УДК 343.13
DOI https://doi.org/10.32782/2524-0374/2020-6/24

ДО ПРОБЛЕМИ ІМПЛЕМЕНТАЦІЇ КОНВЕНЦІЇ ПРО КІБЕРЗЛОЧИННІСТЬ У КРИМІНАЛЬНЕ ПРОЦЕСУАЛЬНЕ ЗАКОНОДАВСТВО УКРАЇНИ

SOME PROBLEMS OF THE CONVENTION ON CYBERCRIME IMPLEMENTATION INTO THE CRIMINAL PROCEDURE LAW OF UKRAINE

Скрипник А.В., аспірант кафедри кримінального процесу
Національний юридичний університет імені Ярослава Мудрого

У статті розглянуто проблеми імплементації Конвенції про кіберзлочинність у кримінальне процесуальне законодавство України. Досліджено основні положення проєкту Закону «Про внесення змін до Кримінального процесуального кодексу України та Кодексу України про адміністративні правопорушення щодо підвищення ефективності протидії кібератакам» № 4003 від 01.09.2020 р.

Висловлено зауваження і пропозиції, спрямовані на збільшення рівня відповідності національних процесуальних дій конвенційним, зниження ризику порушення прав і свобод людини і громадянина під час їх проведення, підвищення ефективності термінового збереження цифрових даних, часткового розкриття даних про рух інформації, а також розширення меж обшуку. Проаналізовано положення проєкту щодо термінового збереження інформації, який потребує не лише термінологічних правок, але й суттєвого узгодження з конвенційним аналогом (терміновим збереженням комп'ютерних даних, що зберігаються). Йдеться, зокрема, про уточнення характеру інформації, зняття обмеження у вигляді переліку кримінальних правопорушень, усунення дискреційного характеру підстав для застосування, уніфікацію термінів для позначення цифрових пристроїв, усунення недоліків часових меж застосування заходу забезпечення кримінального провадження, встановлення диспозитивного правила про зобов'язання не розголошувати відомості про застосування термінового збереження інформації, вдосконалення механізму звернення постанови про термінове збереження інформації до виконання, а її також оскарження.

Піддано критиці запровадження тимчасового доступу до терміново збереженої інформації через невідповідність як конвенційному заходу (частковому розкриттю даних про рух інформації), так і вітчизняним особливостям тимчасового доступу до речей і документів. Низку ризиків для суверенітету інших держав, а також прав і свобод людини і громадянина має і пропозиція розширити коло повноважень слідчого, прокурора під час обшуку в разі виявлення доступу до інформаційної системи, територіально розташованої за межами об'єкта обшуку.

Зроблено висновок про потребу запровадження описаних та інших конвенційних заходів протидії кіберзлочинності в кримінальне процесуальне законодавство України, а також про необхідність суттєвого доопрацювання положень, пропонованих у проєкті Закону «Про внесення змін до Кримінального процесуального кодексу України та Кодексу України про адміністративні правопорушення щодо підвищення ефективності протидії кібератакам» № 4003 від 01.09.2020 р.

Ключові слова: імплементація Конвенції про кіберзлочинність, термінове збереження інформації, часткове розкриття даних про рух інформації.

The article focuses on the problems of the Convention on Cybercrime implementation in the criminal procedure law of Ukraine. The main provisions of the draft Law "On Amendments to the Criminal Procedure Code of Ukraine and the Code of Administrative Offenses of Ukraine to improve the effectiveness of countering cyberattacks" № 4003 of 01.09.2020 are researched.

The aim of remarks and suggestions made due to the draft law is to increase the level of compliance between national and conventional procedural actions, to reduce the risk of violation of human rights and freedoms during their conducting, to increase the efficiency of expedited preservation of stored computer data, partial disclosure of traffic data and extension of the search. The provisions of the draft law on the expedited preservation of stored computer data are analyzed and it is concluded that they require terminological changes as well as significant harmonisation with the conventional provisions. These include clarifying the nature of information, removing restrictions in the list of criminal offenses, eliminating discretionary grounds, unifying terms used for digital devices, improvement of the time limits, establishing a dispositive rule connected with the disclosure of information about expedited preservation, improvement of the execution mechanism and the procedure of appeal.

The provisional access to expeditiously stored data is criticized because of non-compliance with both the conventional measure (partial disclosure of traffic data) and domestic features of provisional access to objects and documents. A proposal to expand the search by accessing to the information system located outside the object of search contains a number of risks to the sovereignty of other states, as well as human rights and freedoms.

It is concluded about the need to implement the described and other conventional measures against cybercrime in criminal procedure law of Ukraine, as well as the need of a significant revision of the draft Law "On Amendments to the Criminal Procedure Code of Ukraine and the Code of Administrative Offenses of Ukraine to improve the effectiveness of countering cyberattacks" № 4003 of 01.09.2020.

Key words: implementation of the Convention on Cybercrime, expedited preservation of stored computer data, partial disclosure of traffic data.

Цифрові технології стали невід'ємною складовою повсякденного життя. Вони, як жодне інше творіння рук людських, сприяють глобалізації. Водночас перевагами інформаційних технологій користуються також і у протиправній діяльності, кордонів для якої вже немає. Через це особливої актуальності набуває міжнародний рівень протидії кіберзлочинності, який передбачає запровадження в національні правові системи низки спільних правових заходів.

Ратифікувавши 07.09.2005 р. Конвенцію про кіберзлочинність (далі – Конвенція), Україна взяла на себе зобов'язання імплементувати низку матеріально-правових та процесуальних заходів протидії кіберзлочинності. Тривалий час значна кількість конвенційних механізмів не знаходила адекватної реалізації у вітчизняному процесуальному законодавстві, залишаючись предметом для наукового осмислення та компенсуючись у практичній діяльності з допомогою чинних процесуальних інститутів. Наприклад, запити про термінове збереження комп'ютерних даних виконуються посередництвом тимчасового доступу до них [1; 2]. Про можливість найближчим часом певною мірою виправити описану ситуацію свідчить інтерес до неї зі сторони законодавця, формалізований у проєкті Закону «Про внесення змін до Кримінального процесуального кодексу України та Кодексу України про адміністративні правопорушення щодо підвищення ефективності протидії кібератакам» № 4003 від 01.09.2020 р. (далі – проєкт № 4003). Положення останнього варті ґрунтовного наукового осмислення з метою висловити зауваження і пропозиції, спрямовані на вдосконалення процесуальних механізмів.

Метою проєкту Закону є імплементація «положень Конвенції про кіберзлочинність у кримінальне процесуальне законодавство України та підвищення ефективності протидії кібератакам» [3]. Йдеться про такі конвенційні механізми: а) термінове збереження комп'ютерних даних (ст. 16 Конвенції); б) часткове розкриття даних про рух інформації (ст. 17 Конвенції); в) розширення меж обшуку комп'ютерних даних (п.п. 2,4 ст. 19 Конвен-

ції). Втілити їх у кримінальному процесуальному законі пропонується через закріплення положень про: 1) новий захід забезпечення кримінального провадження – термінове збереження інформації (зміни до ст.ст. 131, 303, доповнення новою главою 15[1]), а також його процесуальні особливості: а) право доручити виконання (зміни до ст.ст. 36, 40, 41); б) можливу електронну форму рішення про його застосування (зміни до ст.110); в) право оскаржити рішення про його застосування (зміни до ст. 303); 2) модифікацію чинного заходу забезпечення – тимчасового доступу до речей і документів, для доступу до термінову збереженої інформації (зміни до ст.ст. 159, 162, 303, доповнення новими статтями 164[1], 165[1]); 3) право під час проведення обшуку: а) отримати віртуальний доступ до цифрового пристрою, фізичне розташування якого відмінне від об'єкта обшуку; б) подолати логічну систему захисту цифрового пристрою; в) отримувати інформацію про цифрові особливості пристроїв (зміни до ст. 236). Саме в такій послідовності і варто здійснювати осмислення викладених у проєкті № 4003 положень.

Термінове збереження інформації. Викладені у проєкті № 4003 положення про термінове збереження інформації викликають низку зауважень у контексті як конвенційних ідей, так і національного законодавства. Розуміння нового заходу забезпечення кримінального провадження як невідкладного фіксування та подальшого зберігання інформації в електронній (цифровій) формі, яка має значення для встановлення обставин у кримінальному провадженні (абз. 2 ч. 1 ст. 166[1] КПК у редакції проєкту № 4003): 1) не виключає можливості поширення його дії на інформацію, яку буде отримано у майбутньому (натомість конвенційний захід призначений виключно для інформації, яка на момент застосування процесуальної дії вже зберігається в особи, на чому неодноразово наголошували міжнародні експерти [4, с. 12; 5, с. 9; 6, § 149; 7, p. 6]); 2) викликає термінологічні зауваження: а) замість терміна «інформація» радше вживати згаданий у Конвенції «дані», більш коректний із технічної точки зору; б) поєднання прикметників «електронний» та «цифровий» для характеристики форми інформації недоцільне: перший характеризує носії даних, другий – власне дані або інформацію; в) невиправданим видається вжиття терміна «фіксування», який асоціюється з відповідним процесуальним інститутом (глава 5 розділу I Кримінального процесуального кодексу України (далі – КПК). Замість цього можна запропонувати таке формулювання: «Термінове збереження даних полягає у підтриманні їхньої цілісності, тобто недопущенні дій, що можуть привести до втрати або зміни цифрових даних».

Недоліків не позбавлений і перший абзац згаданої вище частини статті. *По-перше*, необґрунтовано звужено перелік кримінальних правопорушень, у кримінальних провадженнях щодо яких допускається застосування термінового збереження інформації (ст. 176, ч. 3 ст. 190, ст.ст. 200, 231, 300, 301, розділ XVI Особливої частини Кримінального кодексу України), натомість дію конвенційного заходу рекомендовано поширювати на будь-які кримінальні правопорушення незалежно від тяжкості або об'єкта посягання [7, p. 7; 5, с. 9]. Це є не тільки можливим (з огляду на мінімальний ступінь втручання у права і свободи людини під час його застосування), але й доцільним (з огляду на потребу використання таких цифрових даних не лише під час розслідування перелічених кримінальних правопорушень). *По-друге*, формулювання «обґрунтовані підстави вважати», будучи за своєю сутністю оцінним, для недопущення свавільного застосування заходу має корелюватися з відповідним пунктом мотивувальної частини постанови, який із невідомих причин відсутній у статті 166[2] (Вимоги до постанови прокурора, слідчого про термінове збереження інформації). *По-третє*, не можна оминути зауваженнями і термінологічну складову частину аналізованої норми. Так, словосполучення «власник, володілець або утримувач інформації» з точки зору цивільного права позбавлене смислу: право власності, правомочність володіння та тягар утримання є майновими (ч. 1 ст. 316, ч. 1 ст. 317, ч. 1 ст. 322 Цивільного кодексу України (далі – ЦК), водночас інформація є не майном (ч. 1 ст. 190 ЦК), а нематеріальним благом (ст. 200 ЦК). Окрім того, складно уявити, в який спосіб буде встановлюватися наявність такого правовідношення між особою й інформацією. Виправити таку ситуацію можна одним із двох способів: а) змінити «об'єкт» права і замість інформації визначити її матеріальний носій, вказавши на володільця або власника пристрою (як це має місце у п. 3 ч. 1 ст. 164[1], п. 4 ч. 1 ст. 166[2] КПК у редакції проєкту № 4003); б) використовувати інший термін для позначення особи на кшталт «особа, яка здійснює обробку цифрових даних», «особа, яка має доступ до цифрових даних», «особа, під контролем якої перебувають цифрові дані». Авторові ж імпонує перший спосіб, який, окрім того, варто застосувати також у ст. 165[1] та ч.ч. 2,3 ст. 166[1] КПК у редакції проєкту № 4003.

Ознаки термінологічної плутанини можна віднайти і в наведенні усього переліку згаданих у КПК цифрових категорій: 1) електронна інформаційна система або її частина; 2) мобільний термінал систем зв'язку; 3) інформаційна (автоматизована) система; 4) телекомунікаційна система; 5) інформаційно-телекомунікаційна система. Перші два терміни мають виключно процесуальне коріння, тому що в жодному іншому нормативному документі не вживаються, та, будучи не розкритими в законі, залишають можливість судово-практичної інтерпретації [8–10]. На відміну від цього, останні три терміни не лише вживаються в інших нормативно-правових актах[1], але і розкриваються в них (ст. 1 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах»). Якщо за чинної редакції процесуального закону термінологічну багатоманітність можна вважати наслідком неузгоджених змін[2], то розміщення усіх варіацій разом свідчить про наявність принципових відмінностей між першим (електронна інформаційна система або її частина, мобільний термінал систем зв'язку) та другим (інформаційна (автоматизована) система, телекомунікаційна система, інформаційно-телекомунікаційна система) «поколіннями» категорій. Видається, що треба остаточно визначитися з термінологією, яка використовується для позначення пристроїв для обробки цифрових даних, уніфікувавши її як на міжгалузевому, так і на галузевому рівні. Відсутність відмінностей у процедурі доступу до будь-якого з виокремлених пристроїв дає змогу позначати їх одним терміном, який відображатиме спільну для всіх пристроїв особливість – цифровий характер оброблюваних даних. Таким може стати один із таких: пристрій для обробки цифрових даних, накопичувач цифрових даних, носії для збереження цифрових даних, машинний носій. Пропозиція стосується усіх норм, в яких вживаються згадані на початку категорії (у проєкті № 4003 такими є п. 3 ч. 1 ст. 164[1], ст. 166[1]-166[4], абз. 2,3 ч. 6 ст. 236).

Викликають зауваження і норми щодо часових меж термінового збереження. Так, потребує уточнення останній абзац ч. 1 ст. 166[1] КПК у редакції проєкту № 4003:

[1] Наприклад, п. 2 Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах, затвердженого Постановою Кабінету Міністрів України від 16 листопада 2002 р. № 1772, п. 2 Порядку роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання, затвердженого Наказом Міністерства юстиції України 11.11.2014 р. № 1886/5, пп. 2 п. 3 Порядку проведення процедури оцінки відповідності у сфері електронних довірчих послуг, затвердженого Постановою Кабінету Міністрів України від 18 грудня 2018 р. № 1215.

[2] Йдеться про Закон України «Про внесення змін до деяких законодавчих актів щодо забезпечення дотримання прав учасників кримінального провадження та інших осіб правоохоронними органами під час здійснення досудового розслідування» № 2213-VIII від 16.11.2017 р. (більш відомий як «Маски-шоу стоп-2»).

а) словосполучення «*невідкладне* збереження інформації» (курсив – *А.С.*) не узгоджується з назвою заходу забезпечення – *термінове* збереження інформації; б) за будь-яких умов строк термінового збереження не має перевищувати строку досудового розслідування; в) верхня темпоральна межа термінового збереження (дев'яносто днів) видається занадто великою для позначення «часу, який необхідний для того, щоб здійснити тимчасовий доступ до терміново збереженої інформації» (абз. 1 ч. 1 ст. 166[1]), що є досить оперативним заходом, адже, окрім певних виключень, може здійснюватися за постановою слідчого, прокурора (ч. 3 ст. 159 КПК у редакції проєкту № 4003); г) тривалість визначеного слідчим, прокурором строку має вмотивовуватись у постанові, як і сама потреба в застосуванні термінового збереження інформації, про що вже йшлося вище. Через це абз. 3 ч. 1 ст. 166[1] КПК у редакції проєкту № 4003 можна викласти в такій редакції: «Строк дії постанови про термінове збереження даних визначається в межах строку досудового розслідування та не може перевищувати 60 днів», а ч. 1 ст. 166[2] потребує доповнення пунктом сьомим такого змісту: «7) строк дії постанови із обґрунтуванням його тривалості».

Це ж стосується і норми про продовження строку термінового збереження інформації (ст. 166[3] КПК у редакції проєкту № 4003). Окрім визначення максимального строку, положення про продовження потребує вдосконалення в такому: 1) абзац другий частини першої цієї статті, який обмежує сукупний строк термінового збереження даних максимальними строками досудового розслідування, позбавлений смислу, тому що застосувати такий захід забезпечення як до початку, так і після закінчення кримінального провадження незаконно (як і будь-який інший, окрім затримання особи без ухвали слідчого судді, суду); 2) частину другу цієї статті, яка встановлює обов'язок зазначити в постанові обґрунтування необхідності продовження строку термінового збереження, краще доповнити обов'язком пояснити причину неможливості отримати доступ до терміново збережених даних протягом строку дії попередньої постанови.

Закріплене у ч. 2 ст. 166[1] КПК у редакції проєкту № 4003 положення про «автоматичне» *зобов'язання* (курсив – *А.С.*) особи, яка здійснює обробку даних, «не допускати розголошення в будь-який спосіб факту отримання та виконання … постанови протягом часу її виконання» для забезпечення «гнучкості» норми варто замінити дискреційним правилом про *можливість зобов'язання* (право зобов'язати) [4, с. 12; 5, с. 9] зберігати конфіденційність факту застосування термінового збереження. Відповідно, доповнення потребує перелік вимог до постанови (ч. 1 ст. 166[2] КПК у редакції проєкту № 4003), серед яких краще вказати такий: «розпорядження не розголошувати інформацію про тимчасове збереження даних». Якщо «автоматичне» зобов'язання видаватиметься більш привабливим [6, § 163], то перелік вимог до постанови все одно потребуватиме доповнення, проте вже пунктом про повідомлення особи про обов'язок не розголошувати. Це матиме важливе значення як для ефективності заходу, так і для притягнення до відповідальності за розголошення інформації.

Пропонована можливість використання електронної форми постанови про термінове збереження інформації (абз. 2 ч. 6 ст. 110, ч. 3 ст. 166[1] КПК у редакції проєкту № 4003) видається прогресивною. Утім доцільність вказівки назви основного закону у сфері «електронного документообігу та використання електронних документів» (преамбула Закону України «Про електронні документи та електронний документообіг») є сумнівною з точки зору нормативної економії: будь-яка зміна в назві або скасування згаданого акта вимагатиме внесення до КПК змін, яких можна було б уникнути через зазначення словосполучення «законодавство про електронні документи та електронний документообіг» (окрім того, останнє не вичерпується названим законом). Невизначеним залишається питання механізму електронного надсилання постанови: на яку електронну адресу або з допомогою яких програмних додатків надсилати, як можна підтвердити факт отримання особою постанови та ознайомлення з її змістом тощо? Особливої актуальності ці питання набувають у контексті виконання постанови (ч. 1 ст. 166[1] КПК у редакції проєкту № 4003) та притягнення до відповідальності за її невиконання (ст. 185[14], якою в проєкті № 4003 пропонується доповнити Кодекс України про адміністративні правопорушення). Разом із тим оперативності застосування термінового збереження даних заважатиме традиційна (письмова) форма видання доручення про його проведення (п. 5 ч. 2 ст. 36, п. 3 ч. 2 ст. 40, ч. 1 ст. 41 КПК, ч. 4 ст. 7 Закону України «Про оперативно-розшукову діяльність» у редакції проєкту № 4003). Водночас якісно вирішити описані проблеми без комплексного врегулювання електронного кримінального судочинства не можна. Окрім того, з точки зору нормативної техніки ч. 3 ст. 166[1] КПК у редакції проєкту № 4003, якою визначається можлива форма постанови, більш логічно розмістити в статті, що закріплює вимоги до постанови, – ст. 166[2] КПК у редакції проєкту № 4003.

Не можна оминути увагою і положення щодо виконання постанови про термінове збереження даних (ст. 166[4] КПК у редакції проєкту № 4003). Так, невизначеним є строк прийняття слідчим, прокурором рішення про скасування постанови про застосування заходу, яке постановляється після здійснення тимчасового доступу до терміново збереженої інформації (ч. 2 ст. 166[4]). Така прогалина може призвести до проблеми, аналогічної тій, що супроводжує інший захід забезпечення – арешт майна. Невиконання закріпленого у ч. 3 ст. 174 КПК обов'язку прокурора скасувати арешт майна одночасно з винесенням постанови про закриття кримінального провадження призводить до продовження обмеження права власності вже після закінчення досудового розслідування. Для того, щоб в описаної проблеми не з'явився цифровий аналог, потрібно: а) визнавати здійснення тимчасового доступу до терміново збереженої інформації підставою для припинення застосування цього заходу забезпечення як такого, що виконав свою функцію; б) визначити підставою для його припинення винесення постанови про закриття кримінального провадження, про що слідчий, прокурор зобов'язані повідомити особу невідкладно, але не пізніше наступного робочого дня з після її постановлення, в письмовій або електронній формі. У такому разі активні дії (повідомити про рішення), щодо яких наявний ризик невиконання, вимагатимуться лише в одному з двох випадків – закриття кримінального провадження. Визначеності потребує і строк виконання слідчим, прокурором іншого обов'язку – надіслати копію постанови про термінове збереження інформації, постанови про продовження строку або скасування термінового збереження (ч. 3 ст. 166[4] КПК у редакції проєкту № 4003). Оптимальною тривалістю строку можна вважати не більшу за один робочий день.

Запровадження можливості оскарження рішень про термінове збереження інформації, про продовження його строку та тимчасовий доступ до терміново збереженої інформації заслуговує на схвалення та підтримку. Водночас зауваження викликає коло осіб, наділених правом на оскарження, – лише особи, визначені у відповідних постановах. Так, не виключається ситуація, коли в рішенні слідчого, прокурора будуть визначені не усі власники або володільці цифрових пристроїв особа, через що заходом забезпечення будуть обмежені права і свободи осіб, не вказаних у постанові. Проте оскаржити таке обмеження вони не зможуть. Через це правом оскаржити вжиття відповідних заходів мають бути наділені не лише визначені в рішенні слідчого, прокурора особи, але і власники та володільці накопичувачів цифрових даних, а також

особи, які здійснюють обробку цифрових даних, тобто усі ті, чиї права і свободи обмежуються застосуванням перелічених заходів забезпечення кримінального провадження.

Тимчасовий доступ до терміново збереженої інформації. Метою модифікації чинного інституту тимчасового доступу до речей і документів розробниками задекларовано імплементацію ст. 17 Конвенції про кіберзлочинність, яка передбачає запровадження термінового збереження і часткового розкриття даних про рух інформації [3]. Сутність конвенційного заходу полягає в такому: провайдер телекомунікаційних послуг, який отримав ордер про термінове збереження, оперативно розкриває такий обсяг даних про рух інформації (*traffic data*), який буде достатнім для надання змоги ідентифікувати інших провайдерів та встановити «маршрут» комунікації [6, § 169]. Водночас моделей втілення цього положення є кілька: а) 1 ордер – 1 провайдер; б) 1 ордер – *N* провайдерів (допомогу в збереженні даних в усьому «ланцюзі» надають самі провайдери) [6, § 168]. Окрім того, Конвенція визначає дані про рух інформації як будь-які комп'ютерні дані, пов'язані з комунікацією за допомогою комп'ютерної системи, які були створені комп'ютерною системою, що становила частину ланцюга комунікації, і які зазначають походження, кінцевий пункт, маршрут, час, дату, розмір і тривалість комунікації або тип основної послуги (ст. 1). Пропонований же проєктом № 4003 механізм лише віддалено нагадує конвенційний.

У національній інтерпретації часткове розкриття видозмінилося і полягає в тимчасовому доступі до інформації, яка: а) була терміново збережена; б) не є персональними даними або передання якої не є приватним спілкуванням (ч. 3 ст. 159 КПК у редакції проєкту № 4003). Якщо конвенційний механізм визначає, які дані можуть бути терміново розкриті, то його вітчизняний аналог закріплює лише ті дані, що оперативно за постановою слідчого, прокурора отримати не можна, причому в доволі розпливчастих формулюваннях [11]. Окрім того, термінове збереження могло стосуватися інформації, відмінної від даних про рух інформації, через що досягти основної мети – оперативно визначити наступного належного адресата постанови про термінове збереження під час тимчасового доступу буде неможливо. Оперативності зашкодить і письмова форма постанови, виключень з якої, на відміну від рішення про термінове збереження, закріпити не пропонується (ч. 6 ст. 110 КПК у редакції проєкту № 4003). Натомість окремі приклади імплементації ст. 17 Конвенції свідчать не лише про потребу закріплення уніфікованих із терміновим збереженням правил, але і навіть про можливість спільного й автоматичного їх застосування (Румунія, Португалія) [7, p. 51].

Неузгодженості можна віднайти і на національному рівні. *По-перше*, тимчасовий доступ до інформації не узгоджується із сутністю інституту тимчасового доступу до речей і документів – її носіїв. Зміни, які суперечать головній ознаці заходу, що має забезпечувальний характер [12, с. 72], тобто передбачає доступ не до доказів, а до їхніх процесуальних джерел, не мають бути точковими. У разі визнання потреби в запровадженні згаданих положень (у чому автор глибоко сумнівається) змін має зазнати або увесь інститут тимчасового доступу, або нормативне «місце» їх імплементації за межами останнього.

По-друге, нова редакція п. 7 ч. 1 ст. 162 КПК, яка передбачає зміну ознак інформації, що знаходиться в операторів і провайдерів телекомунікацій, для зарахування до охоронюваної законом таємниці, дублює низку положень КПК. Йдеться про п. 7 цієї ж частини статті, яким до охоронюваної законом таємниці зараховано персональні дані особи, а також ч.ч. 1, 3 ст. 258 КПК, що забороняє доступ до приватного спілкування без ухвали слідчого судді. Хоча мета змін до п. 7 ч. 1 ст. 162 КПК є раціональною з точки зору оперативності – дозволити доступ до інформації, що не належить до персональних даних або приватного спілкування, без ухвали слідчого судді, визнати її такою з точки зору прав людини складно. Все через те, що нова редакція п. 7 ч. 1 ст. 162 КПК уможливлює доступ до приватного спілкування (як до охоронюваної законом таємниці) в режимі тимчасового доступу до речей і документів без урахування тяжкості вчиненого правопорушення – такої важливої для дотримання закріпленої в засаді таємниці спілкування гарантії (ч. 2 ст. 14 КПК). Тому підтримати таке формулювання п. 7 ч. 1 ст. 162 КПК не можна. Натомість у ньому найбільш доцільно навести виключення щодо даних про рух інформації у розумінні, закладеному у ст. 1 Конвенції.

По-третє, недоліків не позбавлена і норма щодо виконання постанови про тимчасовий доступ до терміново збереженої інформації (ст. 165^1 КПК у редакції проєкту № 4003). Єдиним способом здійснення такого доступу визначено зняття копії інформації (ч. 1). Водночас ч. 3 цієї ж статті покладає на слідчого, прокурора обов'язок залишити «опис інформації, яка була вилучена шляхом копіювання». І навіть, попри популярність словосполучення «вилучити шляхом копіювання» у судовій практиці [13–16], таке формулювання складно визнати вдалим через те, що копіювання і вилучення – це різні способи здійснення тимчасового доступу до речей і документів [17, с. 34; 18, с. 240]. Вилучення інформації позбавляє особу змоги мати доступ до неї, потребу в чому з огляду на тиражованість даних у цифровому середовищі пояснити важко. Тому більш прийнятним видається таке формулювання: «…опис інформації, яка була скопійована на виконання постанови».

Обшук. Причина пропозиції надати змогу розширити цифрові «межі» обшуку – імплементація п.п. 2, 4 ст. 19 Конвенції [3]. Водночас національна інтерпретація конвенційного заходу викликає низку зауважень як у міжнародному, так і національному контекстах. *По-перше*, не вказано територіальні межі доступу до іншої інформаційної системи, у той час як принципово важливим є перебування останньої на території нашої держави [6, § 192, 193, 195]. У разі транскордонного характеру цифрового доступу Конвенція для дотримання суверенітету інших держав та прав і свобод людей, які перебувають на їхній території, пропонує звертатися до механізмів міжнародного співробітництва (ст.ст. 31, 32 Конвенції). *По-друге*, абз. 2 ч. 6 ст. 236 КПК у редакції проєкту № 4003 передає ідею розширення меж обшуку доволі складно та навіть суперечливо. Наприклад, йдеться про ситуацію, коли «слідчий, прокурор виявив або законним чином отримує доступ до … систем, на які не поширюється дозвіл на проведення обшуку». Постає логічне запитання: як встановити законність доступу до віддаленого цифрового пристрою? *По-третє*, у положенні міститься низка ризиків для прав і свобод людини. Наприклад, дозволяється долати/знімати системи логічного захисту незалежно від мети обшуку та об'єкта пошуку (абз. 1); підставою для доступу до віддаленої інформаційної системи є формулювання, що надає занадто широкі дискреційні повноваження виконавцям обшуку – достатність підстав вважати, «що інформація <…> має значення для встановлення обставин кримінального провадження» (абз. 2). За такого положення слідчий, прокурор, отримавши дозвіл на проведення обшуку житла чи іншого володіння особи, матиме змогу дослідити зміст усіх цифрових пристроїв, зокрема із логічними системами захисту, акаунтів соціальних мереж тощо просто через те, що доступ до них фізично перебуває на місці проведення обшуку, хоча судовий контроль за правомірністю втручання в інші, окрім права на недоторканість житла, права (наприклад, права на таємницю спілкування) міг не здійснюватись. Компенсаторного ж механізму оскаржити такі дії особою, права і свободи якої було обмежено, не пропонується. Такого ступеня втручання у права і свободи людини не можна здійснювати без судового контролю:

попереднього (надання прямого дозволу на відшукання відповідної інформації чи пристрою) або наступного (для оцінки правомірності доступу до інформації чи пристрою, не згаданих у судовому дозволі, *post factum*). Окрім того, невизначеними залишаються межі цифрового втручання: які файли можна досліджувати, що знову ж таки містить ризик неконтрольованого втручання у права і свободи людини і громадянина. Натомість ефективні механізми контролю цифрового втручання можна віднайти у прецедентній системі Сполучених Штатів Америки, (концепція розумного очікування на приватність та правило «закритого контейнера») [19]. Без детального врегулювання цифрових дій сторони обвинувачення шляхом запровадження нової слідчої дії – цифрового обшуку – якісно вирішити порушені проблеми не можна. *По-четверте*, в запропонованому формулюванні абз. 3 ч. 6 ст. 236 КПК у редакції проєкту № 4003 немає смислу: він передбачає право, а не обов'язок осіб повідомити інформацію про особливості роботи і захисту цифрових пристроїв, на відміну від конвенційного правила вимагати надання такої інформації (п. 4 ст. 19 Конвенції).

Із наведеного можна дійти висновку, що потреба імплементувати положення Конвенції є очевидною та не піддається сумніву. Водночас пропоновані проєктом № 4003 механізми потребують суттєвого доопрацювання. Окрім наведених вище зауважень і пропозицій, варто вказати на додаткові способи вдосконалення процесуальних механізмів, як-от: 1) запровадження часткового розкриття даних про рух інформації як складової частини термінового збереження даних; 2) об'єднання в одному заході забезпечення – збереженні цифрових даних, як термінового збереження та часткового розкриття даних (ст.ст. 16, 17 Конвенції), так і арешту цифрових даних після здійснення доступу до них (п. 3 ст. 19 Конвенції) – для збереження цифрового оригіналу; 3) надання права застосовувати захід забезпечення не лише слідчому, прокурору під час досудового розслідування, але й суду під час судового провадження (за прикладом Угорщини, Португалії, Румунії, Словаччини та інших держав [7, p. 93, 94, 107, 109, 111]); 4) встановлення відповідальності за незбереження чи нерозкриття даних: а) не адміністративної, а кримінальної; б) не лише для фізичних осіб, але й для юридичних; 5) для досягнення мети термінового збереження в разі загрози активної протидії володільця цифрового пристрою запровадження можливості невідкладного проведення цифрового обшуку [6, § 161] із наступним судовим контролем за його правомірністю. Разом із тим викладені вище зауваження і пропозиції можна вважати запрошенням до наукової дискусії та розробки способів імплементації інших положень Конвенції, що має стати результатом плідної синергії науковців, практичних працівників та нормотворців.

ЛІТЕРАТУРА

1. Ухвала Святошинського районного суду м. Києва від 4 серпня 2020 року (справа № 759/12632/20-к). URL: http://www.reyestr.court.gov.ua/Review/90931393 (дата звернення: 30.09.2020).
2. Ухвала Святошинського районного суду м. Києва від 23 червня 2020 року (справа № 759/7376/20). URL: http://www.reyestr.court.gov.ua/Review/90128550 (дата звернення: 30.09.2020).
3. Пояснювальна записка до проєкту Закону України «Про внесення змін до Кримінального процесуального кодексу України та Кодексу України про адміністративні правопорушення щодо підвищення ефективності протидії кібератакам» від 31.08.2020 р. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=69770&pf35401=534066 (дата звернення: 30.09.2020).
4. Звіт щодо України про чинне законодавство і проекти законів, що доповнюють різні питання, пов'язані з кіберзлочинністю та електронними доказами, та вносять зміни до них 2016/DGI/JP/3608 від 3 листопада 2016 року. 169 с. URL: https://rm.coe.int/16806f3743 (дата звернення: 30.09.2020).
5. Пропозиції щодо проекту правок до процесуального законодавства України, що стосується кіберзлочинності та електронних доказів (2016/DGI/JP/3608) від 28 травня 2017 року. 30 с. URL: https://drive.google.com/drive/folders/1pIM2wTFZjAN1CbwqXh9qN0cWSKzAULtX (дата звернення: 30.09.2020).
6. Explanatory Report to the Convention on Cybercrime (Budapest, 23.XI.2001). 60 p. URL: https://rm.coe.int/16800cce5b (last assessed: 30.09.2020).
7. Assessment report Implementation of the preservation provisions of the Budapest Convention on Cybercrime, adopted by the T-CY at its 8 th Plenary (5–6 December 2012). 132 p. URL: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e722e (last assessed: 30.09.2020).
8. Ухвала Печерського районного суду м. Києва від 10 лютого 2020 року (справа № 757/5768/20). URL: http://www.reyestr.court.gov.ua/Review/87631331 (дата звернення: 30.09.2020).
9. Ухвала Вищого антикорупційного суду від 2 березня 2020 року (справа № 991/1819/20). URL: http://www.reyestr.court.gov.ua/Review/88013481 (дата звернення: 30.09.2020).
10. Ухвала Вищого антикорупційного суду від 18 лютого 2020 року (справа № 991/1414/20). URL: http://www.reyestr.court.gov.ua/Review/87793041 (дата звернення: 30.09.2020).
11. Заява коаліції «За вільний Інтернет» «Пакет законопроектів щодо протидії кіберзлочинності та посилення санкційного механізму від 1 вересня 2020 року містить загрози для цифрових прав». URL: https://dslua.org/publications/paket-zakonoproektiv-shchodo-protydii-kiberzlochynnosti-ta-posylennia-sanktsiynoho-mekhanizmu-vid-1-veresnia-2020-roku-mistyt-zahrozy-dlia-tsyfrovykh-prav-zaiava-koalitsii-za-vilnyy-internet/ (дата звернення: 30.09.2020).
12. Сергєєва Д.Б., Старенький О.С. Використання результатів негласних слідчих (розшукових) дій для проведення тимчасового доступу до речей і документів. *Вісник кримінального судочинства*. 2015. № 4. С. 70–80. URL: http://nbuv.gov.ua/UJRN/vkc_2015_4_11 (дата звернення: 30.09.2020).
13. Вирок Красноармійського міськрайонного суду Донецької області від 16 листопада 2015 року (справа № 35/3606/15-к). URL: http://www.reyestr.court.gov.ua/Review/53461747 (дата звернення: 30.09.2020).
14. Ухвала Новокаховського міського суду Херсонської області від 12 лютого 2020 року (справа № 661/685/20). URL: http://www.reyestr.court.gov.ua/Review/87542742 (дата звернення: 30.09.2020).
15. Ухвала Гайсинського районного суду Вінницької області від 21 листопада 2018 року (справа № 129/3194/16-к). URL: http://www.reyestr.court.gov.ua/Review/77991352 (дата звернення: 30.09.2020).
16. Ухвала Херсонського міського суду Херсонської області від 29 січня 2020 року (справа № 766/1427/20). URL: http://www.reyestr.court.gov.ua/Review/87220375 (дата звернення: 30.09.2020).
17. Кузубова Т.О. Правові засади інституту тимчасового доступу до речей і документів у кримінальному провадженні : дис. … канд. юрид. наук. Харків, 2019. 250 с.
18. Абламський С.Є. Особливості здійснення тимчасового доступу до електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка*. 2017. № 2(78). С. 239–245. URL: https://journal.lduvs.lg.ua/index.php/journal/article/view/305 (дата звернення: 30.09.2020).
19. Marshall H.J. et al. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Washington, DC: U.S. Department of Justice. 2009. 299 p. URL: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf (last assessed: 30.09.2020).