М.І. ДЕДУРА, Д.І. КЛЕПКА, І.О. КРИЦЬКА

Марина Ігорівна Демура, кандидат юридичних наук, асистент кафедри Національного юридичного університету імені Ярослава Мудрого*

ORCID: 0000-0002-5637-3290

Дар'я Ігорівна Клепка, кандидат юридичних наук, науковий співробітник Науково-дослідного інституту вивчення проблем злочинності імені академіка В.В. Сташиса НАПрН України**

ORCID: 0000-0001-8423-4581

Ірина Олександрівна Крицька, кандидат юридичних наук, асистент кафедри Національного юридичного університету імені Ярослава Мудрого***

ORCID: 0000-0003-3676-4582

ЗАБЕЗПЕЧЕННЯ ПРАВ ТА ЗАКОННИХ ІНТЕРЕСІВ ОСОБИ В УМОВАХ «ДІДЖИТАЛІЗАЦІЇ» КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ

Постановка проблеми. Глобальна цифрова революція, що відбувається у світі, не залишила осторонь і нашу країну. Як наслідок, в обігу з'являються нові терміни на кшталт «автоматизація», «оцифровка даних», «діджиталізація» (цифрова трансформація). У світлі цього зазначимо, що слово «діджиталізація» названо словом 2019 р. словником сучасної української мови та сленгу. Цей неологізм, що увійшов в українську мову лише кілька років тому, є транслітерацією англійського «digitalization» та, згідно з визначенням словника, означає зміни в усіх сферах суспільного життя, зв'язаних з використанням цифрових технологій¹.

Говорячи про глобальні процеси цифрової трансформації, не можна оминати увагою й таку сферу суспільних відносин, як кримінальні процесуальні. Аналіз правозастосовної практики та великої кількості проєктів законів, спрямованих на регламентацію певних питань, зв'язаних із цифровою трансформацією, свідчить про актуальність зазначеної проблематики. У науковій спільноті вже тривалий час аргументовано наголошується на необхідності запровадження електронних доказів у кримінальному процесі; пропонується регламентувати нові підходи до проведення обшуку, зв'язаного із втручанням до електронних інформаційних систем; обґрунтовується необхідність вдосконалення нормативної моделі заходів забезпечення кримінального провадження (особливо зв'язаних із доступом до інформації, яка міститься на електронних носіях) тощо.

Водночас варто наголосити, що відповідно до ст. 2 Кримінального процесуального кодексу України (далі – КПК) завданнями кримінального провадження є, зокрема, «захист особи, суспільства та держави від кримінальних правопорушень, охорона прав, свобод та законних інтересів учасників кримінального провадження...». З огляду на зазначене вважаємо доцільним розглянути можливі шляхи діджиталізації кримінального провадження саме крізь призму забезпечення прав та законних інтересів особи.

На підставі викладеного **вважаємо за можливе сформулювати мету статті наступним чином:** визначення та загальна характеристика перспективних векторів цифрової трансформації досудового розслідування крізь призму забезпечення прав та законних інтересів особи.

Аналіз останніх досліджень. Окремі аспекти заявленої проблематики були предметом аналізу у працях таких вчених, як О.Ф. Абдулвалієва, а також О.В. Качалової, П.С. Пастухова, Ю.О. Цветкова та інших. Деякі питання, зв'язані з використанням цифрових носіїв інформації у кримінальному процесі, висвітлені у працях А.С. Білоусова, С.В. Васильєва, О.Г. Григор'єва, М.М. Єгорова, Н.А. Зігури, М.А. Іванова, В.А. Капліної, І.О. Крицької, С.І. Кувичкова, Г.В. Кудрявцевої, Р.І. Оконенка, П.С. Пастухова, Д.М. Цехана, М.Є. Шуміло тощо. Водночас підкреслимо, що саме діджиталізація досудового розслідування, особливо в аспекті прав та законних інтересів особи, не була предметом наукових розвідок учених.

Виклад основного матеріалу. Постійний доступ до мережі Інтернет спричинив трансформацію таких явищ, як булінг, stalking і порнопомста. Анонімність, миттєва поширюваність та необмеженість доступу до цифрової інформації надають цим явища кардинально нових ознак. Водночас спроби запровадження відповідальності за ці правопорушення мають доволі початковий та фрагментарний характер². Так, у науковій спільноті кримінального права точиться дискусія щодо криміналізації зазначених явищ. Крім того, з'явля-

© М.І. Демура, Д.І. Клепка, І.О. Крицька, 2020

* *Maryna Demura, Ph.D. in Law, Assistant of the Chair of Yaroslav Mudryi National Law University*

** *Daria Klepka, Ph.D. in Law, Research of Academician Stachis Scientific Research Institute for the Study of Crime Problems of the National Academy of Legal Sciences of Ukraine*

*** *Iryna Krytska, Ph.D. in Law, Assistant of the Chair of Yaroslav Mudryi National Law University*

ються нові способи вчинення злочинів, зокрема, наприклад, шахрайства (прикладом може слугувати «шахрайство, зв'язане з комп'ютерами». Такий вид злочину передбачений ст. 8 Конвенції про кіберзлочинність, ратифікованою Верховною Радою України ще у 2005 р.).

Вочевидь подібна тенденція зумовлює так само виникнення нових перепон і під час здійснення досудового розслідування, оскільки суттєво ускладнюються процедура та можливості встановлення й доказування ознак таких кримінальних правопорушень (загадаймо можливість видалення повідомлень у Telegram, Viber).

У зв'язку з цим доводиться констатувати, що норми чинного кримінального процесуального законодавства відрізняються певною архаїчністю щодо новітніх проявів протиправних дій у мережі, оскільки містять загальні правила захисту прав та законних інтересів особи від загроз у реальній дійсності, при цьому не враховуючи можливість вчинення кримінальних правопорушень в Інтернет-просторі. А тому традиційні методи запобігання і боротьби з кримінальними правопорушеннями не завжди є дієвими; до того ж труднощі можуть виникати і на етапі встановлення факту вчинення правопорушення.

У контексті зазначеного варто звернути увагу на Резолюцію Ради ООН з прав людини, в якій зазначено, що в Інтернеті мають захищатися ті ж права, якими люди користуються за його межами³. Резолюція прямо поширює права, передбачені Декларацією прав людини, Міжнародним пактом про громадянські та політичні права та Міжнародним пактом про економічні, соціальні та культурні права на Інтернет-простір, підкреслюючи принцип – «права, які належать людям офлайн, мають захищатися і у мережі Інтернет». Це положення декларативно визначає обсяг прав людини в Інтернеті, однак de-facto не вирішує проблеми створення механізму захисту цих прав.

Окрему увагу варто звернути на захист права власності особи та права на *privacy*⁴ під час здійснення слідчих розшукових дій, інших процесуальних дій, спрямованих на доступ до інформації, що зберігається на електронних носіях або вилучення таких систем. Так, наприклад, авторами одного з проєктів Закону пропонується заборонити вилучати пристрої для обробки, передавання та зберігання електронної інформації або їх складових, а також порушувати роботу комп'ютерних та інших мереж, якщо знаряддям, засобом або предметом кримінального правопорушення виступає інформація, що в них міститься⁵. Аналогічні положення містяться в низці інших проєктів законів. Не вдаючись до правової оцінки зазначеного положення, зауважимо, що така законодавча ініціатива свідчить про нагальність внесення змін до окремих норм кримінального процесуального законодавства України, щодо вдосконалення механізму захисту права власності особи, особливо у сфері застосування, зберігання та обігу електронної інформації.

Науковий інтерес також становить положення проєкту Закону «Про внесення змін до деяких законодавчих актів щодо імплементації положень Конвенції про кіберзлочинність та підвищення ефективності боротьби з кіберзлочинністю», яким запропоновано, зокрема, змінити нормативну регламентацію ч. 6 ст. 236 КПК. Так, зазначений проєкт Закону містить положення, відповідно до якого, якщо під час обшуку слідчий, прокурор виявив або законним чином отримує доступ до електронних інформаційних систем або їх частин, мобільних терміналів, систем зв'язку, інформаційних (автоматизованих), телекомунікаційних, інформаційно-телекомунікаційних систем або невід'ємних частин цих систем, на які не поширюється дозвіл на проведення обшуку, але щодо яких є достатні підстави вважати, що інформація, яка на них міститься, має значення для встановлення обставин у кримінальному провадженні, прокурор, слідчий мають право здійснити пошук, виявлення та фіксацію інформації, що на них міститься, на місці проведення обшуку. З цього приводу зазначимо, що така пропозиція є потенційно шкідливою для прав та законних інтересів особи. Авторами проєкту Закону не враховано, що такий доступ пов'язаний із втручанням у право особи на *privacy*, яке за таких обставин знаходиться поза межами судового контролю.

Таким чином, на підставі зазначеного вважаємо можливим сформулювати перший вектор цифрової трансформації досудового розслідування, а саме: **вдосконалення національної моделі виявлення кримінальних правопорушень та їх розкриття**.

Крім того, у контексті досліджуваної проблематики зазначимо, що однією з головних державних ініціатив стала програма «Держава у смартфоні», яка передбачає до 2024 р цифрову трансформацію 100 % публічних послуг, доступних громадянам та бізнесу. Зазначене і спонукало до обґрунтування ідеї **створення цифрової платформи для взаємодії суб'єктів кримінального провадження**. Вбачається, що створення такої платформи може стати додатковою гарантією забезпечення прав та законних інтересів особи під час досудового розслідування, особливо у зв'язку з наявністю у правозастосовній практиці фактів підміни обшуку «добровільним» оглядом; проведення зовнішнього спостереження за особою без законних на те підстав; розповсюдження в мережі Інтернет персональної інформації, отриманої під час досудового розслідування⁶; не відкриття частини матеріалів досудового розслідування у процесі реалізації нормативних приписів ст. 290 КПК; знищення фактичних даних, що свідчать про невинуватість особи у вчиненні кримінального правопорушення тощо.

Вдосконалення національної моделі виявлення кримінальних правопорушень та їх розкриття.

З огляду на окреслені вище аспекти логічним продовженням нашого дослідження повинно стати визначення можливих напрямів адаптації кримінального процесуального доказового права до цифрових реалій сьогодення і викликів найближчого майбутнього з огляду на те, що формування доказової інформації нерозривно зв'язано з потенційним обмеженням прав особи, а отже, важливим є належне його регламентування. До того ж відповідні норми КПК характеризуються певною застарілістю порівняно не лише з подібними нормативними приписами в законодавстві інших держав, але навіть щодо інших процесуальних галузей права (адміністративного, господарського, цивільного). Отже, окреслимо перспективні напрями розвитку.

1. *Визначення місця цифрової інформації та її носіїв у системі процесуальних джерел доказів.* У світлі цього варто звернути увагу на існування істотної плюральності до вирішення цього питання у теорії кримі-

нального процесу: від прагнення віднести цю категорію об'єктів до традиційних процесуальних джерел доказів (лише документів, або тільки речових доказів, або одночасно і до перших і до других залежно від того, яка саме інформація має доказове значення у кримінальному провадженні) до визнання нагальної об'єктивної потреби виокремлення цифрових джерел доказової інформації як самостійного процесуального джерела.

У ключі зазначеної дискусії зазначимо, що через відсутність константного зв'язку між цифровою інформацією та її матеріальним носієм досить складно видається заперечувати наявність таких властивих їй специфічних особливостей, як транслюваність (можливість бути переданою з одного носія на інший), мультиплікативність (можливість існування однієї і тієї інформації одночасно на різних, не зв'язаних та не з'єднаних між собою, носіях), а також мінливість (можливість бути видаленою, повністю чи частково зміненою тощо за відсутності безпосереднього «фізичного» доступу або взагалі без участі людини з використанням відповідного програмного забезпечення)⁷. А тому, на наш погляд, більш доцільними убачаються не спроби «вписати» цифрову інформацію та її носії у незмінну, мабуть, вже протягом декількох десятиліть систему доказів і їх процесуальних джерел, а з огляду на не заперечення її специфіки, визнання за цими об'єктами самостійного доказового значення і, відповідно, розширення кола процесуальних джерел доказів.

Особливо актуальним це питання стає з урахуванням появи зовсім нових, повністю безпредметних, нематеріальних проявів доказової інформації, наприклад, так званої «доріжки електронно-цифрових слідів», тобто «системи утворення слідів у інформаційно-телекомунікаційній мережі, яка складається з декількох хронологічно розташованих і логічно зв'язаних записів про проходження комп'ютерної інформації лініями зв'язку через комутаційне обладнання оператора (-ів) зв'язку від комп'ютера злочинця до комп'ютера потерпілого»⁸.

2. Розширення законодавчо регламентованих способів формування доказової інформації у кримінальному процесі. Йдеться про суттєве оновлення закріпленої у кримінальному процесуальному законі системи способів збирання та дослідження доказів. На нашу думку, запровадження точкових змін, на кшталт передбачення правил про обов'язкову участь спеціаліста у ході проведення слідчих (розшукових) дій, під час яких може постати питання про отримання цифрової інформації та вилучення її матеріальних носіїв, не здатне повною мірою відреагувати на сучасну інформаційно-технологічну реальність. Необхідною уявляється зміна погляду взагалі на систему існуючих процесуальних дій та розуміння їх юридичної природи. У цьому ракурсі важливо також відмітити певну фрагментарність та непослідовність тих пропозицій, про які зазначалося вище. Передусім, йдеться про окремі приписи вже згадуваного проекту Закону «Про внесення змін до деяких законодавчих актів щодо імплементації положень Конвенції про кіберзлочинність та підвищення ефективності боротьби з кіберзлочинністю», згідно з якими санкція на проведення обшуку автоматично дозволяє уповноваженим суб'єктам отримувати доступ до електронних інформаційних систем або їх частин, мобільних терміналів, систем зв'язку, інформаційних (автоматизованих), телекомунікаційних, інформаційно-телекомунікаційних систем або невід'ємних частин цих систем, а також можливість отримання такого доступу навіть у виняткових випадках, коли на них не поширюється дозвіл на проведення обшуку. Як буде проілюстровано далі, подібний підхід цілком нівелює ідею стосовно необхідності подвійного судового контролю – окремо за обмеженням права на недоторканність житла чи іншого володіння особи, та окремо на обмеження права на приватність.

Як продовження дослідження на конкретному прикладі продемонструємо ситуації, зв'язані із можливим втручанням у приватне спілкування за результатами проведення таких дій, як обшук та огляд. Зокрема, останнім часом у правозастосовній практиці досить поширеними є випадки так званого «огляду предмета – цифрового пристрою» (смартфона, планшета, комп'ютера тощо) з метою виявлення та копіювання цифрової інформації, яка зберігається на цих носіях, для її дослідження та використання у кримінальному провадженні. Водночас слідчий, вилучивши певний цифровий пристрій (телефон, комп'ютер, планшет) і оглядаючи цей предмет, зазвичай не обмежується візуальним спостереженням його зовнішніх ознак (що є оглядом предмета у його традиційному розумінні), а намагається отримати інформацію іншого характеру – про смс-повідомлення, повідомлення в Viber, WhatsApp, Telegram, прослухати записані телефонні розмови (оскільки деякі смартфони передбачають таку функцію). Характер таких дій по суті означає втручання у приватне спілкування особи, яке вимагає обов'язкового судового контролю. Крім того, очевидно, що огляд предмета в його класичному розумінні як візуального спостереження ознак певного матеріального об'єкта не відповідає характеру тих дій, які здійснюються з метою дослідження інформації, що може зберігатися у відповідному девайсі.

Звертаючи увагу на цю проблему, Р.І. Оконенко пропонує використовувати поняття «обшук цифрового пристрою», оскільки це, на думку дослідника, відповідатиме природі слідчої дії, яка проводиться в такому випадку⁹. Контекстно зазначимо, що подібний різновид слідчої дії наразі вже передбачений ст. 19 Конвенції про кіберзлочинність. Розмірковуючи у цьому ракурсі, А.В. Шило підкреслює, що оскільки інформація, яка міститься на вилучених у ході процесуальних дій електронних пристроях, не може ототожнюватися із самим електронним пристроєм як її фізичним носієм, то вона є окремим об'єктом права власності та об'єктом права на приватність, а тому її вилучення та/або копіювання вимагає отримання окремого судового рішення – ухвали слідчого судді про залучення експерта для проведення експертизи¹⁰. Не заперечуючи раціональність та обґрунтованість наведених пропозицій, на нашу думку, більш доцільним все ж таки застосування в цьому випадку порядку тимчасового доступу до цифрової інформації шляхом ознайомлення з нею та її копіювання. Причому, якщо для такого доступу необхідне подолання логічного захисту (тобто цифровий пристрій захищений паролем), то необхідним є залучення спеціаліста.

У контексті зазначеної пропозиції ми підтримуємо також висновки А. Скрипника про необхідність адаптації досвіду окремих країн до вітчизняного кримінального процесуального законодавства щодо запро-

вадження правила «закритого контейнеру», яким би передбачався двоступеневий судовий контроль за обмеженням права особи на таємницю спілкування¹¹.

3. *Зміна концептуальних підходів до перевірки та оцінки доказів у кримінальному процесі.* Сучасна «цифрова» людина завжди має під рукою смартфон або планшет; значна частина вулиць, комунальних і приватних будівель обладнана засобами відеоспостереження; автомобілі укомплектовані приладами, придатними фіксувати зміни швидкості, часу та місце розташування у просторі, а також відеореєстраторами. З огляду на це, майже кожен із нас може потенційно стати «збирачем» доказової інформації, що матиме значення для встановлення обставин кримінального правопорушення. До того ж подібна інформація у цифровій формі, створена за допомогою перелічених гаджетів, може бути миттєво переданою до мережі Інтернет та розміщена на загальнодоступних сайтах. Однак, з урахуванням чинного нормативного врегулювання питань, зв'язаних із перевіркою та оцінкою доказів, такою їх властивістю, як допустимість, ця цифрова інформація, навіть не зважаючи на її важливість і силу, досить часто не може бути використаною як доказ у кримінальному провадженні.

Саме тому існує нагальна потреба у зміні законодавчих підходів до регламентації порядку перевірки та оцінки доказів, критеріїв допустимості останніх. Вихідне значення повинно мати не суворе дотримання встановлених, досить часто занадто «формалізованих» правил отримання доказової інформації та її носіїв, а технічна можливість верифікації автентичності цифрової інформації, що представляється суду для дослідження¹². Тобто на нашу думку, первинним критерієм допустимості використання цифрової інформації та її носіїв у кримінальному процесі як засобу доказування обставин, що мають значення для кримінального провадження, має бути наявність технічних можливостей підтвердити автентичність такої інформації.

Створення цифрової платформи для взаємодії суб'єктів кримінального провадження.

Зважаючи на те, що кримінальна процесуальна діяльність являє собою систему заснованих на законі дій та процесуальних рішень, які здійснюються органами держави і всіма особами, які беруть участь в провадженні, поступовій цифровізації, на наш погляд, підлягають всі дії та процесуальні рішення осіб, які беруть участь у кримінальному провадженні.

Вочевидь, одним із напрямів такого оцифрування або «діджиталізації» кримінального процесу має стати створення цифрової платформи для взаємодії суб'єктів кримінальної процесуальної діяльності, оскільки це дасть змогу забезпечити правовий режим транспарентності кримінального процесу, тобто його прозорості, «відкритості» для учасників кримінального провадження.

З огляду на це визначимо потенційні напрями реалізації ідеї щодо створення означеної вище платформи:

1. *Закріплення можливості подачі заяви, повідомлення про вчинення кримінального правопорушення шляхом електронного звернення.* Наразі кримінальне процесуальне законодавство передбачає дві форми заяв: усні або письмові, тобто де *jure* електронні звернення не виділяються в окремий вид. Водночас, виходячи зі змісту п. 1 розділу IV Порядку ведення єдиного обліку в органах (підрозділах) поліції заяв і повідомлень про кримінальні правопорушення та інші події на рівні цього відомчого акта, все ж таки передбачена можливість звернення до органу (підрозділу) поліції із заявами (повідомленнями) з використанням *мережі Інтернет, електронного зв'язку (електронні звернення)*¹³. До того ж на сайті Національної поліції є відповідна форма для подачі електронного звернення¹⁴. У цьому контексті варто зазначити, що подача звернень на сайті Національної поліції відбувається в порядку Закону України «Про звернення громадян». Існує можливість залишення електронного повідомлення про корупційне кримінальне правопорушення і через сайт Національного антикорупційного бюро України¹⁵. Однак порядок роботи із таким зверненням передбачає їх роздрукування на папері й подальшу роботу як з письмовою заявою, що, звісно, не відповідає моделі електронного документообігу. Подібна практика призводить до дублювання інформації, що безумовно заважає процесу документообігу через накопичення паперової роботи поряд із одночасним запровадженням цифрових технологій. З огляду на це доводиться констатувати, що прагнення закріпити можливість подання електронного звернення задля полегшення роботи із реєстрації заяв і повідомлень про кримінальні правопорушення, по суті, спричинило навпаки її ускладнення.

Зрозуміло, що повна відмова від паперових носіїв інформації наразі неможлива, і протягом певного перехідного періоду паперовий документ все ще залишатиметься основним носієм доказової інформації. Серед переваг використання електронних звернень слід навести, наступні. *По-перше*, це дає змогу безкоштовно (або з мінімальними витратами на послуги мережі Internet) відправити будь-яку за обсягом інформацію в найкоротший строк; *по-друге*, таким чином суттєво спрощується забезпечення виконання вимоги щодо обов'язкового попередження про кримінальну відповідальність, зважаючи на те, що на офіційному сайті органу, до якого надсилається повідомлення про кримінальне правопорушення, перед заповненням відповідної форми розміщується повідомлення про кримінальну відповідальність за завідомо неправдиве повідомлення про вчинення злочину за ст. 383 КК України. Таким чином спрощується забезпечення виконання вимоги щодо обов'язкового попередження про кримінальну відповідальність, зважаючи на те, що на офіційному сайті розміщено повідомлення про кримінальну відповідальність. Тобто особа вже ознайомена із цим законодавчим приписом. Чого не можна сказати про ситуацію, коли особа направляє поштовим зв'язком відповідний паперовий варіант звернення.

Випереджаючи час та сучасний стан розвитку системи реєстрації й реагування на заяви і повідомлення про вчинення кримінального правопорушення в Україні, цікаво буде навести приклад інших країн. Так, вчені із Мадридського університету імені Карла III і Кардіфського університету в Уельсі розробили штучний інтелект – алгоритм VeriPol, який здатен виявляти неправдиві повідомлення в поліцію на основі аналізу їх змісту. Ця технологія була протестована поліцією Іспанії у 2017 р.: зокрема, слідчі перевіряли висновки штучного інтелекту на особистих зустрічах із заявниками – цікаво, що у 83 % випадків версія заявника не підтверджу-

валася, наслідком чого стало закриття провадження¹⁶. Зрозуміло, що наразі в умовах українських реалій здається, що такий рівень технологічності є недосяжним. Однак в епоху цифровізації все настільки швидко змінюється, що ми скоро самі опинимося в епіцентрі схожих подій.

Наведене вище дає можливість зробити висновок про те, що наразі потребують зміни законодавчі підходи щодо порядку роботи із електронними зверненнями з заявами і повідомленнями про кримінальні правопорушення.

2. Створення єдиного електронного реєстру матеріалів досудового розслідування, що має забезпечити вільний доступ сторін до матеріалів провадження. Такий доступ до матеріалів провадження повинен передбачати різні можливості: (а) онлайн подання процесуальних документів, обмін документами між учасниками, судами, установами; (б) онлайн доступ до всіх відкритих матеріалів; (в) забезпечення ідентифікації особи у кримінальному провадженні за допомогою електронного підпису, за яким можна встановити, що документ в електронній формі підписала саме конкретна особа; (г) обмін повідомленнями онлайн; (д) отримання результатів розгляду клопотань учасниками провадження та інше.

Створення такого електронного реєстру має на меті забезпечити: *по-перше*, спрощений доступ сторін та суду до матеріалів провадження у будь-який час та у будь-якому місці; *по-друге*, можливість безоплатного відображення документів; *по-третє*, створення додаткової гарантії забезпечення права сторони кримінального провадження на доступ до процесуальної інформації і ознайомлення з матеріалами провадження; *по-четверте*, уникнення ситуацій порушення закону, коли суд вимушений визнати докази недопустимими внаслідок того, що сторона провадження не виконала вимог ст. 290 КПК і не відкрила певний матеріал; *по-п'яте*, скорочення строків здійснення досудового розслідування та судового розгляду шляхом скорочення строків для направлення документів поштовим зв'язком і терміну, необхідного для ознайомлення із матеріалами провадження (можна ознайомлюватися у будь-який час, а не тільки в робочий); *по-шосте*, скорочення розміру процесуальних витрат на виготовлення копій матеріалів, їх роздрукування, поштові витрати, витрат, зв'язаних із прибуттям до місця досудового розслідування або судового провадження для особистої подачі документів; *по-сьоме*, структурування та систематизація матеріалів кримінального провадження, *по-восьме*, зниження ризику фальсифікації документів, перевищення повноважень владними учасниками провадження тощо.

Висновки. Узагальнюючи викладене, нами запропоновано такі напрями вдосконалення національної моделі досудового розслідування щодо забезпечення прав та законних інтересів особи в умовах діджиталізації кримінального провадження.

Проведене дослідження дає підстави стверджувати, що процес цифрової трансформації кримінального провадження, хоча і знаходиться на початковому етапі, втім, вбачається перспективним напрямом для подальших наукових розвідок. Крім того, нагальною є необхідність вдосконалення чинного кримінального процесуального законодавства, особливо в частині нормативного визначення цифрової інформації та її носіїв у системі процесуальних джерел доказів, та проведення обшуку, зв'язаного з доступом до цифрових носіїв інформації.

¹ «Діджиталізація» – слово 2019 року в Україні за версією онлайн-словника «Мислово». URL: <https://itc.ua/news/didzhi-talizacziya-slovo-2019-roku-v-ukrai-na-ver-si%D1%97ni-za-versi%D1%94yu-onlajn-slovnika-mislovo/> (дата звернення: 10.02.2019).

² Спецпроект: Digital та права людини. URL: <https://medium.com/@aiukraine/%D1%81%D0%BF%D0%B5%D1%86%D0%BF%D1%80%D0%BE%D0%B5%D0%BA%D1%82-digital-%D1%82%D0%B0-%D0%BF%D1%80%D0%B0%D0%B2%D0%B0-%D0%BB%D1%8E%D0%B4%D0%B8%D0%BD%D0%B8-c2d312601cc4> (дата звернення: 10.02.2019).

³ Резолюція Ради ООН з прав людини «про сприяння, захист і реалізацію прав в інтернеті» від 27.06.2016 р. URL: https://www.article19.org/data/files/Internet_Statement_Adopted.pdf (дата звернення 10.02.2019).

⁴ У контексті нашого дослідження нами використовується термін *privacy* як узагальнююче поняття, під яким розуміється право людини на повагу до приватного і сімейного життя, яке складається з права на повагу до приватного життя, сімейного життя, житла, кореспонденції і гарантується ст. 8 ЄКПЛ.

⁵ Проект Закону України «Про внесення змін до Кримінального процесуального кодексу України та Кримінального кодексу України (щодо вдосконалення порядку застосування окремих заходів забезпечення кримінального провадження)» № 2740 від 15.01.2020 р.

⁶ Тополевський Р. Право на приватність / Сайт Української Гельсінської спілки з прав людини. 7 березня 2017 р. URL: <https://helsinki.org.ua/pravo-na-privatnist-r-topolevskyj/> (дата звернення: 10.02.2019).

⁷ Пашнев Д.В. Властивості комп'ютерної інформації та особливості збирання комп'ютерних слідів. *Ученые. записки Таврич. нац. ун-та им. В.И. Вернадского*. 2006. Т. 19 (58). № 2. С. 297–298 (Серия «Юрид. науки»).

⁸ Электронные носители информации в криминалистике: монография / под ред. О.С. Кучина. Москва : Юрлитинформ, 2017. С. 164.

⁹ Оконенко Р.И. Электронные доказательства и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации: дис. ... канд. юрид. наук. Москва, 2016. С. 120–121.

¹⁰ Шило А.В. Використання в кримінальному провадженні відомостей, отриманих у результаті проведення негласних слідчих (розшукових) дій: автореф. дис. ... канд. юрид. наук : 12.00.09; Нац. юрид. ун-т ім. Ярослава Мудрого. Харків, 2019. С. 14.

¹¹ Скрипник А. Правило «закритого контейнеру» в українських правових реаліях. *Кримінальний процес: сучасний вимір та перспективні тенденції* : II Харк. кримінал. процесуал. полілог : присвяч. актуал. питанням застосування заходів забезпечення кримінал. провадження (м. Харків, 12 груд. 2019 р.) / редкол. О.В. Капліна, В.І. Маринів, О.Г. Шило. Харків : Право, 2020. С. 29–31.

¹² Кувычков С.И. Использование в доказывании по уголовным делам информации, представленной в электронном виде: дисс. ... канд. юрид. наук. Нижний Новгород, 2016. С. 13.

¹³ Про затвердження Порядку ведення єдиного обліку в органах (підрозділах) поліції заяв і повідомлень про кримінальні правопорушення та інші події: наказ Міністерство внутрішніх справ України від 08 лютого 2019 р. № 100. *Офіційний вісник України*. 2019. № 26. С. 292. Ст. 939, код акта 93922/2019.

¹⁴ Подати звернення. Офіційний сайт Національної поліції: URL: <https://www.npu.gov.ua/podati-zvernennya.html> (дата звернення: 10.02.2019).

¹⁵ Повідомлення про корупційне кримінальне правопорушення. URL: <https://nabu.gov.ua/povidomlennya-pro-korupciyne-kruminalne-pravoporushennya> (дата звернення: 10.02.2019).

¹⁶ Ученые из Уэльса и Испании разработали ПО, оказавшееся настолько эффективным, что его на вооружение взяли испанские полицейские. Алгоритм VeriPol определяет, на какие заявления полиции не стоит тратить силы. URL: <https://high.tech.plus/2018/10/29/ii-detektor-lzhi-vichislyayet-vruna-po-ego-pismam> (дата звернення: 10.02.2020).

Резюме

Демура М.І., Кленка Д.І., Крицька І.О. Забезпечення прав та законних інтересів особи в умовах «діджиталізації» кримінального провадження.

У статті розглядаються питання захисту прав та законних інтересів особи в умовах «діджиталізації» кримінального провадження України. На підставі проведеного дослідження сформульовано вектори цифрової трансформації досудового розслідування. Першим вектором запропоновано виокремити вдосконалення національної моделі виявлення кримінальних правопорушень та їх розкриття, до якого входять такі напрями: визначення місця цифрової інформації та її носіїв у системі процесуальних джерел доказів; розширення законодавчо регламентованих способів формування доказової інформації у кримінальному процесі; зміна концептуальних підходів до перевірки та оцінки доказів у кримінальному процесі. Другим вектором пропонується вважати створення цифрової платформи для взаємодії суб'єктів кримінального провадження. Потенційними напрямками реалізації означеного вектору вважаємо закріплення можливості подачі заяви, повідомлення про вчинення кримінального правопорушення шляхом електронного звернення; створення єдиного електронного реєстру матеріалів досудового розслідування та судового розгляду.

Ключові слова: діджиталізація, кримінальний процес, цифровізація, електронні докази, електронні звернення, цифрова інформація.

Резюме

Демура М.И., Кленка Д.И., Крицкая И.А. Обеспечение прав и законных интересов лица в условиях «диджитализации» уголовного производства.

В статье рассматриваются вопросы защиты прав и законных интересов личности в условиях «диджитализации» уголовного производства Украины. На основании проведенного исследования сформулированы векторы цифровой трансформации досудебного расследования. Первым вектором предложено выделить совершенствование национальной модели выявления уголовных правонарушений и их раскрытия, в который входят следующие направления: определение места цифровой информации и ее носителей в системе процессуальных источников доказательств; расширение законодательно регламентированных способов формирования доказательственной информации в уголовном процессе; изменение концептуальных подходов к проверке и оценке доказательств в уголовном процессе. Вторым вектором предлагается считать создание цифровой платформы для взаимодействия субъектов уголовного производства. Потенциальными направлениями реализации указанного вектора считаем закрепление возможности подачи заявления, сообщения о совершении уголовного преступления путем электронного обращения; создание единого электронного реестра материалов досудебного расследования и судебного разбирательства.

Ключевые слова: диджитализация, уголовный процесс, цифровизация, электронные доказательства, электронные обращения, цифровая информация.

Summary

Maryna Demura, Daria Klepka, Iryna Krytska. Ensuring of the rights and legal interests of the person in the conditions of "digitalization" of criminal proceedings.

The article identifies and characterizes perspective vectors of digital transformation of pre-trial investigation through the prism of ensuring the rights and legitimate interests of the individual.

In particular, the first vector of digital transformation of pre-trial investigation is the improvement of the national model of detection and disclosure of criminal offenses. Its separation is due to the fact that the rules of the current criminal procedural legislation differ with certain archaicity about the latest manifestations of illegal acts on the network, since they contain general rules for the protection of rights and legitimate interests of a person against threats in reality, without considering the possibility of committing criminal offenses online. The main directions of this vector include: (1) determining the position of digital information and its media in the system of procedural sources of evidence; (2) expanding the legislatively regulated ways of generating evidentiary information in criminal proceedings; (3) change of conceptual approaches to the verification and evaluation of evidence in criminal proceedings.

At the same time, the second vector of digital transformation of pre-trial investigation should be the creation of a digital platform for the interaction of the criminal proceedings subjects. The article highlights the potential directions for implementing the idea of creating a designated platform: a) fixing the possibility of filing an application, notification of a criminal offense through electronic appeal; b) the creation of a single electronic register of pre-trial investigation and trial materials, which should ensure free access of parties to the material of proceedings. According to the authors of the article, such access to the materials of the proceedings should provide various possibilities: (1) online submission of procedural documents, exchange of documents between participants, courts, institutions; (2) online access to all publicly available material; (3) ensuring the identification of a person in criminal proceedings by means of an electronic signature whereby it can be established that the document is signed electronically by a specific person; (4) messaging online; (5) obtaining the results of the consideration of the petitions by the parties to the proceedings, and more.

Key words: digital transformation, ensuring the rights and legitimate interests, pre-trial investigation, digital platform, digital evidence, verification and evaluation of evidence.

DOI: 10.36695/2219-5521.1.2020.60

УДК 343.292

М.Д. ДЕНИСОВСЬКИЙ, І.О. ТОМЧУК

Михайло Дмитрович Денисовський, кандидат юридичних наук, декан юридичного відділення Галицького коледжу імені В'ячеслава Чорновола*
ORCID: 0000-0002-2265-4190

Інна Олександрівна Томчук, кандидат юридичних наук, завідувач кафедри Галицького коледжу імені В'ячеслава Чорновола**
ORCID: 0000-0001-9234-043X

ЗДІЙСНЕННЯ ПОМИЛУВАННЯ ЗА ЗАКОНОДАВСТВОМ УКРАЇНИ ТА ЗАРУБІЖНИХ КРАЇН: ПРОБЛЕМНІ АСПЕКТИ

Постановка проблеми. На сучасному етапі державна політика у сфері кримінального права в Україні першочергово спрямована на те, щоб кожен, хто вчинив злочин, був притягнутий до кримінальної відповідальності і поніс відповідно законне й справедливе покарання. Проте застосування виключно каральних заходів бажаних результатів у процесі боротьби зі злочинністю досягти вкрай важко. Поряд з такими принципами кримінального права як законність, справедливість, невідворотність покарання, знаходиться місце застосування не менш важливого принципу гуманізму. Проявом останнього є нормативне закріплення в кримінальному законодавстві інституту звільнення від покарання та його відбування, в межах якого і надалі складним та дискусійним залишається помилування.

Слід зазначити, що інститут помилування засуджених функціонує майже в усіх країнах світу незалежно від форми правління, державного устрою та правової системи та має свої особливості застосування, які доцільно було б розглянути та проаналізувати з метою запозичення позитивного досвіду. Таким чином, неабиякий науковий інтерес викликає дослідження як вітчизняного, так і зарубіжного законодавства з питань застосування помилування.

Аналіз останніх досліджень і публікацій. Серед вітчизняних та зарубіжних науковців, які останнім часом займалися дослідженням проблем правового механізму реалізації права помилування можемо назвати таких, як І.Г. Богатирьов, В.Г. Гончаренко, О.П. Горюх, В.М. Додонов, А.А. Музика, Є.О. Письменський, М.І. Сірий, О.В. Чепелюк, С.М. Школа та інші.

© М.Д. Денисовський, І.О. Томчук, 2020

* *Mykhaylo Denysovskyy, Ph.D. in Law, Lecturer of Law Vyacheslav Chornovil Halytskyi College*

** *Inna Tomchuk, Ph.D. in Law, Lecturer of Law Vyacheslav Chornovil Halytskyi College*