Особливості використання інформаційних технологій під час кримінального переслідування в романо-германській (континентальній) системі права

Particularities of the proceedings recording in the Romano-Germanic (continental) law system

Антон Столітній

Ключові слова:

кримінальний процес, континентальна система права, фіксація, електронна комунікація, інформаційні системи.

Key words:

criminal procedure, continental law system, recording, electronic communication, information systems.

Докорінні зміни, які протягом останніх років відбуваються в соціально-політичних, економічних, культурних умовах життя суспільства й держави, актуалізують потребу вдосконалення кримінального процесу України, що вимагає глибокого дослідження не лише вітчизняних реалій, а й зарубіжного правового досвіду.

Питання використання інформаційних технологій у кримінальній процесуальній діяльності досліджувалось вітчизняними вченими у світлі національного законодавства, разом із тим відповідні питання в іноземній практиці вивчено лише фрагментарно, зокрема, такими вченими, як В.В. Білоус, В.В. Бірюков, В.О. Голубєв, М.В. Карчевський, Є.Д. Лук'янчиков, Т.В. Михальчук, А.В. Молдован, А.С. Рибченко, І.В. Рогатюк, М.І. Смирнов, О.Ю. Татаров, В.Г. Уваров, І.Ф. Хараберюш, Д.М. Цехан, С.С. Чернявський ін.

Метою статті є дослідження використання електронних інформаційних технологій під час кримінальної процесуальної діяльності в романо-германській (континентальній) системі права.

Загальноприйнятим у теорії права є розділення романо-германської правової системи на дві гілки: *романську*, типовими представниками якої є Франція, Бельгія, Люксембург, Голландія, Італія, Іспанія, і *германську*, типові представники – Федеративна Республіка Німеччина (далі – ФРН), Австрія, Швейцарія, Швеція. Для з'ясування особливостей регулювання електронної складової кримінальної процесуальної діяльності романо-германського права розглянемо детальніше деякі з указаних держав.

Фіксація кримінальних процесуальних процедур і оформлення матеріалів розслідування в романо-германському праві має низку особливостей.

У Франції письмовим процесуальним документам, зокрема поліцейським протоколам і рапортам, у деяких випадках надається особлива доказова сила, що значно посилює їхнє процесуальне значення. Поряд із протоколами (рапортами), які визнають «рядовими» доказами, є дві інші їхні категорії: 1) протоколи, що мають силу наперед установленого доказу, доки не буде доведено зворотне (використовуються в справах про правопорушення і проступки. Фактично тут існує спростовна презумпція істинності протоколу (рапорту) дізнання (може бути спростовано за допомогою письмових документів або показань свідків)); 2) протоколи, що мають силу наперед установленого доказу, доки не буде ухвалено рішення про їх підроблення. Тут передбачено необхідність їх спростування не просто шляхом надання інших доказів, а подання заяви про підроблення протоколу, яку розглядає Касаційний суд. Доки останній не визнав такий протокол підробленим, його доказова сила є абсолютною для судді. Такі протоколи можуть бути доказами тільки за вузьким колом проступків [4, с. 441].

Поліцейські Німеччини, на яких покладено функції з розслідування злочинів, найменше займаються складанням процесуальних документів і піклуються про дотримання процесуальної форми. Співробітник

поліції зазвичай фіксує результати проведеної слідчої або оперативно-розшукової дії в офіційній пам'ятній книжці співробітника поліції, а згодом у звіті за підсумками розслідування конкретної справи. Цим звітом він зможе скористатися, коли його викличуть до суду й запропонують дати під присягою свідчення з приводу того, що і як він дізнався в ході розслідування цієї справи. Разом із тим можливе і складання протоколу, хоча такого роду протокол сам по собі не визнається джерелом того, що прийнято вважати доказом [3, с. 8].

Електронні технології набули широкого розповсюдження в системі кримінальної юстиції.

Національне кримінально-процесуальне законодавство Німеччини містить низку ключових положень про використання спеціальних технічних засобів під час збирання доказів. Зокрема, Закон про захист свідків під час допиту в кримінальному процесі і про поліпшення захисту свідків (Закон про захист свідків – ZSchG) від 30.04.1998 містить законодавчі підстави допустимості застосування аудіовізуальних засобів у процесі допиту свідків (включено у формі § 58a, 168e і 247a до Кримінально-процесуального кодексу (далі – КПК) ФРН), використання відеозапису під час судових слухань у справі (§ 255a КПК ФРН), а також проведення допиту свідка з використанням засобів відеоконференцзв'язку (далі – ВКЗ) у процесі як досудового слідства (§ 168e КПК ФРН), так і судового розгляду (§ 247a КПК ФРН) [5, с. 69].

Згідно з § 168b КПК ФРН «Протокол про слідчі дії прокуратури», результат слідчих дій прокуратури фіксується в матеріалах справи. Про допит обвинуваченого, свідка чи експерта повинен складатися протокол відповідно до §§ 168 і 168a, якщо це може бути зроблено без значної затримки дій із виробництва дізнання [6, с. 195].

Згідно з § 58a КПК ФРН «Запис допиту», допит свідка може бути записаний на носії зображення та звуку. Він повинен бути записаний 1) у разі допиту осіб молодше 16 років, якщо вони постраждали в результаті злочину, або 2) якщо існує побоювання, що свідок не зможе бути допитаний під час судового розгляду, і запис потрібен для встановлення істини. Використання запису зображення та звуку допустиме тільки для цілей кримінального переслідування й лише тією мірою, якою це необхідно для встановлення істини [6, с. 195].

Правове регулювання використання ВКЗ в кримінальному судочинстві в країнах романо-германської правової сім'ї (системи континентального права) істотно відрізняється від держав англо-американської правової сім'ї (системи загального права) більшою опрацьованістю й деталізацією відповідних процедур [5, с. 69].

У Королівстві Швеції особливістю застосування ВКЗ є диференціація порядку використання ВКЗ залежно від місцезнаходження особи, яка підлягає допиту [5, с. 69].

Запит на проведення судового засідання за допомогою відеоконференції за участю особи, котра знаходиться на території Швеції, подається окружним судом, який має технічну можливість для проведення відеоконференції. Запит при проведенні слідчих дій з особою за допомогою відеоконференції в процесі досудового розслідування має подаватися прокурором і містити вказівку на те, що особа, яка бере участь у слуханнях за допомогою відеоконференції, висловила свою згоду на це. При проведенні слухання в окружному суді надані особою показання розглядаються як отримані поза основним засіданням. Сторони мають бути сповіщені про час і місце отримання доказів, проте можуть не викликатися у випадку, якщо вони не дають показання або не беруть участі в отриманні доказів в іншій якості. За необхідності суд має право запросити перекладача. Свідок або експерт, яких мають заслуховувати за допомогою відеоконференції, мають право використовувати допомогу інших осіб під час проведення слухань (особистого помічника). За необхідності або на вимогу особи, яка підлягає заслуховуванню, окружний суд має право призначити їй помічника для надання юридичної допомоги з оплатою його послуг за рахунок держави [5, с. 69–70].

Прикладом застосування за кордоном у судових засіданнях режиму віддаленої присутності осіб, які беруть участь у судочинстві (зокрема свідків і підсудних), є досвід італійського правосуддя. Під час судового розгляду у справі колишнього прем'єр-міністра Італії Джуліо Андреотті було зареєстровано більше ніж 100 показань, що давалися за допомогою ВКЗ. Із 1996 року в Італії вже діє система, яка дає змогу під час судових засідань отримати зображення одного з більше як 1 200 свідків, до яких застосовуються заходи безпеки, до того ж усім, за винятком судді, його видно лише зі спини. Крім того, передбачена додаткова лінія для приватного спілкування свідка зі своїм адвокатом із окремого приміщення суду. Нині системами ВКЗ в Італії обладнано вже більше ніж 100 приміщень і 30 засекречених пунктів, аналогічні телекомунікаційні термінали знаходяться й у спеціальних в'язницях на островах Асінара та П'яноса, призначених для утримання під вартою членів мафії [5, с. 70–71].

Захисники Джуліо Андреотті оскаржували конституційність застосування відеоконференцій, оскільки суд, отримуючи «заочні» відповіді, не може врахувати нюанси поведінки, які проявляються при особистому спілкуванні, та ще й у стресовій ситуації, але ці заперечення були відхилені [5, с. 71].

Одним із лідерів у використанні технологій безпаперового документообігу в кримінальному судочинстві є Фінляндія. Передумовами для переходу правоохоронних органів Фінляндії на безпаперовий документообіг стали такі: низька щільність населення, віддаленість правоохоронних органів один від одного, а також та обставина, що Фінляндія є одним зі світових лідерів у галузі телекомунікаційних технологій. Щорічне фінансування програми інтегрованого інформаційного простору системи органів кримінальної юстиції та судочинства в період з 1999 по 2004 роки становило в середньому 37 млн. євро [11, с. 12].

Сьогодні інтегрована інформаційна система правоохоронних органів Фінляндії обслуговує 63 судові округи, 6 апеляційних судів і Верховний Суд Фінляндії. Щорічно системою обробляється 90 тис. кримінальних справ, 52% яких розглядається суддею одноосібно. У систему інтегровано 30 пенітенціарних установ, органи кримінальної поліції, прокуратури, судові пристави, управління по збору штрафів за кримінальні злочини й пенітенціарні суди. Головним координатором програми є Міністерство юстиції Фінляндії [11, с. 7].

Результатом роботи системи є повністю електронний документообіг. Більше того, суди практично не займаються скануванням, оскільки документи надходять до судів уже в електронному вигляді. Документи систематизовані тематично в базах даних [9, с. 23].

Із 1 лютого 2002 року у Фінляндії набув чинності Закон «Про електронний документообіг у судах» (The act on E-service in the courts), згідно з яким електронний документ у кримінальному судочинстві є еквівалентним паперовому документові, а роботу в загальній системі електронного документообігу здійснюють кримінальна поліція, тюремні установи, судові пристави, прокуратура й суди [17, с. 1].

Згідно із цим Законом, на території Фінляндії будь-який документ, який подається у звичайній письмовій формі, може бути присланий у вигляді електронного повідомлення (e-message). Закон виділяє кілька форм електронного повідомлення: факс, електронна пошта (e-mail), електронний файл. Якщо за законодавством документ повинен бути підписаний, то електронний підпис є рівноцінним звичайному підпису. Інформаційна безпека досягається різним рівнем доступу, наявністю системи ідентифікації користувача, і тому підпис, крім тих випадків, коли він законодавчо обов'язковий, не використовується в документообігу [16, с. 1].

Електронний документообіг у ФРН базується на трьох комунікаційних платформах: E-Government (електронне урядування), E-Business (електронний бізнес), E-Rechtsverkehr (електронні документи правового змісту). E-Government – комунікаційна платформа (нім. Dokumentationsplattform) для електронної підтримки процесів державного управління, тобто для обміну електронними документами з використанням можливостей Інтернету. Ця платформа покликана забезпечити широкий доступ до документів і їх проектів на всіх стадіях опрацювання [7, с. 26].

У рамках електронного урядування розрізняють три комунікативні рівні (Beziehungsebenen): G2G (англ. Government To-Government) – між владними органами; G2B (Government-To-Business) – між державою та суб'єктами економічної діяльності; G2C (Government-To-Ciuzen) – між органами влади і громадянами, туристами, претендентами на отримання дозволу на проживання або громадянство тощо. За аналогією з комунікативними рівнями галузі електронного бізнесу пропонується ввести також рівень G2E (Goverament-To Employee, між владними органами та їхніми службовцями) – для виокремлення потоків документів, призначених для внутрішнього використання в закритих системах (IntraNet, Workflow-System та ін.) [7, с. 26].

Фахівці розрізняють три сфери застосування електронного урядування (Anwendungsbereiche): 1) E-Assistance (електронна підтримка) – надання органами влади інформації про їхні послуги й контакти, наприклад, адреси відповідальних працівників із різних питань, можливості отримання освіти, відпочинку тощо, зазвичай така Інформація подана на веб-сайтах органів влади; 2) E-Administration (електронне адміністрування) – контакти зі службовцями органів влади за допомогою електронної пошти, обмін електронними документами, наприклад, у процесі стягнення адміністративних зборів або сплати штрафних квитанцій; 3) E-Demokracy (електронна демократія) – електронна підтримка політичних процесів формування громадської думки і прийняття політичних рішень: контакти з політиками, проведення опитувань, надсилання пропозицій щодо змін законодавства, заявки громадян для внесення їх у списки виборців тощо [7, с. 26].

Система кримінальної юстиції ФРН використовує більше ніж 70 баз даних, реєстрів, інформаційно-пошукових систем і аналітичних програм.

У Німеччині з 1972 року функціонує федеральна інформаційна система поліція – INPOL, яка з 2006 року працює в новій модифікації (5-а версія) [15, с. 1]. Сучасна INPOL-neu є Федеральною транснаціональною системою поліції німецького Bundeskriminalamt (BKA) – Федерального відомства кримінальної поліції. Система складається з двох частин: INPOL-zentral у BKA та у відповідних підрозділах поліції земель (Landespolizei) – System INPOL-Land, яку ще називають POLAS чи POLIS [10, с. 1].

Усі важливі дані як місцевого, так і регіонального характеру зберігаються в INPOL-neu. Наприклад, у систему вищими структурами вноситься інформація як про правопорушників, обвинувачених, підозрюваних, потенційних злочинців, так і про контакти (для зв'язку), партнерів, свідків, інформаторів, жертв і зниклих безвісти [14, с. 34].

INPOL-neu надає дві форми баз даних: одну для кримінального розшуку, а іншу у вигляді файлу стандартних запитів. На додаток до швидкого пошуку інформації існує можливість установлення перехресних посилань між підозрюваними, місцями злочину та зброєю. INPOL-neu здатна автоматизовано встановлювати зв'язки-сітки між людьми, об'єктами (автомобілі, житло) та актуальними кримінальними провадженнями [8, с. 1].

Система надає можливість отримати, наприклад, із патрульної машини на місці події або при прикордонному контролі в німецькому аеропорту відповідь на такі питання: «Чи когось шукають? Чи щось шукають? Чи є ордер на арешт? Чи розшукують іноземні держави? Чи є підозрюваний членом злочинної організації? Чи був викрадений автомобіль?» [12, с. 1].

Доступ до INPOL-neu здійснюється або за допомогою програмного забезпечення AGIL (точніше на узгоджені в програмному забезпеченні INPOL місцевості робочої групи), або безпосередньо через систему обробки транзакцій у провінції [12, с. 1].

До INPOL-neu підключені Федеральне відомство кримінальної поліції, поліція земель із її поліцейськими потужностями, Федеральна поліція та митні органи. Співробітники мають різні можливості перегляду даних. Розбіжності доступу до бази даних урегульовано ієрархічно для запобігання доступу до непідвідомчої інформації [8, с. 1].

INPOL-neu має доступ до національних і міжнародних баз даних (Шенгенська інформаційна система (SIS), Європейський інформаційна система (EIC) Європолу). Окрім того, можливий безпосередній доступ до Центральної інформаційної системи трафіку (ZeViS) Федерального органу автомобільного транспорту (KBA) у Фленсбурзі; Центрального реєстру іноземців (BVA) Федерального управління адміністрації в Кельні [14, с. 35].

Також варто звернути увагу на такі програмні продукти, що використовує поліція. EASy, KRISTAL, MERLIN і CASA, що є синонімами rsCASE, – програмне забезпечення для практичної роботи в галузі оперативних досліджень з боку влади. Koyote – програмне забезпечення, що використовується для перетворення (кодування) даних трафіку операторами комунікації. FBS-TH (Fall Bearbeitungs-SystemTHüringen) є системою управління, спрямованою на створення зручного та ефективного кримінального діловодства [13, с. 1].

Відповідно до стандартів, визначених вимогами Європейського Союзу для держав Шенгенської зони, в Угорщині налагоджена робота телекомунікаційної інформаційної мережі, об'єднаної за принципом NCB (National Computer Board). Ця мережа створена за кошти Європейського Союзу й повноцінно функціонує з 2008 року. Вона об'єднує структури Міністерства оборони, Міністерства внутрішніх справ (усі управління, відділи поліції та прикордонної поліції), спеціальних служб Угорщини, дає змогу здійснювати швидкий обмін інформацією в режимі on-line. NCB Угорщини, окрім правоохоронних органів, пов'язана також із мережами цивільних органів управління, системи охорони здоров'я тощо. В Угорщині вже перенесено або ведуться роботи з перенесення в кібернетичну площину таких процесів: електронна система обліку здійснення оподаткування; електронна система актів і свідоцтв громадянського стану (народження, шлюб, смерть тощо); реєстрація та електронний облік видачі документів громадянам (посвідчень, свідоцтв, актів); реєстрація транспортних засобів і посвідчень водіїв; електронна система транспортної інфраструктури; поліцейські реєстри. До нормативно-правових документів, які регулюють цю сферу, належать такі: Стра-

тегія національної безпеки; Суспільна інформаційна стратегія; Національна стратегія безпеки інформаційних мереж та інформації; Стратегія громадського адміністрування електронної сфери Угорщини [1, с. 33].

У Королівстві Бельгія Федеральна служба інформаційних технологій і комунікацій "FedIct" займається реалізацією державної політики у сфері інформатизації, розвитку технологій електронного урядування, загальними питаннями технічного захисту інформації та інформаційного простору. З моменту створення організації у 2001 році FedIct реалізувала низку інноваційних проектів, серед яких найважливішими є запуск федерального електронного порталу надання державних послуг, упровадження електронного посвідчення особи (смарт-картки eID) і створення комплексних систем електронного документообігу державних структур (e-Justice, Tax-on-Web, Police-on-Web). FedIct також надає можливість інтеграції державного електронного документообігу з документообігом приватних компаній та організацій. Портал Бельгії www.belgium.be позиціонується як державна служба, основний напрям розвитку якої – впровадження в практику реального щоденного життя персональних смарт-карт eID, за якими можливі доступ до віртуальних сервісів надання державних послуг, здійснення інтерактивних операцій: управління власним рахунком у банку, сплата штрафів тощо. Отже, в Бельгії цей портал є «єдиною точкою» надання державних послуг [1, с. 6].

Із 2005 року в Бельгії реалізується проект "e-Justice", що дає змогу судам, іншим інститутам судової влади, суб'єктам правових відносин здійснювати електронний обмін документами або взаємодіяти за допомогою Інтернет-технологій. Відповідно, сервіси Tax-on-Web і Police-on-Web надають можливість автоматизувати процеси взаємодії державних органів. Уведено в дію закон, що дає змогу судовій системі працювати з електронними документами. Це допоможе перейти до системи «електронних справ». Така «справа» створюватиметься на самому початку судової процедури, а потім буде «розвиватися» шляхом додавання документів усіх сторін, що беруть участь у процесі: судів, поліції, адвокатів, позивачів та ін. [1, с. 6].

У Німеччині прийнято схожий закон – "Electronic File Management Act". Використання електронних документів прискорить взаємодію між судами та зацікавленими сторонами, а також надасть можливість зробити документи доступними всім зацікавленим особам і організаціям. Крім цього, з'являється можливість подавати звернення, заявки за допомогою мережі Інтернет [2, с. 98].

З огляду на системне впровадження більшістю розвинених держав інноваційних технологій у кримінальну процесуальну діяльність електронне майбутнє кримінального провадження в Україні є неминучим. Указане підтверджує розпочатий із прийняттям КПК України 2012 року процес переходу з паперового до електронного провадження. Відтак чим швидше буде визнано існування останнього з подальшим нормативним закріпленням як провідного напряму розвитку кримінальної юстиції, тим швидше процес переходу буде завершено.

Анотація

У статті розглядаються актуальні питання використання електронних і телекомунікаційних технологій у кримінальній процесуальній діяльності романо-германської (континентальної) системи права.

Summary

In this article we review the actual questions of the use of the electronic and telecommunications systems in the criminal procedural activities of the Romano-Germanic (continental) law system.

Використна література:

1. Досвід взаємодії державних органів країн світу з інститутами громадянського суспільства, залучення громадськості до формування та реалізації державної політики, протидії корупції, забезпечення електронного урядування. Веб-сайт ініціативи «Партнерство Відкритий Уряд» [Електронний ресурс]. – Режим доступу : http://www.ogp.gov.ua/sites/default/files/library/Dosvid_OGP-MFA.pdf.
2. Дубов Д.В. Основи електронного урядування : [навчальний посібник] / Д.В. Дубов, С.В. Дубова. – К. : Центр навчальної літератури, 2006. – 448 с.
3. Ларичев В.В. Предварительное расследование преступлений в США и Германии : автореф. дисс. … канд. юрид. наук / В.В. Ларичев. – М., 2004. – 24 с.
4. Лобойко Л.М. Кримінально-процесуальне право : [навчальний посібник] / Л.М. Лобойко. – К. : Істина, 2005. – 456 с.
5. Михальчук Т.В. Використання інформації, отриманої телекомунікаційним шляхом, у розслідуванні злочинів : дис. ... канд. юрид. наук : спец. 12.00.09 / Т.В. Михальчук. – К., 2009. – 222 с.
6. Пастухов П.С. «Электронные доказательства» в состязательной системе уголовно-процессуальных доказательств / П.С. Пастухов // Общество и право. – 2015. – № 1 (51). – С. 192–196.
7. Рудюк В.В. Класифікація електронних документів ФРН / В.В. Рудюк // Бібліотекознавство. Документознавство. Інформологія / Міністерство культури і туризму України, Державна академія керівних кадрів культури і мистецтв. – Київ, 2005. – № 3. – С. 26–31.
8. Datenbanken BKA [Електронний ресурс]. – Режим доступу : http://www.datenschmutz.de/moin/Datenbanken%20BKA.
9. Duizend R.V. Guidelines for State Trial Courts Regarding Discovery of Electronically-Stored Information / R.V. Duizend // Materials of Conference of Chief Justices. – 2005.
10. Elektronische Fahndungs und Informationssysteme [Електронний ресурс]. – Режим доступу : http://www.bka.de/nn_205962/DE/ThemenABisZ/ElektronischeFahndungssysteme/elektronischeFahndungssysteme__node.html?__nnn=true.
11. Kujanen K. E-services in the Finnish Courts / K. Kujanen // Proceedings of the Court Technology Conference 8. – Kansas City, 2003.
12. Neues Polizei-Computersystem so einfach wie Internet [Електронний ресурс]. – Режим доступу : http://www.heise.de/newsticker/meldung/Neues-Polizei-Computersystem-so-einfach-wie-Internet-60573.html.
13. Polizei-IT-Anwendungen [Електронний ресурс]. – Режим доступу : https://de.wikipedia.org/wiki/Polizei-IT-Anwendungen.
14. Reboot: Das polizeiliche Informationssystem INPOLNEU und der Datenschutz [Електронний ресурс]. – Режим доступу : http://chaosradio.ccc.de/media/ds/ds082.pdf.
15. Schulzki-Haddouti C. Fass ohne Boden / C. Schulzki-Haddouti [Електронний ресурс]. – Режим доступу : http://www.heise.de/tp/artikel/4/4769/1.html.
16. The act on electronic signatures in Lainsaadanto // Statens Forfattningsdata. – Finland, 2005.
17. The act on E-service in the courts in Lainsaadanto // Statens Forfattningsdata. – Finland, 2005.

Антон Столітній,
кандидат юридичних наук,
викладач відділу підготовки прокурорів з нагляду за додержанням законів органами,
які проводять досудове розслідування,
Національної академії прокуратури України