

ДРОЗДОВ Олександр Михайлович

професор, доктор юридичних наук,
заслужений юрист України, адвокат,
член Комісії з питань правової реформи при
Президентові України,
член Апеляційної палати НАЗЯВО,
член Науково-консультативних рад при
Конституційному Суді України та Верховному Суді,
почесний професор кафедри кримінального права та
кримінології, міжнародного публічного права та
міжнародних відносин Юридичного факультету
Університету Барселони,
адвокат-партнер Адвокатського об'єднання «Лапчинський та партнери»
(м. Барселона, Королівство Іспанія)
професор кафедри кримінально-правових та
адміністративно-правових дисциплін Юридичного факультету
ПВНЗ «МЄГУ імені академіка Степана Дем'янчука»,
(м. Рівне, Україна)
кафедра кримінального процесу
Національного юридичного університету імені Ярослава Мудрого
(м. Харків, Україна)

ДРОЗДОВА Олена Валеріївна

доцентка, кандидатка юридичних наук, адвокатка,
почесна професорка кафедри кримінального права та
кримінології, міжнародного публічного права та
міжнародних відносин Юридичного факультету
Університету Барселони
(м. Барселона, Королівство Іспанія)
доцентка кафедри кримінально-правових та

ПРИВІЛЕЙОВАНІ АДВОКАТСЬКО-КЛІЄНТСЬКІ КОМУНІКАЦІЇ НА ВИЛУЧЕНИХ ЕЛЕКТРОННИХ ПРИСТРОЯХ: СТАНДАРТИ ЄСПЛ У СПРАВІ ČERNÝ AND OTHERS v. THE CZECH REPUBLIC¹ ТА УРОКИ ДЛЯ УКРАЇНИ

1. Цифровізація кримінальної юстиції змінює не лише техніку збирання доказів, а й архітектуру процесуальних гарантій. Смартфон, планшет чи хмарний акаунт підозрюваного концентрує «повний профіль» його приватного життя і професійних зв'язків. Коли такий носій вилучається, органи досудового розслідування фактично отримують потенціал суцільного доступу до змісту комунікацій, у тому числі до листування з адвокатом, проектів процесуальних документів та нотаток щодо стратегії захисту.

У справі Černý та інші проти Чеської Республіки Європейський суд з прав людини (ЄСПЛ, Суд) визнав, що включення таких матеріалів до судового «case file» і їх розкриття прокурору та співобвинуваченим становить втручання у право на повагу до приватного життя і кореспонденції (ст. 8), а відсутність зрозумілої та передбачуваної процедури відбору (sifting) і відокремлення привілейованих даних робить таке втручання не «згідним із законом».

Паралельно Суд встановив порушення статті 13 у поєднанні зі статтею 8 Європейської конвенції з прав людини (Конвенція) через відсутність ефективного засобу юридичного захисту, який дозволяв би адвокатам домагатися вилучення привілейованих даних з матеріалів справи клієнта. Отже це рішення задає стандарт: компенсаційний шлях, який не здатний зупинити поширення та подальше використання привілейованих матеріалів, не є належною відповіддю держави.

¹ <https://hudoc.echr.coe.int/fre?i=001-247564/>

Окрема думка (збіжна) судді Serghides додає до справи ще один вимір — конституційний процес і змагальність. Суддя погодився з висновком про порушення статті 6 § 1 Конвенції, але критично оцінив підхід більшості, яка теоретично допускає ненадсилання подань третіх осіб за наявності «дуже вагомих причин». На його думку, змагальність і рівність сторін є структурними, «категоричними» гарантіями, що не підлягають балансуванню.

Для України, яка одночасно розвиває е-правосуддя і вибудовує цифрові інструменти доказування, цей кейс має безпосередню прогностичну цінність. Поєднання масового вилучення електронних носіїв, використання експертів для «суцільного» витягання даних і недостатньо формалізованих процедур захисту адвокатської таємниці створює ризик системних порушень статей 8 і 13 Конвенції, а також підвищує вразливість конституційних процедур до дефіциту змагальності.

2. ЄСПЛ послідовно підкреслює «спеціальний» характер захисту комунікацій між адвокатом і клієнтом у межах статті 8 Конвенції. У справах щодо перехоплення, моніторингу або доступу до таких комунікацій Суд вимагає особливої якості закону та процедурних запобіжників від свавілля, включно з механізмами ізоляції та незалежного контролю.²

У цифрових контекстах ця лінія була розвинена у справах *Saber v Norway* та *Särgava v Estonia*, де Суд звернув увагу на необхідність передбачуваної процедури огляду електронних носіїв із метою відбору доказів і відокремлення привілейованих матеріалів, а також на потребу не допустити доступу слідства до потенційно привілейованого масиву до вирішення спору судом.³

Справу *Černý* логічно розмістити в цьому ряду, але її специфіка — джерело даних. Привілейовані документи були вилучені не з пристроїв адвоката, а з пристроїв клієнта. Саме це породило внутрішню суперечність національної практики: частина органів виходила з того, що «привілей

² *Michaud v France* (App no 12323/11) Judgment, 6 December 2012, para 118; *Sommer v Germany* (App no 73607/13) Judgment, 27 April 2017, para 56.

³ *Saber v Norway* (App no 459/18) Judgment, 17 December 2020, paras 48–55; *Särgava v Estonia* (App no 698/19) Judgment, 16 November 2021, paras 99–107.

належить клієнту», а тому адвокати не мають процесуальної легітимації вимагати вилучення матеріалів; інші — визнавали незаконність доступу та розкриття листування незалежно від того, на чісму пристрої воно зберігалось.

У теорії та практиці цифрових обшуків дедалі більше уваги приділяється моделям «фільтрації» даних (filtering/sifting), де центральним є питання: хто і як має здійснювати первинний перегляд, щоб держава не отримала «передчасний» доступ до захищеного спілкування. Порівняльно-правова література наголошує, що традиційні інструменти обшуку, сформовані для матеріальних об'єктів, погано масштабуються на цифрові масиви, оскільки цифрові носії вимагають копіювання і подальшого аналізу поза місцем вилучення.⁴

Невирішеною залишається й процесуальна частина: яким має бути ефективний засіб захисту, коли порушення вже відбулося через розкриття листування іншим учасникам провадження. ЄСПЛ прямо вказує, що необхідний засіб має дозволяти домогтися вилучення або знищення матеріалу, а не лише компенсації. Проте на національному рівні такі «матеріальні» засоби часто відсутні або доступні лише клієнту, а не адвокату.⁵

Окремий невирішений сегмент — стандарти змагальності у конституційному провадженні, коли третя особа (наприклад, професійна асоціація) прагне втрутитися, а суд розглядає її подання без комунікації сторонам. У справі Černý ЄСПЛ встановив порушення статті 6 § 1 саме через ненадсилання заявникам клопотання ЧАП про допуск до участі; суддя Serghides натомість пропонує більш жорстку, «нульову толерантність» до ненадсилання таких подань.⁶

4 Orin S Kerr, 'Searches and Seizures in a Digital World' (2005) 119 Harvard Law Review 531.

5 Černý (n 1) para 47; Pruteanu v Romania (App no 30181/05) Judgment, 3 February 2015, paras 55–56.

6 Černý (n 1) paras 92–101; Serghides Opinion (n 4) paras 7–14; Janáček v the Czech Republic (App no 9634/17) Judgment, 2 February 2023, para 53.

Отже, для українського правопорядку невирішеними залишаються: (1) формалізація процедури відокремлення привілейованих даних на вилучених носіях клієнта; (2) процесуальна легітимація адвоката на звернення з вимогою вилучення, видалення; (3) «швидкий» та ефективний засіб захисту, який відновлює конфіденційність до завершення провадження; (4) мінімальні стандарти змагальності щодо подань третіх осіб у конституційному процесі.

3. Фактична матриця та ключові висновки ЄСПЛ: від «суцільного витягання» до розкриття стратегії захисту

Факти справи є типовими для цифрової епохи. Під час обшуку в помешканні підозрюваного Z. поліція вилучила смартфон і планшет, що містили, серед іншого, листування з адвокатами, проекти подань до суду, нотатки щодо правової стратегії та інші матеріали, охоплені legal professional privilege. Суд залучив експертну установу з завданням вилучити всі дані, включно з видаленими, та будь-які комунікації з/до застосунків. У результаті було сформовано масив понад 20 000 сторінок, який включили до матеріалів справи і передали прокурору та співобвинуваченим.⁷

Суддя-головуючий публічно заявив, що приватність або адвокатське листування «взагалі не має значення», оскільки йдеться про доказ і «електронного перехоплення» не було. Цей аргумент демонструє типову помилку: зведення цифрового вилучення до «нейтрального» отримання доказів, без урахування якісної відмінності між перехопленням і форензичним витяганням даних. ЄСПЛ, навпаки, підкреслив, що спеціальний захист адвокатсько-клієнтських комунікацій був би позбавлений змісту, якби не поширювався на електронні дані, збережені як на пристроях адвоката, так і на пристроях клієнта.⁸

Ключова правова кваліфікація Суду: втручання у ст. 8 було, але воно не відповідало критерію «згідно із законом», оскільки національна правова база не

⁷ Černý (n 1) paras 6–10.

⁸ Černý (n 1) para 11; paras 61–62.

забезпечувала передбачуваності, чіткості та процесуальних гарантій для захисту привілейованих даних на вилучених електронних носіях. Національні органи самі визнавали законодавчу прогалину; суди доходили протилежних висновків щодо можливості застосування за аналогією норм, які забороняють долучення перехоплених адвокатсько-клієнтських комунікацій. За цих умов не було визначено ані заборони доступу, ані процедури відбору і відокремлення матеріалів.⁹

Важливо, що Суд не зупинився на «вузькій» процесуальній помилці, а ідентифікував системну проблему: відсутність процедури, яка гарантує, що привілейовані матеріали не стануть доступними стороні обвинувачення до того, як суди проведуть конкретний і детальний аналіз спору. Така процедура, за логікою ЄСПЛ, є елементом якості «закона» у розумінні статті 8.¹⁰

Нарешті, Суд вказав на індивідуальні заходи за статтею 46: вилучення привілейованих матеріалів з кримінальної справи клієнта заявників, а також загальні заходи — приведення правової бази у відповідність до принципів рішення. Це — прямий сигнал, що проблема не вичерпується компенсацією або вибаченням, а вимагає інституційної перебудови процедур цифрового вилучення.¹¹

4. «Згідно із законом» у цифровому обшуку: якість норми та процедурні запобіжники як єдиний тест

У доктрині статті 8 критерій «згідно із законом» традиційно включає три компоненти: наявність правової підстави, доступність і передбачуваність норми, а також сумісність із принципом верховенства права, що передбачає достатні гарантії від свавілля. У справах, пов'язаних із доступом до приватних комунікацій, акцент зміщується від «формальної» наявності норми до її операційної придатності: чи описує право процедуру так, щоб обмежити дискрецію органів та забезпечити контрольованість втручання.¹²

⁹ Černý (n 1) paras 14, 65–73.

¹⁰ Černý (n 1) para 69; Särgava (n 7) para 107.

¹¹ Černý (n 1) paras 108–110.

¹² Kopp v Switzerland (App no 23224/94) Judgment, 25 March 1998, para 55; Big Brother Watch and Others v United Kingdom [GC] (Apps nos 58170/13 and 2 others) Judgment, 25 May 2021, para 332.

Рішення у справі Černý показує, що для цифрових носіїв самі загальні норми про вилучення речей або документів або про експертні дослідження є недостатніми. Потрібна спеціальна «фільтраційна» процедура, яка вирішує принаймні чотири задачі: (1) ідентифікація потенційно привілейованого контенту; (2) ізоляція (герметизація) цього масиву; (3) незалежний (судовий) розгляд заперечень; (4) відновлення статус-кво шляхом видалення або повернення.¹³

На практиці це означає, що орган досудового розслідування не може бути єдиним суб'єктом, який первинно переглядає весь масив даних. Після фізичного вилучення має відбутися «юридичне вилучення» — відокремлення релевантного для провадження від захищеного. У цифровому середовищі ця межа не збігається з межами файлів чи папок: привілейовані фрагменти можуть міститися в чатах, вкладеннях, метаданих, резервних копіях. Отже, вимоги до процедури мають бути технологічно нейтральними (не прив'язаними до конкретного застосунку), але достатньо конкретними щодо ролей і меж доступу.

Для України це ключовий орієнтир на майбутнє: будь-яке розширення режиму електронних доказів, електронного суду та форензичного аналізу має супроводжуватися розвитком «процесуальної інженерії» — правил герметизації, хешування, журналювання доступу, а також судового контролю за фільтрацією. Інакше цифрові інструменти працюватимуть проти прав на захист і приватність.

5. Ефективний засіб захисту (ст. 13 + ст. 8): від компенсації до вилучення даних з матеріалів провадження

Стаття 13 Конвенції не гарантує певного «універсального» засобу; вона вимагає ефективності у світлі характеру порушення. Коли йдеться про незаконне включення привілейованих матеріалів до процесуальної справи, ефективний засіб має бути здатним: (а) забезпечити перегляд законності втручання; (б) призвести до вилучення або знищення матеріалів, якщо

¹³ Černý (n 1) paras 69–72.

втручання визнано незаконним. ЄСПЛ прямо сформулював цю вимогу в *Černý*, спираючись на попередню практику.¹⁴

Чеська модель, яка де-факто зводилася до можливості вимагати вибачення або компенсацію, не відповідала цьому стандарту, оскільки матеріали продовжували перебувати у справі, а отже — залишалися потенційно доступними. Суд окремо наголосив, що навіть визнання незаконності національним цивільним судом не позбавляло заявників статусу жертв, бо не відновлювало конфіденційність.¹⁵

Проектуючи цей підхід на український кримінальний процес, доцільно розрізняти два рівні засобів: «превентивний» (*ex ante*) — який запобігає доступу до привілейованих матеріалів до вирішення спору, і «відновлювальний» (*ex post*) — який забезпечує негайне вилучення/видалення у разі порушення. Компенсація або дисциплінарний механізм не замінюють жодного з цих рівнів, а лише доповнюють їх як вторинні реакції держави.

6. Змагальність у конституційному провадженні: позиція ЄСПЛ та «нормативний» підхід судді Serghides

За статтею 6 § 1 Конвенції право на змагальне провадження означає можливість сторін знати та коментувати всі докази або зауваження, подані з метою вплинути на рішення суду. ЄСПЛ визнає, що в окремих обставинах ненадсилання документа може не підірвати справедливість, але підкреслює: для ненадсилання зауважень, прийнятих і долучених до матеріалів справи, необхідні «дуже вагомі підстави». У *Černý* Суд дійшов висновку, що таких підстав не було, і встановив порушення.¹⁶

Суддя Serghides погодився з констатацією порушення, але посилив стандарт: на його думку, ненадсилання подань, релевантних для справи, є порушенням «*per se*» — незалежно від того, чи завдало воно шкоди, чи вплинуло на результат і чи було виправдане міркуваннями процесуальної

¹⁴ *Černý* (n 1) para 47; *Segerstedt-Wiberg and Others v Sweden* (App no 62332/00) Judgment, 6 June 2006, para 121.

¹⁵ *Černý* (n 1) paras 48, 54.

¹⁶ *Černý* (n 1) paras 93–100; *Vorotnikova v Latvia* (App no 68188/13) Judgment, 4 February 2021, paras 21–22; *Janáček* (n 10) para 53.

економії. Він прямо заперечує можливість балансування структурних гарантій змагальності та рівності сторін.¹⁷

З практичної точки зору для майбутніх змін в Україні ця дискусія має два наслідки. По-перше, під час реформування процедур Верховного Суду, Конституційного Суду України та суміжних проваджень доцільно закласти презумпцію комунікації: будь-яке подання третьої особи, яке суд приймає до розгляду або враховує, має бути надіслане сторонам із розумним строком для відповіді. По-друге, навіть у цифрових кримінальних процедурах концепція «структурних гарантій» підказує, що деякі запобіжники (зокрема, заборона доступу сторони обвинувачення до потенційно привілейованого масиву до судового вирішення спору) не повинні «балансуватися» з міркуваннями ефективності розслідування, а мають діяти як тверді правила.

7. Уроки для України: модель «життєвого циклу» привілейованих цифрових даних та законодавчі орієнтири

На основі рішення ЄСПЛ доцільно описати «життєвий цикл» привілейованих цифрових даних у кримінальному процесі як послідовність етапів, для кожного з яких мають існувати процесуальні гарантії: (1) виявлення потенційно привілейованого контенту; (2) ізоляція і збереження цілісності (sealed copy, хеш-суми, журнал доступу); (3) судовий контроль та вирішення спору (у тому числі з участю адвоката і клієнта); (4) видалення, повернення або долучення лише неприхованої частини; (5) аудит виконання і відповідальність за порушення.

У чинному українському КПК обшуки, тимчасові доступи до речей і документів та їх вилучення не формують повного «цифрового» режиму, який би прямо описував відбір даних із пристроїв і механізм фільтрації привілейованих комунікацій у ситуації, коли носій належить клієнту, а не адвокату. Наявні гарантії щодо адвокатської таємниці (у профільному законі) не завжди мають процесуальне продовження у формі ефективної процедури вилучення/видалення даних із матеріалів провадження. Саме ця лакуна в

¹⁷ Serghides Opinion (n 4) paras 5, 7–12.

майбутньому може стати джерелом конвенційних порушень, аналогічних до Černý.

З огляду на це пропонується закріпити в КПК України спеціальний інститут «фільтрації цифрових даних», який включатиме такі елементи:

- обов'язок прокурора, слідчого створити форензичну копію носія та негайно герметизувати оригінал і копію, визначивши коло осіб, які мають доступ до копії, та заборонивши аналіз привілейованих даних до судового рішення;

- процедуру первинного сортування (sifting) під контролем слідчого судді або за участі незалежного «фільтраційного» суб'єкта (наприклад, уповноваженого судом експерта, який працює за затвердженим протоколом і не розкриває зміст привілею стороні обвинувачення);

- процесуальну легітимацію адвоката і клієнта на подання клопотання про вилучення, видалення привілейованих даних, включно з правом на терміновий розгляд та апеляційний перегляд;

- правило «ексклюзиву до вирішення спору»: прокурор і слідчий не отримують доступу до потенційно привілейованого масиву до моменту, коли суд відсортує матеріали або визначить критерії їх використання;

- обов'язковість документування всіх операцій із цифровими доказами (хеш-суми, лог-файли), а також відповідальність за порушення режиму герметизації та розкриття адвокатської таємниці.

Додатково потрібен «матеріальний» засіб захисту, який відповідає вимогам статті 13: процедура, що дозволяє домогтися саме вилучення, знищення привілейованих даних з матеріалів провадження, а не лише констатації незаконності. Такий засіб має бути доступним не лише підозрюваному, але й адвокату, оскільки порушення конфіденційності підриває професійну функцію захисту і довіру до правосуддя.¹⁸

На рівні правозастосування важливо закласти практику «мінімізації» доступу (data minimisation): вилучення має бути цільовим, а завдання експерту

¹⁸ Černý (n 1) paras 47, 79–84; Michaud (n 6) para 118.

— обмеженим релевантністю до предмета доказування. Суцільна екстракція «всього, включно з видаленим» повинна розглядатися як виняток, який потребує посиленої судової мотивації та додаткових запобіжників.¹⁹

8. Висновки та значення

1) Запропоновано модель «життєвого циклу» привілейованих цифрових даних, яка поєднує критерій якості закону (ст. 8) з вимогами до засобу юридичного захисту (ст. 13) і трансформує їх у конкретні процесуальні кроки (виявлення – ізоляція – судовий контроль – видалення – аудит).

2) Теоретичне значення: рішення Černý демонструє, що в цифрову епоху «процедура» стає частиною самого поняття «закон». Для правової системи це означає зміщення фокуса від декларативних гарантій адвокатської таємниці до операційних протоколів роботи з даними. Окрема думка судді Serghides, у свою чергу, вказує на межі доктрини «загальної справедливості» та пропонує розглядати змагальність як категоричну умову легітимності рішення.²⁰

3) Практичне значення: запропоновані орієнтири можуть бути використані при підготовці змін до КПК України щодо цифрових доказів, при розробленні інструкцій для експертних установ та органів досудового розслідування, а також у практиці слідчих суддів під час санкціонування обшуків і визначення меж форензичного аналізу. Їх імплементація має перспективу зменшити ризик витоків стратегії захисту, підвищити довіру до процесу і забезпечити відповідність майбутніх цифрових реформ стандартам Конвенції.

4) Прогноз на майбутнє: розвиток хмарних сервісів, месенджерів із наскрізним шифруванням та інструментів штучного інтелекту для аналізу даних посилюватиме спокусу «масових» цифрових вилучень. Саме тому українське законодавство має випереджально закріпити фільтраційні процедури та «жорсткі» правила недоступності привілейованого масиву для сторони обвинувачення до судового вирішення спору; інакше цифрова ефективність

¹⁹ Černý (n 1) para 7 (формулювання завдання експерту) та para 70 (вимога ясності і гарантій).
²⁰ Černý (n 1) paras 69–73; Serghides Opinion (n 4) paras 10–14.

розслідування може перетворитися на хронічне джерело конвенційних порушень.

З Богом!