ЗАКОН УКРАЇНИ «ПРО ВНЕСЕННЯ ЗМІН ДО КРИМІНАЛЬНОГО ПРОЦЕСУАЛЬНОГО КОДЕКСУ УКРАЇНИ ТА ЗАКОНУ УКРАЇНИ «ПРО ЕЛЕКТРОННІ КОМУНІКАЦІЇ» ЩОДО ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ДОСУДОВОГО РОЗСЛІДУВАННЯ «ЗА ГАРЯЧИМИ СЛІДАМИ» ТА ПРОТИДІЇ КІБЕРАТАКАМ» № 2137–IX: АНАЛІЗ НОВЕЛ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ

Матеріал підготували:

- *Ірина ГЛОВЮК – Заслужений юрист України, адвокат, д.ю.н., професор;*
- *Віктор ЗАВТУР – к.ю.н., адвокат*

Сьогодні набули чинності зміни до КПК України, внесені Законом України «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» № 2137–IX (http://www.golos.com.ua/documents/z-2137-ix.pdf), які торкнулися багатьох інститутів кримінального провадження: статусу спеціаліста, документів як джерела доказів, фіксування кримінального провадження, процесуальних документів, заходів забезпечення кримінального провадження, слідчих (розшукових) та негласних слідчих (розшукових) дій, особливого режиму досудового розслідування та продовження строків тримання під вартою під час судового провадження в умовах воєнного, надзвичайного стану або у районі проведення антитерористичної операції чи заходів із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії Російської Федерації та/або інших держав проти України.

Охарактеризуємо зміни, які торкаються загального порядку кримінального провадження.

Закон України № 2137-IX передбачає уточнення у ст. 71 КПК України процесуального статусу спеціаліста, вказуючи на його право надавати «консультації, пояснення та довідки». Окремо доповнено перелік прав спеціаліста у ч.4 цієї статті пунктом 8 «надавати довідки з питань, що належать до сфери його знань, у випадках, передбачених ч.3 ст. 2451 КПК України». Чинний КПК України і положення Закон України № 2137-IX не деталізують нормативних вимог до змісту такої довідки. Із цього можна зробити висновок, що вона як джерело доказів відноситиметься до документів.

Внесено деякі термінологічні зміни до положень ст. 99 КПК України. В редакції, передбаченої Законом України № 2137-IX вони формулюються наступним чином:

П.1 ч.2 ст. 99 КПК України: 1) матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі комп'ютерні дані);

Ч.4 ст. 99 КПК України: Дублікат документа (документ, виготовлений таким самим способом, як і його оригінал), а також копії інформації, у тому числі комп'ютерних даних, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних

системах, комп'ютерних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа.

Пункт 3 ч.3 ст. 104 КПК України, яка регламентує зміст протоколу, доповнено новим абзацом такого змісту: «виготовлені дублікати документів, а також копії інформації, у тому числі комп'ютерних даних, та спосіб їх ідентифікації».

У пункті 4 ч.2 ст. 105 КПК України слова «носії комп'ютерної інформації» замінено словами «носії комп'ютерних даних».

Закон України № 2137-IX вперше передбачив виготовлення у разі необхідності оригіналу кримінального процесуального рішення – постанови слідчого, прокурора в електронній формі з використанням кваліфікованого електронного підпису службової особи, яка прийняла відповідне процесуальне рішення або створення його з використанням Інформаційно-телекомунікаційної системи досудового розслідування відповідно до ст. 106-1 КПК України.

Розширено перелік процесуальних витрат, шляхом включення до них витрат, пов'язаних із виготовленням дублікатів і копій документів (п.4 ч.1 ст. 118 КПК України).

Другий абзац ч.1 ст. 159 КПК України, відповідно до Закону України № 2137-IX викладено у такій редакції: «Тимчасовий доступ до електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку здійснюється шляхом зняття копії інформації, що міститься в таких електронних інформаційних системах, комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку, без їх вилучення».

Термінологічного уточнення зазнали і норми ст. 168 КПК України, яка встановлює процесуальний порядок тимчасового вилучення майна. Другий і третій абзаци ст. 168 КПК України після слів «електронних інформаційних систем» доповнено словами «комп'ютерних систем». Термінологічно було уточнено і абзац четвертий ст. 168 КПК України, який передбачає право слідчого, прокурора здійснювати копіювання інформації, що міститься в інформаційних (автоматизованих) системах, телекомунікаційних системах, інформаційно-телекомунікаційних системах, їх невід'ємних частинах. В редакції Закону України № 2137-IX відповідна норма має таке формулювання: «У разі необхідності слідчий чи прокурор виготовляє за допомогою технічних, програмно-технічних засобів, апаратно-програмних комплексів копії інформації, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах. Копіювання такої інформації здійснюється із залученням спеціаліста».

Також ст. 168 КПК України доповнена нормою, відповідно до якої особа, яка здійснює тимчасове вилучення комп'ютерних систем або їх частин, залишає на вимогу їх володільця копії інформації з таких комп'ютерних систем або їх частин з використанням матеріальних носіїв володільця.

Закон України № 2137-IX встановлює процесуальний порядок накладення арешту на комп'ютерні системи чи їх частини у ст. 170 КПК України за наявності альтернативних умов: 1) вони отримані внаслідок вчинення кримінального правопорушення або є засобом чи знаряддям його вчинення; 2) вони зберегли на собі сліди кримінального правопорушення; 3) є необхідність забезпечення спеціальної конфіскації, конфіскації майна як виду покарання або заходу кримінально-правового характеру щодо юридичної особи, відшкодування шкоди, завданої внаслідок кримінального правопорушення (цивільний позов), чи стягнення з юридичної особи отриманої неправомірної вигоди; 4) їх надання разом із інформацією, що на них містяться, є необхідною метою проведення експертного дослідження; 5) доступ до відповідних комп'ютерних систем чи їх частин обмежується власником, володільцем або отримувачем чи пов'язаний із подоланням систем логічного захисту.

Крім того, законодавець розширює перелік майна, на яке може бути накладено арешт у ч.10 ст. 170 КПК України, додаючи до нього віртуальні активи. Віртуальний актив – нематеріальне благо, що є об'єктом цивільних прав, має вартість та виражене сукупністю даних в електронній формі (ст. 1 Закону України «Про віртуальні активи», https://zakon.rada.gov.ua/laws/show/2074-20#Text).

Відмітимо, що під час дії надзвичайного або воєнного стану повноваження слідчого судді щодо надання дозволу на тимчасовий доступ до речей та документів, що містять окремі види охоронюваної законом таємниці, а саме: 1) відомостей, які можуть становити лікарську таємницю; 2) відомостей, які можуть становити банківську таємницю; 3) інформації, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо; 4) персональних даних особи, що знаходяться у її особистому володінні або в базі персональних даних, яка знаходиться у володільця персональних даних делегуються прокурору. Останній наділяється повноваженням здійснити тимчасовий доступ до речей і документів, що містить відповідну охоронювану законом таємницю на підставі постанови, погодженої із керівником органу прокуратури.

Велика кількість змін торкається і проведення слідчих (розшукових) дій, зокрема, у аспекті комп'ютерних систем та комп'ютерних даних (що логічно випливає із назви Закону). Зокрема, слідчий, прокурор набули повноважень долати системи логічного захисту, якщо особа, присутня при обшуку, відмовляється зняти (деактивувати) систему логічного захисту.

При цьому ж, якщо під час обшуку слідчий, прокурор виявив доступ чи можливість доступу до комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, для виявлення яких не надано дозвіл на проведення обшуку, але щодо яких є достатні підстави вважати, що інформація, що на них міститься, має значення для встановлення обставин у кримінальному провадженні, прокурор, слідчий має право здійснити пошук, виявлення та

фіксацію комп'ютерних даних, що на них міститься, на місці проведення обшуку.

Без сумніву, зважаючи на особливості таких систем та необхідність дотримання конвенційних гарантій по ст. 8 Конвенції про захист прав людини і основоположних свобод, відмітимо, що межі розсуду сторони обвинувачення у даному випадку сформульовані надзвичайно широко, дискреція по суті є необмеженою. Це не корелюється із практикою ЄСПЛ, адже «повноваження державних органів на проведення таємного спостереження за громадянами в ході кримінального розслідування визнаються Конвенцією в тій мірі, в якій вони є абсолютно необхідними (див. mutatis mutandis, рішення у справі Klass and Others v. Germany, від 6 вересня 1978 року, п. 42) … закон має з достатньою чіткістю визначати межі такої дискреції, наданої компетентним органам, і порядок її здійснення, з урахуванням законної мети даного заходу, щоб забезпечити особі належний захист від свавільного втручання" … Суд має бути впевненим щодо існування адекватного та ефективного захисту від зловживання, оскільки система заходів таємного спостереження, що розроблена для захисту національної безпеки та громадського порядку, пов'язана із ризиком порушення або навіть зруйнування принципів демократії на підставі її захисту (див. вищевказане рішення у справі Klass and Others v. Germany, пп. 49-50). Такі гарантії захисту мають бути чітко встановлені законом та мають застосовуватись до нагляду за діяльністю відповідних органів або служб. При наглядових провадженнях мають дотримуватись цінності демократичного суспільства настільки добросовісно, наскільки це можливо, зокрема верховенство права, про що прямо говориться у Преамбулі Конвенції (995_004). Верховенство права між іншим (inter alia) передбачає, що втручання органів виконавчої влади у права осіб має підлягати ефективному контролю, який зазвичай має здійснюватись судовим органом, щонайменше як останньою інстанцією, оскільки судовий контроль надає найбільші гарантії незалежності, безсторонності та здійснення належного провадження (див. вищевказане рішення у справі Klass and Others v. Germany, п. 55)» (рішення «Волохи проти України», https://zakon.rada.gov.ua/laws/show/974_138#Text). Вважаємо, що такі повноваження були б релевантними у разі, якщо б дозвіл на їх реалізацію містився б у судовому рішенні, навіть в ухвалі про обшук.

Крім того, передбачається, що особи, які володіють інформацією про зміст комп'ютерних даних та особливості функціонування комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, можуть повідомити про це слідчого, прокурора під час здійснення обшуку, про що вносяться відомості до протоколу обшуку. Проте, як видно з положень КПК України, це не виключає пошуку, виявлення та фіксації комп'ютерних даних на місці проведення обшуку.

Положеннями щодо огляду законодавець вирішив проблему, яка існувала стосовно огляду інтернет-сторінок, профілів у соцмережах, ютуб-каналах, тік току тощо. Огляд комп'ютерних даних визнано різновидом огляду, який проводиться слідчим, прокурором шляхом відображення у протоколі огляду інформації, яку вони містять, у формі, придатній для сприйняття їх змісту (за

допомогою електронних засобів, фотозйомки, відеозапису, зйомки та/або відеозапису екрану, тощо або у паперовій формі).

Систему слідчих (розшукових) дій доповнено такою дією, як зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису. Її сутність полягає у наступному: одержання слідчим, прокурором від особи, яка є власником або володільцем відповідних приладів або засобів, необхідної з метою з'ясування обставин, що мають значення для кримінального провадження, копії фото- або кінозйомки, відеозапису, які було здійснено в публічно доступних місцях, в тому числі в автоматичному режимі, за виключенням місць, що відносяться до приватних помешкань осіб; здійснюється на підставі постанови слідчого, прокурора та, за необхідності, за участю спеціаліста; здійснюється у присутності слідчого, прокурора шляхом копіювання самостійно особою, яка є власником або володільцем відповідних приладів та засобів, або нею за участю спеціаліста відповідних записів на носії, які надаються слідчим, прокурором; про проведення зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису складається протокол. Відмітимо, що, судячи з формулювань, ця дія вже може проводитись у кримінальних провадженнях як щодо злочинів, так і щодо проступків, проте, чомусь дізнавач там не згадується. Аналіз цих положень дозволяє зробити висновок, що у разі відмови виконати постанову слідчого, прокурора застосовуватиметься механізм тимчасового доступу до речей і документів.

Істотні трансформації характеризують і негласні слідчі (розшукові) дії. Зокрема, у статтях 258, 263, 265, 268 КПК України слова «транспортні телекомунікаційні мережі» замінено на «електронні телекомунікаційні мережі». Уточнено визначення у ст. 263 КПК України: зняття інформації з електронних комунікаційних мереж (комплекс технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг) є різновидом втручання у приватне спілкування, яке проводиться без відома осіб, які використовують засоби електронних комунікацій (телекомунікацій) для передавання інформації, на підставі ухвали слідчого судді, якщо під час його проведення можна встановити обставини, які мають значення для кримінального провадження.

Крім того, уточнено назву та зміст негласної слідчої (розшукової) дії, регламентованої ст. 268 КПК України – установлення місцезнаходження радіообладнання (радіоелектронного засобу) є негласною слідчою (розшуковою) дією, яка полягає в застосуванні технічних засобів для отримання від мережевої інфраструктури або мобільного кінцевого (термінального) обладнання відомостей щодо місцезнаходження мобільного кінцевого (термінального) обладнання (точки його підключення до мережі), а в мережі фіксованого зв'язку – даних про фізичну адресу кінцевого пункту мережі без розкриття змісту повідомлень, що передаються, якщо в результаті його проведення можна встановити обставини, які мають значення для кримінального провадження. Відтепер не потребує дозволу слідчого судді установлення місцезнаходження

радіообладнання (радіоелектронного засобу), за заявою його власника. Хоча КПК України це окремо і не прописує, йдеться про письмову добровільну заяву, хоча логічніше було прописати не заяву, а згоду. Проте, ці зміни не вирішують питання, наприклад, у разі, якщо цей засіб належить неповнолітньому, чи можливо установлення місцезнаходження радіообладнання (радіоелектронного засобу) за заявою (згодою) законного представника.
Істотні зміни, які торкаються верифікації фіксування негласних слідчих (розшукових) дій, внесено до ст. 266 КПК України.

Зокрема, передбачено: носії інформації на яких зафіксовані відомості, отримані в результаті проведення зазначених негласних слідчих (розшукових) дій, повинні зберігатися у стані, придатному для їх дослідження, до набрання законної сили вироком суду; носії інформації на яких зафіксовані відомості, отримані в результаті проведення зазначених негласних слідчих (розшукових) дій можуть бути предметом дослідження відповідних спеціалістів або експертів у порядку, передбаченому цим КПК України. Якщо порівняти з попередньою редакцією, то вже нема вимоги, що мають зберігатися технічні засоби, що застосовувалися під час проведення зазначених негласних слідчих (розшукових) дій, а також первинні носії отриманої інформації, а також нема вимоги, що технічні засоби, за допомогою яких отримано інформацію, можуть бути предметом дослідження відповідних спеціалістів або експертів у порядку, передбаченому цим КПК України.

Те, що ці зміни до КПК України скеровані на спрощення порядку збирання та перевірки доказів, і у цій частині спрямовані на забезпечення ефективності досудового розслідування, є безспірним. Разом з тим, деякі зміни потребують додаткової оцінки пропорційності втручання у аспекті обмеження прав людини, оскільки більшість внесених змін містить загальні, а не спеціальні (в умовах воєнного стану) норми й торкається не лише протидії кібератакам, боротьба з якими в умовах інформаційної війни проти України з боку країни-агресора є життєво важливою для усього Українського народу.