.2022 № 8153. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/40707 (дата звернення: 16.01.2023)

[3] Басай В Д, Король І Б 'Кримінологічні фактори (загрози) порушення права на недоторканність приватного життя' (2015) 3 Частина 2 Право і суспільство 174–180

[4] Уханова Н С 'Виклики і загрози правам та безпеці людини в інформаційній сфері' (2018) 4 (27) Інформація і право 33–45

[5] Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163 – VIII. URL: https://zakon.rada.gov.ua/laws/show/2163–19#Text (дата звернення: 16.01.2023)

[6] Басай В Д, Король І Б 'Кримінологічні фактори (загрози) порушення права на недоторканність приватного життя' (2015) 3 Частина 2 Право і суспільство 174–180

в злочинних цілях. Це можуть бути кілоґґери, що розробляються під егідою різних урядових організацій або які можуть створюватися розробниками різних закритих операційних систем і включатися до складу ядра операційної системи; або які розроблені в обмеженій кількості (часто тільки в одній або кількох копіях) для вирішення конкретного завдання, пов'язаного з викраданням критичної інформації з комп'ютера користувача; або що є модулями для перехоплення натискань клавіш на комп'ютері користувача, що включаються до складу програм-вірусів тощо[1]. Якщо пристрій заражений шпигунською програмою під назвою «keylogger», введена інформація вмить відправиться в руки стороннім особам, вона перехоплює весь текст, що вводиться з клавіатури, а разом із ним і суто особисту інформацію – ПІН-коди, логіни, паролі та ін. Варто не забувати й про використання методів соціальної інженері, тобто прихованих методів, які дають можливість «запрограмувати» особу до виконання певних дій, спрямованих на отримання суттєвої вигоди, причому це практично не потребує фінансових витрат (фішинг-атаки, таргінг, бейтинг, претекстинг, зворотна соціальна інженерія, метод «дорожнє яблуко», сайти-пастки тощо)[2].

Чинники які, пов'язані з роботою правоохоронних органів. «Додержання закону об'єктивно не може ґрунтуватись виключно на індивідуальній свідомості та добропорядності соціальних суб'єктів – це завдання правоохоронних та контрольних органів»[3]. Помилки, допущені слідчими та дізнавачами під час розслідування кримінальних правопорушень, є наслідком низької як загальної, так і спеціальної професійної підготовки. По-перше, чимало повідомлень про порушення права на недоторканність приватного життя безпідставно не вноситься в ЄРДР[4][5], або ж такі провадження закриваються дізнавачами передчасно[6] через намагання співробітників правоохоронних органів уникати розслідування кримінальних правопорушень, які важко кваліфікувати, довести вину та зібрати докази; значна кількість постанов слідчих і процесуальних керівників на стадії досудового розслідування не відповідає вимогам процесуального законодавства, є невмотивованими та необґрунтованими[7] тощо. Причиною ж низької спеціальної підготовки, на думку А. Бегми та О. Ховпуна, є «відсутність якісних методичних розробок, у реалізації яких були б повною мірою задіяні сучасні інформаційні технології»[8]. З одного боку, виявлення, розкриття та розслідування кримінальних правопорушень в ІТ-сфері (у тому числі й у сфері privacy) має чимало особливостей, виникають складнощі з виявленням, фіксацією та вилученням доказів. Існують великі ризики того, що криміналістично значуща інформація може бути ненавмисне змінена чи втрачена через допущені помилки працівниками органів досудового розслідування. З другого боку, існує питання обмеженої контрольованості діяльності таких суб'єктів під час провадження слідчих (розшукових) дій, зокрема негласних, адже під час збору доказової інформації у межах кримінального провадження працівникам правоохоронних органів стають відомі таємниці приватного життя осіб. Яскравим прикладом є ситуація, коли під час обшуку у в. о. начальниці Головного управління ДПС у м. Києві, яка підозрюється в корупційній діяльності, працівники ДБР знайшли списки її новорічних бажань та опублікували відповідні фото у соціальні мережі[9]. Такі фото не є доказами та стосуються приватного життя чиновниці, а орган досудового розслідування під час їх оприлюднення порушив кілька статей Конвенції про захист прав

[1] Keylogger <https://uk.wikipedia.org/wiki/Keylogger> (дата звернення: 17.01.2023)

[2] Половенко Л П, Мерінова С В 'Виявлення ознак соціальної інженерії та технологія протидії соціальним хакерам на підприємстві' (2019) 10 Підприємництво та інновації 183–187

[3] Гилинский Я И *Девиантология: социология преступности, наркотизма, проституции, самоубийств и других «отклонений».* 2-е изд., испр. и доп. (Юридический центр Пресс, 2007) 254

[4] Ухвала Ренійського районного суду Одеської області від 25 жовтня 2022 р., судова справа № 510/1761/22. URL: https://reyestr.court.gov.ua/Review/106941346 (дата звернення: 19.01.2023)

[5] Ухвала Жовтневого районного суду м. Дніпропетровська від 23 вересня 2022 р., судова справа № 201/6714/22. URL: https://reyestr.court.gov.ua/Review/106593267 (дата звернення: 19.01.2023)

[6] Ухвала Городенківського районного суду Івано-Франківської області від 31 березня 2022 р., судова справа № 342/221/22. URL: https://reyestr.court.gov.ua/Review/103814009 (дата звернення: 19.01.2023)

[7] Ухвала Дарницького районного суду міста Києва від 11 травня 2022 р., судова справа № 753/22/22. URL: https://reyestr.court.gov.ua/Review/104261528 (дата звернення: 19.01.2023)

[8] Бегма А П, Ховпун О С 'Розслідування злочинів в ІТ-сфері' (2021) 28 Наукові праці Національного університету «Одеська юридична академія». Одеса: Видавничий дім «Гельветика» 12–19

[9] Мазуренко А, Ткач М 'Соболина шуба, мільйон доларів і Breguet: під час обшуку у посадовиці податкової знайшли список бажань' (Українська правда, 1 лютого 2023) <https://www.pravda.com.ua/news/2023/02/1/7387432/> (дата звернення: 08.02.2023)

людини і основоположних свобод, зокрема і статтю 8, а також чинне процесуальне законодавство, а саме статті 7 та 15 КПК України. Крім того, правоохоронці досить часто порушують приписи чинного законодавства у сфері privacy під час здійснення заходів запобігання злочинності.

Соціально-культурні чинники вчинення порушень privacy отримують своє наочне виявлення у правовій свідомості суспільства, соціальних груп, окремої особи щодо ставлення до інституту приватного життя. Особа не є пасивним об'єктом, який лише сприймає вплив оточення, вона активно взаємодіє із середовищем, формуючи умови свого життя та, власне, особистість[1]. Вважаємо за доцільне виділити такі соціально-культурні фактори порушень приватності, як освітній і культурний рівень населення, менталітет, звичаї, традиції та стереотипи поведінки, а також рівень розвитку та духовної організації конкретної особи і всього населення в цілому. Українське суспільство, на думку І. Король, характеризується відсутністю загальної культури та традицій поваги до приватності, а також соціальних і правових норм поведінки у зв'язку з необхідністю дотримання права на недоторканність приватного життя[2]. Такий стан, на нашу думку, пов'язаний з ідеологічними штампами про пріоритет класових і суспільних інтересів над інтересами особистості, які були сформовані ще за радянських часів. Досить яскравим прикладом є практична діяльність мас-медіа, які демонструють порушення приватності задля чергового сенсаційного матеріалу. У своїй роботі журналісти нехтують не лише етичними принципами, а й порушують чимало приписів чинного національного та міжнародного законодавства. Так, дійсно, журналісти можуть «перетнути межу дозволеного» – втрутитися у приватне життя публічних осіб без їх згоди, але лише тоді, коли існує хвачений суспільний інтерес, який виправдовує оприлюднення інформації. Але ж проста цікавість або пошук сенсацій ніколи не можуть виправдати порушення privacy. Наприклад, журналістські розслідування про статки богослужителів, їх бізнес, що нерідко зареєстрований «в обхід закону»[3], дійсно становлять суспільний інтерес й можуть допомогти зафіксувати чималу кількість правопорушень, у тому числі й кримінальних, а ось поширення інформації про фізичну близькість секретаря Чернівецької єпархії УПЦ МП з 17-річним хлопцем, що співає в місцевому хорі[4], вже є прямим порушенням privacy.

Варто визнати й той факт, що порушення недоторканності приватного життя простежуються у побуті кожної людини. Батьки, члени подружжя нехтують або навіть зневажають особистий простір дітей чи один одного, підслуховуючи розмови, читаючи листування та ін. Вчителя не лише пліткують про учнів/студентів та їх родини, а й, маючи певну приватну інформацію, можуть привселюдно цькувати останніх, тим самим даючи витік такої інформації. Така сама ситуація існує з лікарями та лікарською таємницею, іншими професіями, представнице яких так чи інакше мають доступ не лише до personal data, а й іншої інформації про приватне життя особи.

Віктимологічні чинники. На нашу думку, всі віктимологічні чинники кримінальних правопорушень проти приватності доцільно розділяти на три групи: ті, що пов'язані з невіглаством потерпілого у зазначеній сфері; ті, що пов'язані з недбалим ставленням до свого приватного життя; ті, що пов'язані з кібергігієною користувачів інформаційних технологій.

В одному зі своїх досліджень науковиця А. Тренті згадує, що ще у 70-х роках XX ст. вчені наголошували, у комп'ютерних злочинах злочинець покладається, серед іншого, й на невігластво потерпілого. Дійсно, порушення права на недоторканність приватного життя є високо латентними. Такий стан пов'язаний з тим, що здебільшого люди не знають про правову регламентацію права на приватність у чинному міжнародному та національному законодавстві і, як наслідок, не розуміють, що є потерпілими від злочинних посягань

[1] Журавель А П Соціально-психологічні особливості та детермінанти формування особистості зі злочинною поведінкою (2020) (31 (71)) 3 Вчені записки ТНУ імені В. І. Вернадського. Серія: Психологія 76–80 <https://doi.org/10.32838/2709–3093/2020.3/13>

[2] Басай В Д, Король І Б 'Кримінологічні фактори (загрози) порушення права на недоторканність приватного життя' (2015) 3 Частина 2 Право і суспільство 174–180

[3] Стежар Т, Засаднюк А 'Бізнес-імперія УПЦ МП: звідки у божих людей беруться гроші на розкішні маєтки та автівки' (Інформаційне агенство «УНІАН», 13 грудня 2018) <https://www.unian.ua/politics/10376331-biznes-imperiya-upc-mp-zvidki-u-bozhih-lyudey-berutsya-groshi-na-rozkishni-mayetki-ta-avtivki.html> (дата звернення: 08.02.2023)

[4] Кошкіна С 'Обшуки в Чернівецько-Буковинській єпархії УПЦ МП: знайшли паспорт РФ у митрополита і 17-го річного хлопця в ліжку архімандрита' (LB.ua, 25 листопада 2022) <https://lb.ua/society/2022/11/25/537108_obshuki_chernivetskobukovinskiy.html> (дата звернення: 08.02.2023)

у цій сфері. Освіченість осіб можна охарактеризувати як опосередковану, оскільки вони не мають чітких знать ані про поняття privacy, ані про компоненти, що є складовими права на приватне життя. У свою чергу, це позначається й на тому, що люди не знають, що мають право на захист своєї приватності шляхом звернення до компетентних органів, зокрема, правоохоронних та судових.

Стан недостатньої обізнаності у сфері privacy провокує існування віктимологічних чинників, пов'язаних із недбалим ставленням до свого приватного життя. На наш погляд, проблема криється в бажанні людей ділитися різноманітними деталями своєї приватності (рівнем доходів, житловими умовами, сімейними стосунками, сексуальним життям, станом здоров'я тощо) на широкий загал заради популярності, монетизації свого блогу, банального задоволення своєї психологічної потреби здаватися краще за інших і т. п. Відомо чимало випадків, коли зловмисники збирали інформацію про життя блогерів, відстежуючи їхні акаунти в Instagram, щоб пограбувати їх будинки[1] чи завдати іншої шкоди як матеріальної[2], так фізичної й моральної. Великий сплеск активності у поширенні приватної інформації ще донедавна простежувався серед користувачів соціальних мереж, зокрема, блогерів та інфлуенсерів, однак останнім часом тенденція пішла на спад. Припускаємо, що такий стан пов'язаний, зокрема, з повномасштабним вторгненням рф на територію України, чисельними кібератаками на сайти органів публічної влади, онлайн-банкінги та акаунти користувачів у соціальних мережах, оскільки у XXI ст. поле бою – не лише географічне розташування лінії розмежування, а й інфопростір. Інформація у соціальних мережах, онлайн-платежі, історія місцезнаходжень, електронні листи, а також повідомлення, надіслані через платформи обміну миттєвими повідомленнями, – частина даних, які складають так званий «цифровий слід» особи, його повнота залежить від звичок поширення інформації та ставлення до конфіденційності. І найголовніше те, що стерти такий «слід», з точки зору так званого «ефекту Стрейзанд»[3], практично неможливо.

Існує тісний зв'язок між недбалим ставленням до власного приватного життя, неосвіченістю осіб у сфері privacy та гігієною кібербезпеки. Розгляд цієї групи чинників доцільно розпочати з визначення поняття «кібергігієна», оскільки у побуті пересічних користувачів існує хибна думка, що остання пов'язана з особистою гігієною, наприклад, протиранням клавіатури дезінфікуючими серветками чи дотриманням інших санітарно-гігієнічних норм роботи з гаджетами. Однак, кібергігієна, або гігієна кібербезпеки, являє собою набір корисних звичок, які доцільно використовувати як корпораціям, так й окремим особам із метою забезпечення безпеки персональних даних та їх захисту від потенційних крадіжок чи атак. Вона включає (але не обмежується цим): використання ліцензованих продуктів; аналіз програм, що завантажуються користувачем; регулярне оновлення операційних систем, програмного забезпечення, а також антивірусів та іншого програмного забезпечення безпеки; перевірку безпеки активних акаунтів; створення надійних паролів та додаткових рівнів захисту облікових записів; резервне копіювання інформації; ознайомлення з правилами конфіденційності, умовами надання послуг чи cookie; усвідомлене ставлення до підозрілих sms-повідомлень, гіперпосилань тощо. Здебільшого користувачі не дотримуються жодного з визначених вище правил, і початком цього є встановлення так званої «піратської» продукції – операційних систем, програмного забезпечення, антивірусів тощо. Попит на таку продукцію досить великий, оскільки користувачі таким чином намагаються мінімізувати витрати на задоволення пов'язаних із благами комп'ютерної ери потреб, однак їх використання не дає жодної гарантії захисту персональних даних осіб у порівнянні з ліцензійним продуктом. Не менш важливим є й регулярне оновлення програмного забезпечення задля виправлен-

[1] Малай К 'У Києві пограбували будинок відомої блогерки: вона була всередині. Відео з камер спостереження' (OBOZREVATEL, 4 листопада 2021) <https://news.obozrevatel.com/ukr/show/people/dyakuyu-scho-zalishili-zhivoyu-u-kievi-pograbuvali-kolishnyu-divchinu-kyivstoner-zlodii-potrapili-na-kameri-video.htm> (дата звернення: 08.02.2023)

[2] 'У франківської блогерки вкрали фари з нового автомобіля. ФОТО/ВІДЕО' (ІАА «Ратуша», 9 листопада 2020) <https://www. ratusha. if. ua/%d1%83-%d1%84%d1%80%d0%b0%d0%bd%d0%ba%d1%96%d0%b2%d1%81%d1%8c%d0%ba%d0%be%d1%97-%d0%b1%d0%bb%d0%be%d0%b3%d0%b5%d1%80%d0%ba%d0%b8-%d0%b2%d0%ba%d1%80%d0%b0%d0%bb%d0%b8-%d1%84%d0%b0%d1%80%d0%b8-%d0%b7/> (дата звернення: 08.02.2023)

[3] Феномен «ефект Стрейзанд» полягає в тому, що спроба видалити певну інформацію або обмежити доступ до неї призводить лише до її розповсюдження. Наприклад, спроба обмежити доступ до фотографії, файлу або тексту призводить до дублювання цієї інформації на інших серверах або появи її в файлообмінних мережах.

ня вразливостей та помилок у ньому (яке, до речі, неможливо виконати у «піратській» версії). Йдеться, зокрема, про антивіруси, що захищають операційну систему від потенційних вірусів, небажаних програм, а також відновлюють пошкоджені останніми файли. Користувачі нехтують безпекою своїх профайлів, зокрема, у соціальних мережах, створюючи ненадійні паролі (дата народження, номери телефонів чи поширені загальновідомі комбінації), нерідко – один для безлічі акаунтів, а також не використовують двофакторну аутентифікацію, що передбачає підтвердження особистості під час входу. Резервне копіювання інформації також має велике значення, оскільки захищає інформацію, у тому числі й приватну, не лише від знищення самим володільцем, а й від використання чи викрадення сторонніми суб'єктами, шифрування програмою-вимагачем або видалення шкідливим програмним забезпеченням, у разі проникнення такого до операційної системи. Однак існують й інші ризики: зовнішні жорсткі диски чи USB-накопичувачі як об'єкти матеріального світу досить легко втратити, а критичним недоліком так званих «хмарних» технологій є знаходження даних в різних місцях, через що не завжди можливо визначити правові норми, які слід застосувати для захисту інформації від суб'єктів, що можуть вимагати доступ до інформації[1]. Більшість людей сліпо приймає політику конфіденційності, умови надання послуг або cookie, що є одним із способів отримання персональних даних як своєрідної плати за цифровий контент[2], а клікання на посилання у різних sms-розсилках чи перехід на невідомі сайти через настирливі рекламні повідомлення або спам задля вдоволення своєї цікавості нерідко активує шахрайські програми-шпигуни. Враховуючи, що превалююча більшість personal data зберігається на комп'ютерних та хмарних носіях, а певна приватна інформація взагалі перетворюється у так званий «цифровий слід», порушення базових правил кібергігієни створює небезпеку доступу до них й до порушення недоторканності приватного життя в цілому. Отже, недостатня обізнаність суспільства у питаннях охорони і захисту всіх аспектів приватності нерідко призводить до її порушення, що має негативний вплив не лише на конкретну особу, а й на ціле суспільство та розвиток держави в цілому.

Висновки. Отже, елементи детермінаційного комплексу кримінальних правопорушень проти приватності являють собою складну сукупність криміногенних чинників, що мають тісний зв'язок між собою та виступають умовами формування криміногенних поглядів, традицій та звичаїв, установок у суспільній свідомості, пов'язаних зі зневажливим ставленням до права на недоторканність приватного життя. Нами перелічені хоча і не всі можливі чинники, але найбільш очевидні та пов'язані з учиненням кримінальних правопорушень проти приватності.

[1] Радейко Р Право на приватність у соціальних мережах, *Право на забуття: зб. ст.* / за ред. І. В. Спасибо-Фатєєвої (ЕКУС, 2021) 103–114

[2] Бернерс-Лі Т, Фічетті М *Заснування павутини: З чого починалася і до чого прийде Всесвітня мережа* / пер. з англ. А Іщенка (Київ: Вид. дім «Києво-Могилянська академія», 2007) 224

REFERENCES

List of legal documents

Legislation

1. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 05.10.2017 r. №2163 – VIII URL: https://zakon.rada.gov.ua/laws/show/2163–19#Text (in Ukrainian).
2. Proekt Zakonu pro zakhyst personalnykh danykh: vid 07.06.2021 r. №5628 URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72160 (in Ukrainian).
3. Proekt Zakonu pro zakhyst personalnykh danykh: vid 25.10.2022 r. №8153 URL: https://itd.rada.gov.ua/billInfo/Bills/Card/40707 (in Ukrainian).

Cases

1. Ukhvala Reniiskoho raionnoho sudu Odeskoi oblasti vid 25 zhovtnia 2022 r., sprava №510/1761/22 URL: https://reyestr.court.gov.ua/Review/106941346 (in Ukrainian).
2. Ukhvala Zhovtnevoho raionnoho sudu m. Dnipropetrovska vid 23 veresnia 2022 r., sprava №201/6714/22 URL: https://reyestr.court.gov.ua/Review/106593267 (in Ukrainian).
3. Ukhvala Horodenkivskoho raionnoho sudu Ivano-Frankivskoi oblasti vid 31 bereznia 2022 r., sprava №342/221/22 URL: https://reyestr.court.gov.ua/Review/103814009 (in Ukrainian).

4. Ukhvala Darnytskoho raionnoho sudu mista Kyieva vid 11 travnia 2022 r., sprava № 753/22/22 URL: https://reyestr.court.gov.ua/Review/104261528 (in Ukrainian).

Bibliography

Authored books

1. Berners-Li T and Fichetti M, *Zasnuvannia pavutyny: Z choho pochynalasia i do choho pryide Vsesvitnia merezha* [The foundation of the web: Where it began and where the World Wide Web will come] / per. z anhl. A Ishchenka (Vyd. dim «Kyievo-Mohylianska akademiia», 2007) 224 (in Ukrainian).
2. Hylynskyi Ya Y, *Devyantolohyia: sotsyolohyia prestupnosty, narkotyzma, prostytutsyy, samoubyistv y druhykh «otklonenyi»* [Deviantology: sociology of crime, drug addiction, promiscuity, suicide and other «deviant»] 2-e yzd., yspr. y dop. (Iurydycheskyi tsentr Press, 2007) 254 (in Russian).
3. Kohut Yu I, *Kiberbezpeka ta ryzyky tsyfrovoi transformatsii kompanii: praktychnyi posibnyk* [Cyber security and risks of digital transformation of the company: a practical guide] (Konsaltynhova kompaniia «SIDKON», 2022) 372 (in Ukrainian).
4. Kuznetsova N F, *Problemy krymynolohycheskoi determynatsyy* [Problems of criminological determination] (M.: MHU, 1984) 208 (in Russian).
5. Radeiko R, Pravo na pryvatnist u sotsialnykh merezhakh in I V Spasybo-Fatieieva, *Pravo na zabuttia: zb. st.* [The right to be forgotten: a collection of articles] (EKUS, 2021) 103–114 (in Ukrainian).
6. Zakaliuk A P, *Kurs suchasnoi ukrainskoi kryminolohii: teoriia i praktyka:* u 3 kn [Course of modern Ukrainian criminology: theory and practice] Kn. 1: *Teoretychni zasady ta istoriia ukrainskoi kryminolohichnoi nauky* [Theoretical foundations and history of Ukrainian criminological science] (Vydavnychyi Dim «In Yure», 2007) 424 (in Ukrainian).

Journal articles

1. AFP and Prigg M, 'Harward professors warn 'privacy is dead' (2015) Jan 25 The Sunday Times 2 (Sri Lanka) Page 5 <https://www.pressreader.com/sri-lanka/sunday-times-sri-lanka/20150125/282153584681118> (in English).
2. 'Causal Determinism' (2016) Jan 21 Stanford Encyclopedia of Philosophy Archive <https://plato.stanford.edu/archives/spr2016/entries/determinism-causal> (in English).
3. Determann L, 'No One Owns Data': articles (2018) Vol. 70:1 Hastings Law Journal Pages 1–44. <https://www.researchgate.net/publication/323617530_No_One_Owns_Data> (in English).
4. Trenti A, 'Victimological Aspects of Computer Crimes' (1997) Advances in Psychology and Law. International Contributions <https://www.degruyter.com/document/doi/10.1515/9783110801163.88/html> (in English).
5. Basai V D and Korol I B, 'Kryminolohichni faktory (zahrozy) porushennia prava na nedotorkannist pryvatnoho zhyttia' [Criminological factors (threats) of violation of the right to privacy] (2015) 3 Chastyna 2 Pravo i suspilstvo 174–180 (in Ukrainian).
6. Behma A P and Khovpun O S, 'Rozsliduvannia zlochyniv v IT-sferi' [Investigation of crimes in the IT sphere] (2021) 28 Naukovi pratsi Natsionalnoho universytetu «Odeska yurydychna akademiia» (Odesa: Vydavnychyi dim «Helvetyka») 12–19 (in Ukrainian).
7. Holovkin B M, 'Pro determinatsiiu zlochynnosti' [About the Determination of Crime] (2020) 1 Chasopys Kyivskoho universytetu prava 274–280 (in Ukrainian).
8. Holovkin B M, 'Prychynnist u systemi determinatsii zlochynnosti' [Causality in the crime determination system] (2014) 1 Teoriia i praktyka pravoznavstva: elektron. nauk. fakh. vyd. <https://dspace.nlu.edu.ua/bitstream/123456789/6358/1/Golovkin.pdf> (in Ukrainian).
9. Holovko A Ya, 'Postindustrialna transformatsiia svitovoho hospodarstva v konteksti formuvannia kontseptsii sotsialnoi vidpovidalnosti TNK' [Postindustrial transformation of world economy within the context of transnational corporations social responsibility formation] (2013) 9 Efektyvna ekonomika: elektron. zhurn. <http://www. economy. nayka. com. ua/?op=1&z=2330> (in Ukrainian).
10. Novikov O V, 'Nedoliky y prorakhunky polityky derzhavy v epokhu postindustrialnoi ekonomiky yak determinuiuchyi kompleks zlochynnosti u sferi intelektualnoi vlasnosti' [Shortcomings and miscalculations of state policy in the era of post-industrial economy as a determining complex of crime in the field of intellectual property] (2014) 4 Yurydychnyi visnyk 338–342 (in Ukrainian).
11. Polovenko L P and Merinova S V, 'Vyiavlennia oznak sotsialnoi inzhenerii ta tekhnolohiia protydii sotsialnym khakeram na pidpryiemstvi' [Identification of signs of social engineering and the technology of combating social hackers at the enterprise] (2019) 10 Pidpryiemnytstvo ta innovatsii 183–187 (in Ukrainian).
12. Ukhanova N S, 'Vyklyky i zahrozy pravam ta bezpetsi liudyny v informatsiinii sferi' [Challenges and threats to human rights and security in the information sphere] (2018) 4 (27) Informatsiia i pravo 33–45 (in Ukrainian).

13. Zhuravel A P, 'Sotsialno-psykholohichni osoblyvosti ta determinanty formuvannia osobystosti zi zlochynnoiu povedinkoiu' [Socio-psychological features and determinants of personality formation with criminal behavior] (2020) (31 (70)) 3 Vcheni zapysky TNU imeni V I Vernadskoho Seriia: Psykholohiia 76–80 <doi: https://doi.org/10.32838/2709–3093/2020.3/13> (in Ukrainian).<https://www.pravda.com.ua/news/2023/02/1/7387432/> (in Ukrainian).

Thesis abstracts

1. Korol I B 'Okhorona nedotorkannosti pryvatnoho zhyttia: kryminalno-pravovi ta kryminolohichni aspekty' [Protection of Privacy: Criminal Law and Criminological Aspects] (avtoref dys kand yuryd nauk Lviv, 2015) 22 (in Ukrainian).

Conference paper

1. Karchevskyi N V, '«Kyberprestuplenye» yly prestuplenye v sfere yspolzovanyia ynformatsyonnykh tekhnolohyi?' [«Cybercrime» or a crime in the field of information technology?] *Kiberbezpeka v Ukraini: pravovi ta orhanizatsiini pytannia:* materialy Vseukr. nauk.-prakt. konf. (m Odesa, 21 zhovt. 2016 r.) 10–14 (in Russian).

Websites

1. Keylogger <https://uk.wikipedia.org/wiki/Keylogger> (in Ukrainian).
2. Koshkina S, 'Obshuky v Chernivetsko-Bukovynskii yeparkhii UPTs MP: znaishly pasport RF u mytropolyta i 17-ho richnoho khloptsia v lizhku arkhimandryta' [Searches in the Chernivtsi-Bukovyna Diocese of the UOC MP: they found a Russian passport from the metropolitan and a 17-year-old boy in the archimandrite's bed] (LB.ua, 25 lystopada 2022) <https://lb.ua/society/2022/11/25/537108_obshuki_chernivetskobukovinskiy.html>(in Ukrainian).
3. Malai K, 'U Kyievi pohrabuvaly budynok vidomoi bloherky: vona bula vseredyni. Video z kamer sposterezhennia' [In Kyiv, the house of a famous blogger was robbed: she was inside. Video from surveillance cameras] (OBOZREVATEL, 4 lystopada 2021) <https://news.obozrevatel.com/ukr/show/people/dyakuyu-scho-zalishili-zhivoyu-u-kievi-pograbuvali-kolishnyu-divchinu-kyivstoner-zlodii-potrapili-na-kameri-video.htm> (in Ukrainian).
4. Mazurenko A and Tkach M, 'Sobolyna shuba, milion dolariv i Breguet: pid chas obshuku u posadovytsi podatkovoi znaishly spysok bazhan' [A sable fur coat, a million dollars and a Breguet: during the search of the tax office, you will find a wish list] (Ukrainska pravda, 1 liutoho 2023) <https://www.pravda.com.ua/news/2023/02/1/7387432/> (in Ukrainian).
5. Stezhar T and Zasadniuk A, 'Biznes-imperiia UPTs MP: zvidky u bozhykh liudei berutsia hroshi na rozkishni maietky ta avtivky' [The business empire of the UOC MP: where do people of God get money for luxurious estates and cars] (Informatsiine ahenstvo «UNIAN», 13 hrudyz 2018) <https://www.unian.ua/politics/10376331-biznes-imperiya-upc-mp-zvidki-u-bozhih-lyudey-berutsya-groshi-na-rozkishni-mayetki-ta-avtivki.html> (in Ukrainian).
6. 'U frankivskoi bloherky vkraly fary z novoho avtomobilia. FOTO/VIDEO' [Headlights from a new car were stolen from a Frankish blogger. PHOTO/VIDEO] (IAA «Ratusha», 9 lystopada 2020) <https://www. ratusha. if. ua/%d1%83-%d1%84%d1%80%d0%b0%d0%bd%d0%ba%d1%96%d0%b2%d1%81%d1%8c%d0%ba%d0%be%d1%97-%d0%b1%d0%bb%d0%be%d0%b3%d0%b5%d1%80%d0%ba%d0%b8-%d0%b2%d0%ba%d1%80%d0%b0%d0%bb%d0%b8-%d1%84%d0%b0%d1%80%d0%b8-%d0%b7/> (in Ukrainian).

Полях Є. В.
Кримінологічна детермінація порушення недоторканності приватного життя

У статті розглянуто низку кримінологічних чинників порушень недоторканності приватного життя. Вказане дослідження є актуальним через свою практичну значущість, оскільки осмислення останніх є методологічною основою наукового обґрунтування заходів запобігання кримінальним правопорушенням проти приватності.

Усі криміногенні чинники порушень privacy запропоновано поділяти на такі групи: чинники, що пов'язані з цифровізацією суспільних відносин; чинники, що пов'язані з недостатнім захистом інформації; чинники, що пов'язані з роботою правоохоронних органів, а також соціально-економічні, соціально-політичні (правові), соціально-культурні та віктимологічні чинники.

Визначальну роль у детермінаційному комплексі порушень приватності відіграють чинники, пов'язані з цифровізацією суспільних відносин. Зроблено висновок про те, що у сучасному світі персональні дані особи не належать їй. Потужні можливості цифровізації призвели до цілковитої комерціалізації персональних даних, тому ще однією групою чинників є соціально-економічні. Персональні дані, інші відомості про приватне життя стали джерелом формування капіталу, а політична еліта в багатьох країнах оцінила зазначені вище ризики доволі пізно, що спровокувало появу соціально-політичних (правових) чинників порушень privacy. Зазначено, що доцільно вести мову й про чинники, що пов'язані з недостатнім захистом інформації, оскільки будь-яка система не позбавлена слабких сторін захисту, крім того, існують й недоліки у роботі правоохоронної системи, що провокує появу чинників, пов'язаних із діяльністю останньої.

Значну увагу приділено віктимологічним чинникам, які пропонується поділяти на три групи: ті, що пов'язані з невіглаством потерпілого у зазначеній сфері; ті, що пов'язані з недбалим ставленням до свого приватного життя; ті, що пов'язані з кібергігієною користувачів інформаційних технологій. Також виділено соціально-культурні фактори порушень privacy.

Зроблено висновок про те, що елементи детермінаційного комплексу кримінальних правопорушень проти приватності являють собою складну сукупність криміногенних чинників, що мають тісний зв'язок між собою та виступають умовами формування криміногенних поглядів, традицій та звичаїв, установок у суспільній свідомості, пов'язаних зі зневажливим ставленням до права на недоторканність приватного життя.

Наголошено, що у дослідженні перелічені не всі можливі чинники, а найбільш очевидні та пов'язані з учиненням кримінальних правопорушень проти приватності.

Ключові слова: *порушення недоторканності приватного життя; приватне життя (privacy); детермінація злочинності, кримінальні правопорушення проти приватності.*

Poliakh Ye. V.

Criminological determination of violation of privacy

The article considers a number of criminological factors of violations of privacy. This study is relevant due to its practical significance, since the understanding of the latter is the methodological basis of the scientific justification of measures to prevent criminal offenses against privacy.

It is proposed to divide all criminogenic factors of privacy violations into the following groups: factors related to the digitalization of social relations; factors associated with insufficient protection of information; factors related to the work of law enforcement agencies, as well as socio-economic, socio-political (legal), socio-cultural and victimological factors.

Factors related to the digitalization of social relations play a decisive role in the deterministic complex of privacy violations. It was concluded that in today's world, a person's personal data do not belong to him. The powerful possibilities of digitalization have led to the complete commercialization of personal data, so another group of factors is socio-economic. Personal data and other information about private life became a source of capital formation, and the political elite in many countries assessed the above-mentioned risks quite late, which provoked the emergence of socio-political (legal) factors of privacy violations. It is noted that it is expedient to talk about factors related to insufficient protection of information, since any system is not without weak points of protection, in addition, there are also shortcomings in the work of the law enforcement system, which provokes the appearance of factors related to the activity the last one

Considerable attention is paid to victimological factors, which the author proposes to divide into three groups: those related to the victim's ignorance in the specified area; those related to a careless attitude to one's private life; those related to the cyber hygiene of information technology users. Social and cultural factors of privacy violations are also highlighted.

It was concluded that the elements of the determinative complex of criminal offenses against privacy represent a complex set of criminogenic factors that are closely related to each other and act as conditions for the formation of criminogenic views, traditions and customs, attitudes in the public mind, associated with a contemptuous attitude to the right to privacy.

The author emphasizes that the study does not list all possible factors, but the most obvious and related to the commission of criminal offenses against privacy.

Key words: *violation of privacy; private life (privacy); determination of crime; criminal offenses against privacy.*

Стаття надійшла до редакції:15.04.2023 р.
Прийнята до друку: 10.05.2023 р.