DOI: 10.31359/2079-6242-2024-47-30
УДК 343.1(477):347.991

Н. В. Глинська, доктор юридичних наук, старший науковий співробітник**,** завідувачка відділу дослідження проблем кримінального процесу та судоустрою Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса Національної Академії правових наук України
ORCID ID 0000-0001-5835-3798

Д. І. Клепка, кандидат юридичних наук, старший науковий співробітник відділу дослідження проблем кримінального процесу та судоустрою Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса Національної Академії правових наук України
ORCID ID 0000-0001-8423-4581

ПРИНЦИПИ ВИЗНАЧЕННЯ РОЗУМНИХ МЕЖ ЦИФРОВІЗАЦІЇ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ УКРАЇНИ

Постановка проблеми. Всебічна інформатизація та діджиталізація суспільства є вже неминучим процесом, який цілком закономірно «зачепив» й кримінальне судочинство, яке «піддається перманентній зміні й реформуванню, перебуває в пошуку оптимального балансу інтересів держави, суспільства та окремих учасників кримінального процесу, прагне йти в ногу з науково-технічним прогресом»[1]. На сьогодні у більшості країн світу, зокрема у країнах європейського простору, активно триває процес діджиталізації сфери правосуддя, що супроводжується постійним пошуком оптимальних цифрових інструментів та моделі нормативного правового регулювання суспільних відносин, що виникають у зв'язку з переходом до цифрових технологій.

У Повідомленні про цифровізацію правосуддя в Європейському Союзі зазначається, що за останні десять років Комісія та держави-члени визнали необхідність впровадження нових технологій з метою створення більш ефективних систем правосуддя та прийняли ряд ініціатив, які привели до позитивних результатів щодо цифровізації правосуддя.[2] Крім зазначеного, аналізований документ встановив новий підхід до цифровізації правосуддя на основі «набору інструментів» – комплексного набору правових, фінансових та ІТ-інструментів, які будуть використовуватися різними учасниками системи правосуддя відповідно до їхніх потреб.[3]

[1] Луцик В В, Самарін В І, *Сучасний кримінальний процес країн Європи : монографія* (Право, 2018) 5; Мурзановська А В 'Основні тенденції розвитку науки кримінального процесу в Україні в сучасних умовах' *Legal science and education in Ukraine and EU countries: a paradigm shift: Collective monograph*. («Baltija Publishing», 2021) 285–310 <http://www.baltijapublishing.lv/omp/index.php/bp/catalog/book/159> (дата звернення: 15.04.2022)

[2] Access to justice: seizing the opportunities of digitalisation. Council Conclusions 11599/20. Council of the European Union. Brussels, 2020. URL: https://data.consilium.europa.eu/doc/document/ST-11599–2020-INIT/en/pdf (дата звернення: 15.02.2024)

[3] *Примітка.* Зокрема у повідомленні йдеться про такі інструменти: 1) фінансування в контексті багаторічної фінансової програми на 2021–2027 роки та заходів ЄС наступного покоління для просування процесу цифрової трансформації; 2) обговорення використання додатків на основі штучного інтелекту (AI) на користь систем правосуддя з урахуванням пов'язаних ризиків; 3) перетворення цифрового каналу на стандартний варіант у судовій співпраці ЄС; 4) створення кращих інструментів доступу до інформації для громадян і практиків шляхом створення та взаємозв'язку реєстрів; 5) використання доступних ІТ-інструментів для безпечної транскордонної співпраці в цивільних, комерційних і кримінальних справах; 6) оновлення та модернізація цифрових інструментів для судової співпраці та обміну інформацією у кримінальних справах у всьому ЄС, особливо тих, які є в розпорядженні агенцій та органів ЄС з питань юс-

13 жовтня 2020 року Рада ЄС прийняла програмний документ Висновки «Доступ до правосуддя: використання діджиталізаційних можливостей»[1] (далі – Висновки Ради ЄС), в якому викладено сукупність конкретних пропозицій щодо взаємного посилення політики щодо ефективного доступу до правосуддя та цифровізації. У розвиток Висновків Європейською Комісією у грудні 2020 року прийнято документ «Цифровізація правосуддя в Євросоюзі: інструментарій можливостей» (далі по тексту для корисності посилання – Інструментарій), в якому встановлено новий підхід до цифровізації правосуддя на основі «набору інструментів» – комплексного набору правових, фінансових та ІТ-інструментів, які будуть використовуватися різними учасниками наших систем правосуддя відповідно до їхніх потреб[2]. Відмічаючи вже здобуті результати діждиталізації Комісія наголосила на необхідності системних, поетапних змін, щоб побачити весь потенціал сучасних цифрових інструментів, в повній повазі основних прав.

Як вже предметно висвітлювалось у попередніх публікаціях (на попередніх сторінках) переваги цифровізації кримінального провадження (далі – ЦКП) є чисельними. Одночасно цей процес має бути виваженим та контрольованим, аби не зазіхнути на права та свободи людини, цінність, забезпечення якої та постає на чолі ЦКП. У контексті специфіки сфери правосуддя доречно виснувала Комісія при формулюванні Інструментарію діджиталізації про те, що «судова система є сектором, де, враховуючи характеристики типової діяльності, можна очікувати значних ризиків» (п. 43). Тому вкрай обережно в цій царині слід підходити до використання усіх здобутків цифровізації, зокрема й штучного інтелекту (далі – ШІ), адже всі цифрові рішення в кримінальному провадженні мають бути зважені з огляду на їх потенційний вплив на права особи.

Тому вкрай важливим є дотримання розумних меж, «кордонів» такого процесу, допустимої міри проникнення цифрових технологій у сферу правосуддя, поза якими позитивний ефект, що очікується від діджиталізаціїї правових відносин, перетвориться на зворотній – негативний, здатний породжувати небажані правові наслідки. Тут слід згадати популярний серед процесуалістів вислів Шарля-Луї де Монтеск'є – «якщо на судові формальності поглянути як на перешкоди, які ускладнюють громадянину захист своїх прав та інтересів, то можна відшукати їх надто багато. Якщо ж судові формальності розглядати з погляду їх відношення до свободи й безпеки громадян, то їх надто мало, оскільки всі ускладнення, витрати та зволікання і самі помилки правосуддя є тією ціною, яку громадянин сплачує за свободу». Цей ідеологічний посил є цілком релевантним й до виваженості усіх цифрових рішень у кримінальному провадженні.

Аналіз останніх досліджень і публікацій. Проблематика цифровізації є популярною у зарубіжній та вітчизняній економічній літературі. Що ж до кримінальної процесуальної науки, то окремі питання використання цифрових технологій під час кримінального провадження були предметом дослідження таких українських науковців, як: В. Білоус, В. Бірюков, В. Голубєв, М. Гуцалюк, О. Жученко, О. Капліна, М. Карчевський, О. Колотило, Є. Лук'янчиков, О. Метелев, Т. Михальчук, А. Молдован, Т. Павлова, Д. Патрелюк, А. Рибченко, М. Смирнов, В. Уваров, І. Хараберюш, В. Хахановський, С. Чернявський, Г. Чигрина, С. Шаренко та ін. Нечисельними є монографічні дослідження, що присвячені саме проблематиці цифровізації у царині кримінального провадження. Серед них слід вказати на праці А. Скрипника, А. Столітнього, Д. Літвекича, Д. Цехана.

Окремим напрямом наукової розвідки у сфері ЦКП є застосування відеоконференції (далі – ВКЗ) в кримінальному провадженні, у цьому сенсі не можна оминути увагою монографічне дослідження А. Бєжанової, Г. Тетерятник, Г. Мудрецької «Застосування режиму відеоконференції у кримінальному судочинстві».

Утім, попри значний науковий інтерес до впровадження цифрових технологій в царину кримінального провадження, науковці у своїх дослідженнях лише точково торкались проблематики меж такого впровадження. Здебільшого науковий інтерес викликали питання меж допустимості тех-

тиції та внутрішніх справ; 7) створення «My e-Justice space», який забезпечить громадянам і підприємствам «точку входу», що об'єднує доступні національні електронні послуги; 8) проведення регулярного моніторингу досягнутого прогресу.

[1] Access to justice: seizing the opportunities of digitalisation. Council Conclusions 11599/20. Council of the European Union. Brussels, 2020. URL: https://data.consilium.europa.eu/doc/document/ST-11599–2020-INIT/en/pdf

[2] Digitalisation of justice in the European Union: A toolbox of opportunities» European Commission. COM/2020/710 final. Brussels, 2020.. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020DC0710_(дата звернення: 15.02.2024)

нологій ШІ у кримінальному провадженні (Т. Каменєва, О. Капіліна, Д. Кісленко А. Туманянц та ін.), «рівень довіри» до електронної інформації, можливість повного переведення документообігу у кримінальному провадженні в електронний формат, забезпечення інформаційної безпеки електронного кримінального провадження, проблематика «адаптивності» нормативного механізму до збирання та фіксування цифрової інформації тощо.[1]

Утім комплексне дослідження питання меж ЦКП як багатогранного процесу ще не проводилось сучасними дослідниками. Це підкреслює доктринальний аспект актуальності поставленої проблематики.

Звісно у правовій царині, котра, як правило, не піддається суворій кількісній оцінці та градації, визначити межі, що є розумно допустимими для здійснення її цифрової модернізації, можливо лише у спосіб формулювання та аналізу основних положень принципового характеру, сукупність яких має враховуватися як визначальний регулятор тих рамок, до яких вплив цифровізації на кримінальне судочинство буде позитивним та конструктивним.

Тож ефективне здійснення процесу системної ЦКП, на відміну від точкового підходу до цього процесу, вимагає розробки позначеної сукупності положень загального характеру.

Метою статті є визначення та загальна характеристика основних положень принципового характеру, сукупність яких має бути врахована у процесі ЦКП для забезпечення його розумних меж.

Виклад основного матеріалу. Під межами ЦКП слід розуміти зумовлені низкою чинників певні «кордони» цифрового оснащення кримінальної процедури та необхідний рівень нормативної адаптації цієї царини до діджитал середовища. Фактично це про те, наскільки широка перспектива впровадження цифрових технологій в царину правосуддя та з іншого боку, рівень корекції кримінальної процесуальної форми для її адаптації (пристосування) до цифрового середовища.

Саме розумна межа є тим бар'єром, поза яким позитивне перетворюється в його антипод. Наприклад при всій корисності технології ВКЗ, дистанційний формат провадження не може бути правилом у кримінальній процедурі. Адже значний відхід від фізичних до гібридних або дистанційних слухань також може підірвати конституційний статус судового процесу, зокрема його символічний характер (Висновок КРЄС № 14 (2011), пункт 6). Участь у судочинстві з дому, в автомобілі чи в громадському місці може підірвати розуміння суспільством громадянської важливості процесу. У такий спосіб статус і легітимність судової влади на інституційному рівні як частини держави можуть бути пошкоджені. Що стосується індивідуальних проваджень, це може призвести до того, що учасники не сприйматимуть провадження настільки серйозно, як їм слід. Це може негативно вплинути на характер і якість доказів, особливо на показання свідків під присягою, що також може поставити під загрозу здатність судової системи забезпечити справедливий суд. (п. 67 ВКРЕС № 26).[2]

Звичайно у царині кримінального провадження, яка об'єктивно не може бути повністю алгоритмізованою, врахуванню ситуативності (ad hoc) належить іноді центральна роль у досягнені справедливого вирішення правового конфлікту. Тому важко окреслити чіткі «грані дозволеного», визначально встановити, під час якої процедури оцифрування чи використання цифрової інформації є допустимим, а коли ні, коли право особи буде порушено через його дистанційну участь у судовому розгляді, а коли ні та ін. Не можна також чітко позначити, наскільки кримінальна процесуальна форма як нормативний механізм ЦКП потребує модифікації у цифровому середовищі, зокрема, кількість необхідних цифрових процесуальних дій, наскільки потрібна деталізація цифрових прав учасників процесу, рівень дискретних повноважень сторони обвинувачення у цифровому досудовому розслідуванні тощо.

Тож межі ЦКП являють собою юридичні рамки застосування цифрових технологій в кримінальній процедурі, якими держава оптимізує балансування приватних та публічних інтересів, обмежує втручання у приватні інтереси особи. Пошук таких оптимальних меж ЦКП вимагає формулювання (виокремлення) та розгляд основних положень принципового характеру, сукупність яких є необ-

[1] Каменєва Т. 'Можливості та межі використання цифрових технологій в сфері кримінально-процесуальної діяльності' (2020) 8 (193) Громадська думка про правотворення 17–21 <http://nbuviap.gov.ua/images/dumka/2020/8.pdf> (дата звернення: 15.02.2024)

[2] Висновок Консультативної ради європейських суддів до уваги Комітету міністрів Ради Європи про правосуддя та інформаційні технології (ІТ) № 14 (2011) URL: https://rm.coe.int/opinion-n-14–2011-on-justice-and-information-technologies-it-/16806a1fc0 (дата звернення: 15.02.2024)

хідною для врахування в перебігу здійснення ЦКП. Такі принципи ЦКП своєю чергою є основою для формулювання похідних від них більш конкретних вимог практичного характеру – стандартів ЦКП.[1]

Переходячи до формулювання стандартів (принципів) ЦКП передусім слід наголосити на необхідність врахування при цьому положень релевантних міжнародно-правових актів. Оскільки це питання вже було предметом нашого дослідження[2] тут лише доповнимо цей аспект сформульованими у нещодавньому Висновку КРЕС № 26 від 1 грудня 2023 року «Рухаючись вперед: використання асистивних технологій у судочинстві» (далі – Висновок КРЄС № 26)[3] загальними принципами, що стосуються використання технологій в судових системах. Як зазначила КРЕС, використання технологій повинно, перш за все, поважати природу судового процесу. По-перше, багато судових рішень є дискреційними рішеннями, заснованими на конкретних фактах окремої справи. По-друге, судді відіграють суттєву роль у розвитку права. Вони не просто застосовують фіксовані та незмінні правила. Судді повинні мати можливість виправляти або доповнювати закон, якщо він не відповідає вимогам або загрожує зашкодити його застосуванню в певних справах. Технології не повинні втручатися у сферу справедливості. Технології не повинні знеохочувати або перешкоджати критичному мисленню суддів, оскільки це може призвести до стагнації правового розвитку та ерозії системи правового захисту. Тому технологічні інструменти повинні поважати процес ухвалення судових рішень і автономію суддів (п. 90).[4]

Так, у п. 91 зазначеного документа КРЄС вказала на, по-перше, обов'язкову відповідність технологій Європейській етичній хартії щодо використання штучного інтелекту в судових системах та їхньому середовищі (2018) та Керівним принципам Європейської комісії з ефективності правосуддя Ради Європи (далі – CEPEJ) щодо електронного подання документів у суд (e-filing) та цифровізації судів (2021). По-друге, сформулювала та охарактеризувала сукупність принципів, котрі мають керувати майбутнім дизайнуванням, впровадженням і використанням технологій для підтримки суддів. Головна мета цих принципів полягає в кращому забезпеченні ефективного та практичного доступу до правосуддя, що відповідає незалежності судової влади та верховенству права. Вони призначені для підтримки та посилення судової легітимності та впевненості в судовій владі. Ці принципи є такими: (i) Верховенство права; (ii) Незалежність і неупередженість судової влади: (iii) Судова автономія;(iv) Судовий нагляд; (v) Доступність і якість; (vi) Сумісність і безперервне вдосконалення; (vii) Пілотування; (viii) Недискримінаційний дизайн і функціонування; (ix) Прозорість і зрозумілість: (x) Підзвітність; (xi) Цілісність, безпека та захист даних; (xii) Відкритість і конфіденційність: (xiii) Фінансування: (xiv) Навчання та експлуатаційна здатність.

Тож крізь призму викладеного перейдемо безпосередньо до визначення принципів (стандартів) ЦКП.

---

[1] *Примітка.* З огляду на тісний зв'язок між категоріями «принцип» (як основне, найзагальніше, вихідне положення, засіб, правило, яке визначає природу та соціальну сутність явища, його спрямованість і найсуттєвіші властивості) і «стандарт» (як взірець, еталон, модель, що беруться як вихідні для зіставлення з ними інших подібних об'єктів) ми, допускаючи певну їх синонімічність як керівних векторів будь-якої правової діяльності, звичайно не дорівнюємо їх зміст. Як влучно у контексті співвідношення зазначених термінів відмічено в правовій літературі «…принцип може стати стандартом у тому разі, коли він визначається через чітку систему вимог, які закріплюються у праві. Можна навіть сказати, що стандарти – це принципи, які досягли стану найвищої регламентованості, закріпленості й обов'язковості, що говорить про їх зникнення, недійсність або перетворення на нові стандарти у разі мінімальної зміни. Водночас принцип може існувати в неписаній формі, стандарт же повинен мати джерело свого закріплення. Цим обумовлюється те, що стандарт є не філософською, а загалом юридичною й технічною категорією. Слід також відзначити, що стандарти формуються поступово, доводячи свою «життєздатність» у процесі правозастосування. Вони, як правило, становлять узагальнення накопиченої практики, у зв'язку з чим у міжнародному праві їх називають правовими позиціями певного суду. Разом з цим стандарти є меншими за обсягом, ніж принципи. На нашу думку, один принцип може породжувати кілька стандартів. Наприклад, принцип справедливості у кримінальному процесі містить такі стандарти, як побачення з адвокатом до першого допиту, зрозуміла мова процесу та ін. (Прийма С. В. 'Поняття принципу в аспекті співвідношення з суміжними категоріями' (2014) 28 Державне будівництво та місцеве самоврядування 46–55 <http://nbuv.gov.ua/UJRN/dbms_2014_28_7>)

[2] Глинська Н. В., Дроздов О. М., 'Євроінтеграційний вектор цифровізації кримінального провадження: виклики та шляхи реалізації' *Перспективні напрями розвитку кримінальної юстиції в цифрову еру* : матеріали Всеукр. заоч. наук.-практ. конф. (м. Харків, 24 лип. 2023 р.) 104–117. <https://ivpz.kh.ua/wp-content/uploads/2023/10/Збірник-тез_Перспективні-напрями_2023.pdf> (дата звернення: 15.02.2024)

[3] Висновок Консультативної ради європейських судів: Рухаючись вперед: використання асистивних технологій у судочинстві № 26 (Страсбург, 1 грудня 2023 року). URL: https://hcj.gov.ua/page/vysnovky-kryes

[4] Висновок № 26 (2023) Консультативної ради європейських судів: Рухаючись вперед: використання асистивних технологій у судочинстві (Страсбург, 1 грудня 2023 року). URL: https://hcj.gov.ua/page/vysnovky-kryes (дата звернення: 15.02.2024)

1. Ключовим стрижневим принципом ЦКП звичайно є засада *верховенство права*, серед основних аспектів котрої у царині кримінального судочинства особливого значення набуває пріоритетність прав та свобод людини при просуванні на будь-якому напряму ЦКП[1]. Адже ч. 1 ст. 8 КПК визначає, що кримінальне провадження здійснюється з додержанням принципу верховенства права, відповідно до якого людина, її права та свободи визнаються найвищими цінностями та визначають зміст і спрямованість діяльності держави. Це положення корелює зі ст. 3 Конституції України, за якою права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави.[2]

Інакше кажучи, формула ЦКП має корелювати із забезпеченням прав та свобод особи в цій царині. Відповідно гарантованість прав та свобод особи під час кримінальної процедури є основним вектором прийняття цифрових рішень. При цьому недопустимим є будь-яке звуження прав учасників кримінального провадження. Адже побудова сучасного кримінального процесу має сенс тільки тоді, коли його осучаснення не тягне за собою звуження прав суб'єктів кримінального провадження. Принцип недопустимості звуження прав людини є конституційним, та таким, що ґрунтовно досліджений у науці конституційного права[3], а тож не потребує галузевого тлумачення.

«Будь-яка дія, пов'язана з цифровізацією правосуддя, повинна виконуватися в повній відповідності до фундаментальних прав, таких як права на захист персональних даних, на справедливий суд і на ефективний засіб правового захисту, а також принципів пропорційності та субсидіарності….Має бути гарантовано право на справедливий суд та ефективний засіб правового захисту. Зокрема, у кримінальному провадженні в цифровому середовищі слід уникати будь-якого втручання в права на захист, включаючи право на доступ до адвоката та право на доступ до речових доказів» (п. 4 Інструментарію). Для цього «використання технологій має відповідати праву на справедливий судовий розгляд, що застосовується до судових проваджень, як це передбачено статтею 6 Європейської конвенції прав людини (далі – ЄКПЛ), а також має відповідати праву на приватність і захист даних, передбаченому статтею 8 ЄКПЛ, і праву на свободу вираження поглядів для громадськості, включаючи ЗМІ, передбаченому статтею 10 ЄКПЛ. У зв'язку з особливим ризиком того, що використання технології може бути упередженим або частковим у її застосуванні чи наслідках, використання технології має особливо враховувати необхідність гарантувати ці права відповідно до принципу недискримінації (п. 82 ВКРЕС № 26).[4] При цьому КРЄС визнала, що Європейський суд з прав людини (далі – ЄСПЛ) розвинув і продовжуватиме розвивати свою практику у світлі технологічного розвитку. Наприклад, фізична відсутність на слуханні колись розглядалася як порушення статті 6 ЄКПЛ. За певних умов і з розвитком ефективних засобів відеоконференцій зараз визнається, що участь у судовому засіданні за допомогою таких засобів еквівалентна фізичній присутності, а отже, не суперечить статті 6. (п. 83)

По суті всі наступні принципи ЦКП є похідними чи продиктованими засадою верховенство права як нормою-вимогою найвищого рівня. При цьому вважаємо за доцільне виокремити як самостійний принцип таку невід'ємну компоненту верховенства права як *правова визначеність*.

2. Стандарт *правової визначеності* є одним з основних сучасних стандартів якості закону. Так, за усталеною практикою ЄСПЛ поняття «передбачено законом» або «згідно із законом» у положеннях Конвенції вимагають не лише того, щоб заходи компетентних органів держави мали правове підґрунтя в джерелах національного права, але й вимагають достатню якість норм права, що передбачає наявність у них гарантій проти свавілля, а також їх відповідність принципу верховенства права («Санді Таймс» проти Сполученого Коро-

[1] *Примітка.* Засада верховенства права знайшла закріплення як у низці міжнародних нормативно-правових актів (у преамбулі КЗПЛ; преамбулі та ст. 3 Статуту Ради Європи тощо), так і на національному рівні (ст. 8, ст. 129 Конституції України, ст. 8 КАСУ, ст. 2, ч. 1 ст. 6 ЗУ «Про судоустрій і статус суддів», ст. 5 ЗУ»Про безоплатну правову допомогу», . ст. 3 Закону України «Про правотворчу діяльність» від 24 серпня 2023 р. № 3354-IX (який хоча і не набрав чинності, але закріплені у ньому правила мають розглядатися як орієнтир для розв'язання питань правотворчості) та ін.)

[2] Капліної О. В., Шило О. Г. (ред) *Кримінальний процес : підручник* (Право, 2019) 66.

[3] Шило О. Г. (ред) *Концептуальні основи побудови сучасного кримінального процесу України* (НДІ ВПЗ імені акад. В. В. Сташиса НАПрНУ, 2016) 64–65

[4] Висновок Консультативної ради європейських судів: Рухаючись вперед: використання асистивних технологій у судочинстві № 26 (Страсбург, 1 грудня 2023 року). URL: https://hcj.gov.ua/page/vysnovky-kryes (дата звернення: 17.09.2023)

лівства, заява № 6538/74, 26 квітня 1979 року, п. 49)[1]. Зазначене насамперед обумовлює необхідність запроваджувати та будувати норми права таким чином, щоб вони були доступними відповідним особам. А їх формулювання було б настільки чіткими, щоб дозволити особам передбачити, в розумних межах у світлі особливостей конкретних обставин, наслідки, які можуть настати внаслідок тієї або іншої дії цих осіб («Маестрі проти Італії», заява № 39748/98, 17 лютого 2004 року)[2].

Неодмінна затребуваність правової визначеності нормативної основи ЦКП (чіткість, ясність та зрозумілість правових норм) є очевидною з огляду на потенційні ризики безконтрольного застосування цифрових технологій для прав та свобод людини. Звичайно це питання потребує самостійного дослідження при розробці чи оцінці нормативних цифрових рішень. Тут лише позначимо окремі напрями, які на наш погляд потребують подальшого чіткого унормування в кримінальному процесуальному законі на шляху до ЦКП: механізм електронного документообігу; спрощення кримінальної процесуальної форми внаслідок усунення «зайвого» дублювання фіксації процесуальної інформації; формат дистанційного провадження; специфіка збирання та оцінки цифрових доказів; розширення цифрових прав учасників провадження; технологія «цифрового» міжнародного співробітництва та багато інших аспектів.

3. Наступним принциповим положенням, що впливає на масштабність процесу ЦКП та якісну цифрову трансформацію царини правосуддя є *пріоритетність цифрового формату* в кримінальній процедурі *(«цифровий за замовчуванням»)*. Зазначений принцип здебільшого стосується документообігу та передбачає максимально допустиме впровадженням режиму Paperless чи пріоритетність цифрового формату кримінальних процесуальних документів.

Як вже неодноразово зазначалось, одним з основних очікуємих позитивних ефектів ЦКП є значна економія ресурсів органів кримінальної юстиції, полегшення доступу до правосуддя у спосіб значного спрощення процесуальної форми. Однак якщо насичувати кримінальний процес цифровими елементами як альтернативами традиційним, сама суть процесу ЦКП нівелюється, оскільки неконтрольоване дискретне обрання суб'єктами провадження зручного для нього способу реалізації своїх прав чи обов'язків (іноді з огляду на суб'єктивні протистояння новому, закоренілість та небажання розвиватись тощо) лише внесе плутанину й невизначеність у право реалізаційний процес та не сприятиме досягненню необхідного результату. Саме тому лише форсована законодавцем пріоритетність є необхідною вимогою для цифрової трансформації суспільства. Інакше кажучи, цифрові механізми в кримінальному провадженні мають бути «не варіантами, а в пріоритеті». Попереджуючи можливий аргумент скептиків щодо «цифрової неготовності» суспільства наведемо декілька тез Л. М. Лобойко, сформульованих науковцем ще у 2016 році у контексті трансформації кримінального процесу з радянського в сучасний: «Будь-який законопроєкт (чи проєкт КПК, чи проєкт окремих змін до нього) передбачає врегулювання відносин наперед. Він має бути спрямований у майбутнє, а не закріплювати «радянські» процесуальні традиції….Закон повинен містити нормативні моделі майбутніх правових відносин, часто випереджаючи при цьому чинний рівень розвитку суспільних відносин. Це, звичайно, не завжди сприяє його ефективності, дієвості в силу об'єктивного відставання правової свідомості суб'єктів, їх консерватизму чи інертності мислення. До зазначених причин можна додати ще й побоювання учених виглядати не послідовними у своїх поглядах на ті чи інші питання правового регулювання у кримінальному провадженні. Ці причини стоять на заваді закріпленню у законопроєктах дійсно прогресивних, таких, що відповідають європейським стандартам, нормативних положень. Змінити «процесуальний менталітет» українців можна, але треба це робити шляхом зміни правил процесуальної діяльності. «Нові правила змінять менталітет». Менталітет не можна змінити протягом декількох місяців чи, навіть, років. Але ж починати це робити колись треба. Не можна ж заперечувати, що за двадцять років незалежності й здійснюваної в Україні судово-правової

[1] Справа «Санді Таймс» (The Sunday Times) проти Сполученого Королівства» (Заява № 6538/74) : Рішення Європейського суду з прав людини від 26 квіт. 1979 р. URL: http://hudoc.echr.coe.int/rus?i=001–57584 (дата звернення: 17.09.2023)

[2] Справа «Маестрі проти Італії» (Заява № 39748/98) : Рішення Європейського суду з прав людини від 17 лют. 2004 р. URL: http://hudoc.echr.coe.int/rus?i=001–61638 57584 (дата звернення: 17.09.2023)

реформи менталітет українців залишився на рівні радянського»[1].

Як зазначається у Рекомендації Європейської Комісії з ефективності правосуддя щодо електронного подання документів до суду (е-подання) та оцифрування їх судом від 9 грудня 2021[2], «цифровий за замовчуванням» – це принцип, який має як організаційні, так і технічні виміри та стратегічне значення, і його слід реалізовувати як такий. Загалом це означає надання державних послуг цифровими засобами як кращий варіант для людей, тобто цифрові послуги, є настільки простими та зручними, що всі, хто може ними користуватися, вирішать це робити, тоді як ті, хто не може або не бажає не виключаються.

Більш докладно зазначений принцип буде розглянутий далі. Тут позначимо, що надання пріоритету цифровій формі здійснення кримінальної процесуальної діяльності є важливим стримувачем хаотичності та надмірної дискретності при обранні форми документування в кримінальному провадженні (цифрової чи письмової) стороною обвинувачення та судом. З іншого боку, цифровий за замовчуванням формат реалізації прав учасників процесу (зокрема, у контексті процесуальної комунікації з посадовими особами, що ведуть процес) сприятиме впорядкуванню та спрощенню процесуальної взаємодії, запобігати випадкам зволікань з реагуванням на звернення таких учасників. Відповідно така пріоритетність має бути унормована в законі. З урахуванням специфіки структурної побудови КПК України видається доцільним формулювання положення щодо пріоритетності цифрової форми кримінального провадження як окремого засадничого положення в Главі 2 КПК (засади кримінального провадження).

Водночас позначимо й те, що хоча переведення роботи системи органів державної влади, зокрема, системи правоохоронних органів та суду, у режим PaperLess, тобто повної відмови від паперових документів є аджентою розвитку нашої держави, запорукою інтеграції нашої країни до світових економічних та інформаційних процесів, з урахуванням об'єктивних (відсутність *технологічних та нормативних* умов для повноцінного функціонування єдиної інформаційно-аналітичної системи як інструменту взаємодії між всіма органами кримінальної юстиції, стадійність при переході на електронний документообіг) та суб'єктивних (суспільну інерцію як перепону для інтенсифікації переходу до формату PaperLess*)* чинників на сучасному етапі розвитку суспільства доцільним є лише гібридний формат документообігу в межах кримінального провадження. Мова йде фактично про необхідність гнучкого підходу до процесу ЦКП, що обумовлює визначення наступного однойменного принципу ЦКП.

4. *Гнучкість процесу ЦКП* передбачає неформальний підхід до реалізації цього процесу як на законодавчому, так і правозастосовному рівні.

Суть гнучкого підходу до унормування питань ЦКП вбачається у двох аспектах : змістовному та юридико-технічному.

Змістовний аспект гнучкого підходу до ЦКП передбачає унормування альтернатив цифровим процедурам та можливість звернення до паперового формату документообігу (за формулою – пріоритет за цифровим, втім – за наявності підстав – альтернативні процедури та доступні засоби документування); можливість повертатись до традиційних процедур у перебігу здійснення процесуальної діяльності у разі, якщо виникли для цього підстави (гнучко реагувати на потреби).

Духом гнучкого підходу до використання цифрових технологій в правосудді пронизаний вже згадуваний Висновок КРЕС № 26. Так, зокрема, вказуючи на те, що законодавство також має передбачати дедалі більший перехід судових органів до використання технологій, КРЕС наголошує на необхідність передбачити підтримку, *альтернативних нетехнологічних засобів доступу до судових органів і правових процедур* для тих, хто не може отримати доступ або ефективно використовувати технології (п. 86). Особливо важливо передбачити продовження слухань, не пов'язаних із застосуванням технологій. Хоча аудіо- та/або відеоконференції можуть бути доцільними для деяких слухань, вони не обов'язково будуть доречними для тривалих слухань, зокрема таких, які,

[1] Шило О. Г. (ред) *Концептуальні основи побудови сучасного кримінального процесу України* (НДІ ВПЗ імені акад. В. В. Сташиса НАПрНУ, 2016) 83–85

[2] Рекомендації Європейської Комісії з ефективності правосуддя щодо електронного подання документів до суду (е-подання) та оцифрування їх судом від 9 грудня 2021 // Guidelines on electronic court filing (e-filing) and digitalisation of courts. Document adopted at the 37th plenary meeting of the CEPEJ, Strasbourg and online, 8 and 9 December 2021 URL: https://rm.coe.int/cepej-2021–15-en-e-filingguidelines-digitalisation-courts/1680a4cf87 (дата звернення 20.03.2023)

з-поміж іншого, передбачають отримання та оцінку показань свідків (п. 87).[1]

У загальній законодавчій базі процесуальні норми повинні передбачати судове визначення використання технології для конкретних цілей. Держави-члени повинні зробити доступними диференційовані правила для різних форм процедури. Будь-яка дискреція, передбачена процесуальними правилами, а з цього приводу й законодавством, щодо використання технологій у конкретних провадженнях. має здійснюватися радше в судовому, а не в адміністративному порядку (п. 89).[2]

Як влучно зазначено у Висновку №14 (2011) Консультативної ради європейських суддів «Судочинство та інформаційні технології» ІТ повинні бути інструментом або засобом …забезпечення гарантій, встановлених ст. 6 ЄКПЛ. Тож використання ІТ не повинно обмежити процесуальні права та гарантії тих, хто не має доступу до сучасних технологій; держави мають гарантувати, що їм надають відповідну допомогу в цій сфері (п. 10). Через те, що не всі особи мають доступ до ІТ, не можна нехтувати традиційними засобами доступу до інформації. Довідкові стенди та інші форми допомоги, що надаються в судах, не повинні зникнути з огляду на те, що ІТ зробили судочинства доступним для усіх. Ці заходи – невідкладна турбота про соціально незахищені та уразливі верстви населення (п. 9).[3]

Принагідно зауважимо, що ЄСПЛ в аспекті гарантованих прав і свобод за статтею 6 Конвенції (право на справедливий суд) у своїй практиці наголошує на недопустимості відмови особі звертатись до суду в традиційному «паперовому форматі». Так, у рішення по справі XAVIER LUCAS v. France, ЄСПЛ визнав відмову апеляційного суду прийняти від заявника паперову версію процесуального документа надмірним формалізмом, адже адвокат заявника обґрунтовував неможливість подання документа за допомогою електронної платформи помилками в її функціонуванні. Тож ЄСПЛ констатував порушення вимог статті 6 Конвенції.[4]

Видається вдалим прикладом збалансованого підходу до ЦКП (за формулою цифровий за замовчуванням + унормована альтернативність) є ч. 3 ст. 160–2 КПК Естонії, котра встановлює правило про те, що учасники провадження подають заяви, скарги інші документи особі, що веде провадження, електронним засобом, якщо відсутня поважна причина для подання процесуального документа в іншій формі.

Юридико-технічний аспект гнучкого підходу до ЦКП вбачається в уникненні надмірної конкретизації нормативного механізму цифрових процедур, залишаючи правозастосовникам певну свободу для маневрування (дискреційне коло) (щоб норма залишалась положенням загального порядку, яке «розраховано на ситуації масового вжитку»… а не створювалась під ситуацію на кшталт «тут і тепер»[5]). Зазначений аспект у розвиток попереднього вимагає побудови нормативних конструкцій підстав та порядку проведення цифрових процедур у спосіб визначення мінімальних вимог, залишаючи певний простір для їх індивідуалізації правозастосовником згідно з фактичною ситуацією (ad hoc), що склалась у перебігу прийняття рішення (*баланс мінімальних вимог і творчості*), тим самим забезпечуючи гнучкість правореалізаційного процесу. Інакше кажучи, затребуваним є унормування альтернативності традиційного формату провадження, залишаючи правозастосовнику певний діапазон дискреції – реагувати адекватно конкретній правовій та фактичній ситуації (ad hoc), з іншого боку – можливість учасників процесу за наявності достатніх підстав реалізовувати свої права у традиційній формі (письмовій, за фізичною присутністю) (наприклад, у контексті права сторони захисту на дистанційне ознайомлення з матеріалами провадження).

Тож пріоритетність цифрового формату має балансувати із гнучкістю щодо конкретного випадку, коли у конкретній правовій ситуації найбільш прийнятним та доцільним з урахуванням основного вектора цифровізації – прав та свобод

---

[1] Висновок Консультативної ради європейських судів: Рухаючись вперед: використання асистивних технологій у судочинстві №26 (Страсбург, 1 грудня 2023 року). URL: https://hcj.gov.ua/page/vysnovky-kryes (дата звернення: 15.02.2024)

[2] –

[3] Висновок №14 (2011) Консультативної ради європейських суддів до уваги Комітету міністрів Ради Європи про правосуддя та інформаційні технології (ІТ) URL: https://rm.coe.int/opinion-n-14–2011-on-justice-and-information-technologies-it-/16806a1fc0 (дата звернення 20.03.2024)

[4] AFFAIRE XAVIER LUCAS c. FRANCE (Requête no 15567/20) ARRÊT Cour européenne des droits de l'homme 9 juin 2022 URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001–217615%22]} (дата звернення 20.03.2024)

[5] Гмирко В. П. *Доказування в кримінальному процесі: діяльнісна парадигма. Теоретичний аналіз. Проблематизація. СМД-репрезентація: монографія* (Акад. митної служби України, 2010) 179

учасників процесу буде обрання саме паперового формату документування. Адже, усі гарантії справедливого судового розгляду поширюються на цифрове судове провадження. Зміни до регламенту у зв'язку з цифровізацією судочинства, у тому числі актів і документів, мають бути внесені з дотриманням права на справедливий суд. Доступ до ефективних засобів судового захисту має надаватись у випадку негативного впливу або шкоди основним правам будь-якого користувача через використання технологій.

Видається правильним ставити питання не про можливість в перспективі повної технологізації кримінального провадження із супутнім усуненням традиційних процедур та паперу з кримінального провадження, а максимальну гнучкість та системність процесу переходу до розумно техногенного процесу. Останнє є можливим лише за наявності виваженої правової та технологічної стратегії, яка буде предметом подальшої наукової розвідки.

5. Пошук оптимальних балансуючих механізмів, котрі б запобігали надмірним ризикам ЦКП, втім не стримували цей процес підводить нас до наступного принципу ЦКП – ризикоорієнтованого підходу у процесі цифровізації (далі – РОП), функціональне призначення якого вбачається навіть ширше ніж принципу, а саме як методологічної основи прийняття всіх цифрових рішень.

Кожне явище для цивілізованого суспільства, як правило, має дві сторони: позитивну і негативну. Це стосується й цифрових технологій, масштабне впровадження яких в загальносоціальному форматі обіцяє якісний прогрес щодо усіх напрямів суспільного буття, звільнення людей від рутини у будь-якій сфері діяльності. З іншого боку, супутні цифровізації проблеми у разі її не контрольованості здатні звести нанівець увесь очікуваний позитивний ефект, зокрема й в царині правосуддя. Невипадково у згаданому Висновку №26 КРЕС не лише детально описала, як суди можуть використати у своїй роботі переваги технологій, але й перелічила ризики, які неодмінно супроводжують переваги використання асистивних, тобто, допоміжних технологій під час здійснення правосуддя. Якщо під ризиками ЦКП розуміти імовірні можливості небезпеки у вигляді отримання під час реалізації цього процесу небажаних, з точки зору досягнення запланованої мети та виконання поточних завдань, результатів у вигляді спричинення шкоди охоронюваним законам інтересам, то потенційно ризикованими напрямами ЦКП, реалізація яких містить елемент небезпеки виникнення небажаних негативних результатів, є більшість з виділених нами векторів ЦКП (переведення документообігу в електронну форму; запровадження єдиної інтегрованої (розумної) електронної системи органів кримінальної юстиції, поєднаної із загальнодержавними електронними реєстрами та базами даних (електронного кримінального провадження (ЕКП)); використання цифрової інформації у доказуванні (збирання, закріплення та зберігання); переведення процесуальної комунікації в цифровий формат; розширення цифрового сегмента під час проведення слідчих (розшукових), негласних слідчих (розшукових) та інших процесуальних дій розширення дистанційності в кримінальному провадженні, використання технологій штучного інтелекту).

Ідентифікації можливих ризиків на кожному з виділених векторів ЦКП є необхідною умовою системного управління такими ризиками як на правотворчому, так й правозастосовному рівнях. Інакше кажучи, потрібно розуміти, з якими загрозами ми маємо справу, та відповідно до їх змісту та рівня обирати надійні засоби їх упередження. Тож сам факт імовірної небезпеки не є червоним світлом для ЦКП, а вимагає системного підходу до управління такими небезпеками як під час стратегічної діяльності правозастосовника, так і під час тактичного правозастосування. В той час як системна невирішеність цих питань може призвести до неефективності та уповільнення темпів розвитку ЦКП, реалізації «реакційної», а не стратегічної кримінальної процесуальної політики. Тому на доктринальному та правотворчому рівні постає завдання максимального «просування» у бік ЦКП – в допустимих межах з урахуванням ризиків, які супутні цьому процесу (керування ризиками). З огляду на це видається принциповим та необхідним використання популярної у світі концепції РОП, як методологічної основи прийняття у царині кримінального судочинства цифрових управлінських рішень стратегічного та тактичного характеру, що стане предметом подальшого дослідження.

6. Виокремлення наступного принципу зумовлено стрімким розвитком технологій ШІ. З огляду на проспективні можливості ШІ для царини кримінального судочинства важливим є *збереження провідної ролі людського фактора при прийнятті кримінальних процесуальних рішень*.

ШІ та його використання у сфері правосуддя та кримінальному судочинстві активно обговорюється правничою спільнотою як в Україні, так і у світі. В Європейській хартії етичного використання ШІ в судових системах та суміжному середовищі, ухваленої на 31 пленарному засіданні у м. Страсбурзі 3–4 грудня 2018 р.[1] (далі – Хартія) позначені високі очікування від використання ШІ[2] як потенційного засобу ефективного та якісного правосуддя. У вже згадуваному документі Висновки Ради ЄС:[3] наголошено на очевидний потенціал використання інструментів ШІ для покращення функціонування систем правосуддя (прискорення судових проваджень, сприяння підвищенню узгодженості судової практики, якості судових рішень) та перспективність ШІ у майбутньому для виконання, зокрема, таких завдань, як то: аналіз, структурування та підготовка інформації щодо предмета справ, автоматична транскрибація записів усних слухань, машинного перекладу, підтримки аналізу та оцінки юридичних документів і рішень судів/трибуналів, автоматичної анонімізації судової практики та надання інформації через юридичні чат-боти та ін.(п. 38). На думку Європейської комісії особливий інтерес у сфері правосуддя становлять анонімізація судових рішень (анонімізація – це метод обробки даних, при якому ідентифікаційна інформація видаляється або змінюється), транскрибація записів судових засідань, машинний переклад, чат-боти, що підтримують доступ до правосуддя, та автоматизація процесів роботів (п. 3.3. програмного документа ЄС Цифровізація правосуддя в Євросоюзі: інструментарій можливостей» (далі по тексту для корисності посилання – Інструментарій)[4]).

Як відмічають сучасні дослідники, існує світовий досвід й щодо використання штучного інтелекту для прийняття процесуальних рішень у кримінальному провадженні[5]. Зокрема, під час прийняття рішення про реєстрацію заяви або повідомлення про кримінальне правопорушення в Іспанії. США, будучи одним з передових користувачів ШІ у правосудді, використовують такі технології під час обрання запобіжного заходу.[6]

Обґрунтованими є очікування від систем ШІ, що органічно мають бути закладені в систему електронного кримінального провадження (ЕКП). Так, зокрема, на думку Т. О. Павловой «….електронний інтелект, закладений в основу ЕКП, суттєво спростить процес кваліфікації, що пов'язан з обранням необхідного складу кримінального правопорушення, який містить усі ознаки вчиненого кримінального правопорушення». Як зазначає авторка «…«розумна система» допоможе з'ясувати, яке кримінальне правопорушення було вчинено, електронний інтелект може розробити необхідний та поетапний план розслідування, із пропонуванням необхідної норми (норм), за якою слід кваліфікувати вчинене кримінальне правопорушення». Також, на її думку, з якою ми погоджуємось, «… електронний інтелект здатний контролювати строки проведення необхідних слідчих дій, наприклад, строки проведення обшуку або арешту майна, таким чином виключається порушення норм КПК України та незаконний тиск на учасників процесу. У разі застосування запобіжного заходу у виді тримання під вартою, підозрюваний (обвинувачений) буде знаходитися під вартою стільки часу, скільки передбачено в КПК України, програма повідомляє про закінчення таких строків, що виключить затягування розслідування.»[7] Позначені

[1] European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment / Adopted at the 31st plenary meeting of the CEPEJ (Strasbourg, 3–4 December 2018). URL: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699 (дата звернення: 15.02.2024)

[2] *Примітка.* Під ШІ у Хартії розуміється набір наукових методів, теорій та технологій, що мають на меті відтворення за допомогою машини когнітивних здібностей людського мозку.

[3] Access to justice: seizing the opportunities of digitalisation. Council Conclusions 11599/20. Council of the European Union. Brussels, 2020. URL: https://data.consilium.europa.eu/doc/document/ST-11599–2020-INIT/en/pdf_(дата звернення: 15.02.2024)

[4] Digitalisation of justice in the European Union: A toolbox of opportunities» European Commission. COM/2020/710 final. Brussels, 2020.. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020DC0710 (дата звернення: 15.02.2024)

[5] Кісленко Д. П. 'Захист прав особи в аспекті діджиталізації кримінального провадження' (2021) 29 Наукові записки Львівського університету бізнесу та права 118

[6] *Примітка.* Так, дослідники зі Стенфордського університету (Stanford Computational Policy Lab) розробили алгоритм, який асистує судді під час обрання до підсудного: тримання під вартою або застави. Розглянувши близько 100 тисяч процесуальних документів, пов'язаних з обранням запобіжних заходів, розробники виявили, що одні судді в 90% випадків дозволяють громадянам виходити під заставу, тоді як інші – тільки в 50%. Програма дає змогу справедливо оцінити ризики й обирати тримання під вартою значно меншій кількості осіб [' Штучнийінтелект у правосудді' (Центр демократії та верховенства права) <https://cedem.org.ua/analytics/shtuchnyj-intelekt-pravosuddia/>(дата звернення: 12.04.2024)].

[7] Павлова Т. О. 'Діджиталізація як напрям трансформації кримінального провадження' (2021) 41 Правова держава 96 <http://pd.onu.edu.ua/article/view/225612> (дата звернення: 15.02.2024)

та інші напрями звичайно є надто перспективними та мають бути опановані в процесі ЦКП. Втім вони є лише допоміжними для працівників органів кримінальної юстиції та в певних випадках безпосередньо сприяють ефективному забезпеченню прав учасників. Водночас чи в змозі технології ШІ стати самостійним інструментом прийняття рішень в кримінальному провадженні як кульмінаційного етапу всієї інтелектуально-праксеологічної діяльності, що здійснюється правозастосовниками?

Одним з популярних аргументів прихильників технологій ШІ є його об'єктивність, обумовлена тим, що «ШІ інтелект позбавлений висловлення власних точок зору, а діє виключно за алгоритмом, тобто порушення прав та законних інтересів учасників кримінального провадження із використанням штучного інтелекту мінімізоване», тож ніби то «унеможливлює корупційну та емоційну складову[1]. Втім як показує світовий досвід використання у правосудді популярного через його зручність ChatGPT для пошуку релевантних судових рішень виявило як мінімум 2 ризики, що пов'язані з його непрозорістю (як і будь-якої іншої системи ШІ): по-перше, це ризик використання неправдивої інформації, а отже, взагалі спотворення його функційного призначення як оперативного допоміжника правозастосовнику (зокрема, феномен «галюцинації» – відповідь чат-бота, що здається правдоподібною, проте насправді є неправильною). По-друге, ризик генерування упереджених даних та пов'язаний з цим ризик дискримінації.

Зазначимо, що в загальному механізмі справедливого вирішення кримінальної справи чільне місце відведено саме використанню *унікальних емоційно-когнітивних здібностей та компетенції особи, що приймає те чи інше процесуальне рішення.* Слушною слід визнати думку Каменєвої Т. про те, що «саме людська здатність поєднувати правову обізнаність з когнітивною та емоційною компетенціями дозволяє знаходити оптимальне рішення в ситуації, коли не можна не брати до уваги моральні норми й в суперечність вступають справедливість та законність. Звідси випливають суто інтуїтивні наміри щодо вивчення додаткових доказів, прийняття рішення про необхідність перекваліфікації злочину, наполягання на звинуваченні або відмови від нього тощо».[2] Судове рішення, принаймні у кримінальному провадженні, не може стати результатом механічного застосування норм закону, його зміст є «квінтесенцією інформації та знань, що формально відображаються у ньому і вироблені на основі специфічних практичних навичок, а їх підґрунтям є норми кримінального процесуального законодавства. У досліджуваному аспекті кримінальне процесуальне законодавство встановлює межі застосування герменевтики судових рішень у кримінальному провадженні.[3] Звісно, що людський фактор нерідко обумовлює різність судової практики. Утім, хоча й «…окремі судді можуть по-різному тлумачити закон, але вони роблять це публічно та їхні рішення можуть бути оскаржені. Це має зменшити ступінь різності судового правотлумачення з часом – принаймні в теорії. Але якщо програма занадто сувора або занадто гнучка у контексті обрання та застосування закону, це може бути дуже важко виявити та виправити.»[4]

Інакше кажучи, технологія прийняття рішень у такій царині як кримінальне провадження не може бути позбавлена людського фактора. Саме цей посил пронизує останній висновок КРЕС №26, в якому Європейською інституцією однозначно наголошено про те, що попри безумовну корисність передових технологій у сприянні ефективності суддівської діяльності, сам процес ухвалення судового рішення не може бути ним делегований. КРЕС, висвітлюючи виклики ШІ для незалежності судової влади, неупередженості суду та справедливого судового розгляду, вказала, зокрема на те, що використання технологій повинно, перш за все, поважати природу судового процесу. По-перше, багато судових рішень є дискреційними рішеннями, заснованими на конкретних фактах окремої справи. По-друге, судді відіграють суттєву роль у розвитку права. Вони не просто застосовують фіксовані та незмінні правила. Судді повинні мати можливість виправляти або доповнювати закон, якщо він не відповідає вимогам або загрожує за-

[1] Каменєва Т. 'Можливості та межі використання цифрових технологій в сфері кримінально-процесуальної діяльності' (2020) 8 (193) Громадська думка про правотворення 21 <http://nbuviap.gov.ua/images/ dumka/2020/8.pdf.>

[2] Каменєва Т. –

[3] Циганюк Ю. В. 'Герменевтика судових рішень у кримінальному провадженні' (2021) 4 Дніпровський науковий часопис публічного управління, психології, права. 38–39 <https://chasopys-ppp.dp.ua/index.php/chasopys/article/view/98/89>(дата звернення: 15.02.2024)

[4] Kennedy Rónán 'AI: why installing 'robot judges' in courtrooms is a really bad idea' (The Conversation) <https://theconversation.com/ai-why-installing-robot-judges-in-courtrooms-is-a-really-bad-idea-208718> (дата звернення: 15.02.2024)

шкодити його застосуванню в певних справах. Технології не повинні втручатися у сферу справедливості. Технології не повинні знеохочувати або перешкоджати критичному мисленню суддів, оскільки це може призвести до стагнації правового розвитку та ерозії системи правового захисту. Тому технологічні інструменти повинні поважати процес ухвалення судових рішень і автономію суддів (п. 90).[1]

КРЕС також застерегла про прогнозований негативний вплив на професійні якості правозастосувачів внаслідок надмірного покладання на цифрові технології, зокрема, спроможність визначати та оцінювати силу доказів через залежність від технічної допомоги, яка не завжди супроводжується достовірністю та об'єктивністю результатів.

Ухвалення судових рішень є висококваліфікованою діяльністю. Це вимагає значної підготовки та досвіду. Використання інструментів обробки даних як заміни правового дослідження суддею та асистивного ШІ для допомоги суддям в ухваленні рішень може підірвати здатність кожного судді досліджувати та ухвалювати рішення. Використання прогностичного кодування може, наприклад, підірвати здатність судді визначати, що є, а що ні, релевантним доказом, і може негативно вплинути на його або її здатність оцінювати надійність доказів. Попри те, що такі інструменти призначені для сприяння ухваленню судових рішень, з часом вони можуть знизити кваліфікацію та досвід суддів. (п. 60). Одним із можливих наслідків того, що судді більше не зможуть Таким чином, те, що покликано бути допоміжним, може фактично стати рішенням. Особливо проблематичним може бути те, якщо така допомога надає окремим суддям оцінку норм щодо ухвалення рішень на основі загальних тенденцій серед суддів; дана проблема згодом буде лише поглиблюватись, оскільки все більше суддів слідуватимуть тенденції, визначеній інструментами обробки даних. У більш широкому плані це створює загрозу для інституційної незалежності, оскільки фактично віддасть процес ухвалення рішень у руки тих, хто розробляє інструменти обробки даних (п. 61).[2]

7. Наступним стандартом ЦКП, на нашу думку, є прозорість використання цифрових технологій в кримінальному провадженні.

Одним з основних потенційних «недоліків» використання ШІ у судочинстві у контексті забезпечення справедливої кримінальної процедури є супутній ефект непрозорості чи ефект «чорної скриньки», котрий «перешкоджає належній і необхідній відповідальності та унеможливлює перевірку того, як було досягнуто результату та чи він відповідає вимогам з відповідними нормативними актами. Цей брак прозорості може підірвати можливість ефективного оскарження рішень, прийнятих на основі таких результатів, і, таким чином, може порушити право на справедливий судовий розгляд та ефективний засіб правового захисту, а також обмежити сфери, в яких ці системи можуть використовуватися на законних підставах» (п. 41 Висновків Ради ЄС). Це обумовлює необхідність заборони автоматизації, яка зробить процес ухвалення судових рішень непрозорим (п. 44). Застосування штучного інтелекту в секторі правосуддя може також містити ризик збереження та, можливо, посилення існуючої дискримінації, включаючи стереотипи, упередження чи структурну нерівність, а також дозволу спотвореного або непрозорого прийняття рішень, і, таким чином, може призвести до порушення основних прав, таких як людська гідність, право на свободу, недискримінацію, приватність і захист даних і право на справедливий суд (п. 40).[3]

Зазначимо, що у фінальній версії Закону про штучний інтелект (Artificial Intelligence Act, AI Act), одноголосно схваленої членами Європейського Союзу 2 лютого 2024 року до заборонених віднесено використання прихованих технологій та програм, що використовують штучний інтелект для підсвідомої маніпуляції або зловживання слабкостями людей, що може призвести до фізичної або психологічної шкоди, невибіркового використання біометричної ідентифікації в реальному часі в громадських місцях для забезпечення правопорядку або використання владою «соціальних оцінок», отриманих за допомогою штучного інтелекту, для обмеження прав окремих осіб чи груп. Закон повністю забороняє останнє, в той час, як для

[1] Висновок Консультативної ради європейських судів: Рухаючись вперед: використання асистивних технологій у судочинстві № 26 (Страсбург, 1 грудня 2023 року). URL: https://hcj.gov.ua/page/vysnovky-kryes (дата звернення: 15.02.2024)

[2] –

[3] Access to justice: seizing the opportunities of digitalisation. Council Conclusions 11599/20. Council of the European Union. Brussels, 2020. URL: https://data.consilium.europa.eu/doc/document/ST-11599–2020-INIT/en/pdf (дата звернення: 12.04.2024)

перших трьох пунктів пропонується режим дозволу в контексті правоохоронної діяльності. Тож системи штучного інтелекту будуть зобов'язані надавати інформацію про те, як вони працюють і приймають рішення, тим паче у царини правосуддя.[1]

На додаток, вважаємо, що в сенсі зазначеного стандарту має йти мова не тільки про застосування ШІ, а щодо використання будь-яких цифрових технологій у кримінальному провадженні. Тож видається, що викладене є релевантним й щодо застосування інших цифрових інструментів.

8. Важливим регулятором використання цифрових технологій та систем ШІ у судочинстві має бути й *покладення відповідальності за ризики, супутні їх застосуванню під час кримінальної процедури, на представників органів кримінальної юстиції.*

Таке положення обумовлено загальним вектором меж ЦКП, та носить здебільшого праксеологічний характер, оскільки зводиться до відповідального підходу слідчого, дізнавача, прокурора, судді при оцінці ризиків використання цифрових інструментів під час провадження. Адже, як правило, застосування цифрових технологій у кримінальному процесі характеризується певною дискретністю правозастосовника в межах, дозволених законом. Наочно це демонструє процедура *розв'язання питання про можливість проведення дистанційного провадження*, яке у контексті вимоги справедливого судового розгляду за настановами міжнародних організацій має відбуватися з урахуванням всіх особливостей конкретної справи. Так, Європейська комісія з питань ефективного правосуддя (CEPEJ) у пункті 41 «Керівництва щодо проведення судових проваджень у режимі відеоконференції» (далі – Керівництво) від 30.06.2021 (CEPEJ(2021)4REV4) також рекомендувала судам залежно від вимог національного законодавства забезпечувати можливість участі осіб у судових засіданнях в режимі відеоконференції із залів суду, місць позбавлення волі, приміщень юридичних фірм чи інших безпечних місць, перелік яких не є вичерпним. Комісією також наголошено на тому, що держави повинні забезпечити, щоб правова база надала судам достатні підстави для розв'язання питання про те, чи можна або потрібно проводити дистанційне слухання в окремому випадку. Адже *саме суд, виходячи з правової бази, наданої державою, повинен визначити, чи проведення дистанційного слухання є розумним і доцільним за конкретних обставин справи, та обґрунтувати своє рішення*.

Як показує аналіз законодавства та правозастосовної практики питання про допущення учасника до судового засідання з використанням власних технічних засобів вирішується суддями нерідко діаметрально протилежно залежно від конкретної правової ситуації. В основі позитивного розв'язання вказаного питання полягає внутрішнє переконання судді не лише в тому, що існують достатні підстави для дистанційного провадження (зокрема, легітимна мета[2]), але й будуть забезпечені всі необхідні умови ідентифікаційного та конфіденційного характеру. Тож однією з проєкції визначеного стандарту меж ЦКП є відповідальний підхід правозастосовників при розв'язанні питань щодо допущення використання цифрових інструментів у конкретній справі.

Як наголошує КРЕС, судді мають чітко відзначати як переваги, так і недоліки цифрових технологій, враховувати та не допускати будь-яких порушень у здійсненні правосуддя. Цифрові технології не повинні обмежувати процесуальні права сторін. Судді повинні усвідомлювати можливість такої загрози, оскільки с*аме вони є відповідальними за дотримання та захист прав сторін* (п. 7,8 Керівництва).

Окремим практичним зрізом позначеного стандарту є відповідальне використання особами, що ведуть провадження, технічних засобів під час реалізації процесуальної діяльності. Так, наприклад, в одному з практичних кейсів, «технічна» недбалість суддів під час переходу до режиму нарадчої кімнати призвела до розголошення таємниці їх наради. Нагадаємо, що у випадку здійснення наради суддів у залі судового засідання без видалення в окреме приміщення, забезпечення дотри-

[1] Artificial Intelligence Act P9_TA(2024)0138 (COM(2021)0206 – C9-0146/2021–2021/0106(COD)) European Parliament 19.4.2024 URL: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL–COR01_EN.pdf (дата звернення: 05.05.2024)

[2] *Примітка*. Як наголошується у міжнародних рекомендаціях з питань ВКЗ, Легітимна мета дистанційного слухання у кримінальному провадженні має базуватися на таких цінностях, як охорона громадського порядку, здоров'я населення, попередження правопорушень, захист права на життя, свободу та безпеку свідків і жертв злочинів. Дотримання права на судовий розгляд упродовж розумного строку може розглядатися судом, зокрема, на стадіях провадження після першої інстанції» (Рекомендації щодо відеоконференцзв'язку в судовому провадженні, 2021, § 21–22).

мання вимоги таємниці такої наради як функційного обов'язку суду передбачає влаштування судом такого технічного формату суддівського обговорення, що виключив би об'єктивну можливість присутніх бути обізнаними щодо суті змісту такого обговорення під час перебування суду у режимі нарадчої кімнати. Втім, у відповідно до матеріалів КП _1 пасивні дії суду у вигляді не вимкнення мікрофона в залі судового засідання під час наради суддів призвели до розголошення таємниці наради суддів, яка охороняється законом.

Поміж позначених праксеологічних зрізів регулятор ЦКП, що розглядається, має бути також дороговказом й для законодавця у разі унормування ризиків супутніх використанню цифрових технологій у кримінальному провадженні. З огляду на це заперечення викликає положення Закону України «Про внесення змін до Кримінального процесуального кодексу України щодо забезпечення поетапного впровадження Єдиної судової інформаційно-телекомунікаційної системи» № 8219 від 23.11.2022 (який прийнято Верховною Радою України 23 лютого 2024 р.) щодо перекладення відповідальності за технічні ризики (переривання зв'язку тощо) під час участі у відеоконференції поза межами приміщення суду з використанням власних технічних засобів, на учасника кримінального провадження, який подав відповідне клопотання (ч. 6 ст. 336 КПК). Адже такий підхід є хоча і застосовним до інших процесів (цивільного (ч. 5 ст. 212 Цивільного процесуального кодексу України) та господарського (ч. 5 ст. 197 Господарського процесуального кодексу України)), утім не може автоматично переноситись до царини кримінального судочинства як потенційно «шкідливе» нормативне рішення з точки зору захисту прав та законних інтересів людини. Адже, як справедливо зазначає ЄСПЛ, вимоги справедливого судового розгляду є суворішими у сфері кримінального права, ніж у цивільному аспекті статті 6 («Морейра Ферейра проти Португалії (№ 2)» (Moreira Ferreira v. Portugal (no. 2)) [ВП], § 67; «Кармель Саліба проти Мальти» (Carmel Saliba v. Malta), § 67)[1].

Крім того, на недосконаліть аналізованого нормативного положення вказує й те, що, по-перше, не зовсім зрозумілим є змістовне навантаження такого положення, враховуючи, що наслідки переривання зв'язку та технічної неможливості участі особи у відеоконференції не передбачаються чинним законодавством. По-друге, виникає питання щодо можливості покладення на особу ризиків переривання зв'язку та технічної неможливості участі у відеоконференції внаслідок неможливості суду забезпечити стійкий зв'язок або взагалі розпочати відеоконференцію (особливо враховуючи перебої з електропостачанням, які спостерігаються останнім часом у нашій державі).[2]

9. Наступним засадничим положенням ЦКП є *забезпечення інформаційної безпеки (кібербезпеки) кримінального провадження*[3].

Поряд із чисельними можливостями, які надають цифрові технології у царині судочинства, не можна забувати й про супутні небезпеки та за-

[1] *Посібник зі статті 6 Конвенції – Право на справедливий суд (кримінально-процесуальний аспект)* <https://www.echr.coe.int/Documents/Guide_Art_6_criminal_UKR.pdf> (дата звернення: 15.02.2024)

[2] Клепка Д. І. 'Здійснення судового контролю під час досудового розслідування в порядку дистанційного судового провадження: аналіз судової практики' (2022) 45 Питання боротьби зі злочинністю 93

[3] *Примітка.* Щодо співвідношення понять інформаційна безпека та кібербезпека то варто зазначити про таке. Інформаційна безпека електронного кримінального провадження – це стан захищеності інформаційного середовища електронного кримінального провадження (апаратного і програмного сегментів та суб'єктів кримінального провадження), що забезпечує його функціонування, формування, використання і розвиток для ефективного виконання завдань кримінального провадження. [Каланча І. Г. 'Інформаційна безпека електронного кримінального провадження України' (2018) 3 Науковий часопис Національної академії прокуратури України 11–22.] Інформаційну безпеку на рівні держави у найзагальнішому розумінні можна визначити як такий стан захищеності інформаційного простору держави, за якого неможливо завдати збитку властивостям об'єкта безпеки, що стосуються інформації та інформаційної інфраструктури, і який гарантує безперешкодне формування, використання й розвиток національної інфосфери в інтересах оборони [Толубко В. Б (ред) *Інформаційна та кібербезпека: соціотехнічний аспект: підручник* (ДУТ, 2015) 13–15. В цифрову еру інформація, в тому числі і в судочинстві, все більше переноситься в кіберпростір (середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, і в хмару, що обумовлює необхідність захисту інформації саме в діджитал (кібер) середовищі. Кібербезпека – захищеність життєво важливих інтересів людини й громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі (п. 5 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України»)Тож Кібербезпека – це вже новий виток інформаційної безпеки, який спрямований саме на діджитал середовище. Кібербезпека має на увазі не тільки сам по собі захист інформації, а й захист всієї системи в інформаційному полі, в ІТ-полі (поле комп'ютерних технологій) в цілому. Втім як би ми не називали безпеку інформації в кримінальному провадженні це є обов'язковим об'єктом забезпечення як на рівні держави, так і на рівні органів кримінальної юстиції.

грози. Адже досягнення прогресу в інформаційно-комунікаційній сфері широко використовуються й злочинцями – вони також використовують переваги цифровізації, чи то скоюючи онлайн-злочини, чи використовуючи цифрові інструменти для здійснення злочинної діяльності. Як зазначено Комітетом Ради Європи «..використання цифрових технологій у секторі правосуддя є дуже чутливим і тому має відповідати найсучаснішим стандартам щодо інформаційної та кібербезпеки та повністю відповідати законодавству про конфіденційність і захист даних. Збільшення довіри до цифрових технологій, зокрема до автоматизованих процесів, вимагає ретельного моніторингу таких систем, включно тих, що використовують штучний інтелект, і підвищеної прозорості для забезпечення довіри громадськості» (п. 21 Висновків). «Технологія повинна підлягати ефективним організаційним і технічним заходам, узгодженим із застосовними стандартами, які вимагає будь-яке чинне законодавство про захист даних, щоб підтримувати цілісність і безпеку даних, які використовуються судовими органами, щоб підтримувати довіру до неї та легітимність судової влади. Такі заходи мають передбачати диференційований контроль доступу до таких даних для суддів, судової адміністрації, сторін, законних представників та громадськості» (п. 92 (xi) ВКРЕС №26)[1]

Оскільки ж поступова діджиталізація з неминучістю перенесе процесуальну комунікацію учасників провадження у кіберпростір на базі відповідних інформаційних систем, а основний сегмент доказово фонду кримінального провадження складатиме інформація, що зафіксована в електронній формі, забезпечення інформаційної та кібербезпеки кримінального провадження стає пріоритетним напрямком науково-технічної діяльності, вимагаючи істотної уваги й зусиль як з боку держави, так і безпосередньо органів кримінальної юстиції. Тож, як влучно зазначає І. Г Каланча активного дискурсу набуває потреба в комплексному забезпеченні інформаційної безпеки електронного кримінального провадження, що зумовлює актуальність дослідження цього питання[2]. Слід погодитись з авторкою, що захист інформації під час використання електронних технологій у кримінальній юстиції сьогодні виокремлюється як самостійний інститут, а також як складова процесуальної діяльності, а тож потребує окремого дослідження. На цих сторінках ми лише позначили цей аспект як чинник, що впливає на масштабність процесу ЦКП.

Звичайно забезпечення інформаційної безпеки, в тому числі належний захист бази даних у кримінальному провадженні, є окремим напрямом державної діяльності, складовою частиною національної безпеки. Наприклад, через потенційний ризик знищення електронних матеріалів провадження нового технічного підходу вимагає механізм забезпечення таємниці слідства й захисту свідків, потерпілих та ін., адже розголошення інформації може загрожувати їхній безпеці та життю. Так, зокрема, право підсудного на захисника під час дистанційного судового розгляду може бути реалізоване за умови ефективного забезпечення його конфіденційного спілкування з захисником, а тож держава має забезпечити такі дистанційні канали зв'язку, конфіденційність яких не викликає сумнівів.

10. Рівність цифрових прав учасників процесу. Цей стандарт є похідним від загального принципу рівності учасників провадження та в цифровому сенсі вимагає від держави гарантувати дотримання принципу рівності учасників провадження у контексті доступу до цифрової інформації та технологій.

Передусім, сам факт переведення спілкування учасників процесу в digital-площину, надає реальну можливість забезпечити рівноправність сторін, їх прав мати повноцінний доступ до основної інформації та здійснювати пряму реалізацію наданих процесуальних прав. У контексті ж можливої цифрової нерівності на державу покладається обов'язок забезпечити додаткові гарантії для вразливих осіб. Так у п. 7 Висновків Ради ЄС наголошено, що всі громадяни повинні користуватися перевагами додаткових цифрових можливостей і мати рівні можливості щодо цифрового доступу до правосуддя та справедливого розгляду, і що цифрова участь має бути безумовно гарантована всім групам суспільства без будь-якої дискримінації. Особливо слід брати до уваги потреби вразливих груп населення, включаючи дітей і вразливих дорослих, таких як люди похилого віку

[1] Висновок Консультативної ради європейських судів: Рухаючись вперед: використання асистивних технологій у судочинстві № 26 (Страсбург, 1 грудня 2023 року). URL: https://hcj.gov.ua/page/vysnovky-kryes (дата звернення: 15.02.2024)

[2] Каланча І. Г. 'Інформаційна безпека електронного кримінального провадження України' (2018) 3 Науковий часопис Національної академії прокуратури України 11–22.

та особи з обмеженими можливостями, а також потреби жертв злочинів. У будь-якому випадку використання цифрових технологій у системі правосуддя не повинно зменшувати процесуальні гарантії для тих, хто не має доступу до таких технологій.

Видається стандарт «цифрової» рівності учасників провадження чи рівності «цифрових» прав учасників процесу має бути досліджений принаймні у таких напрямах: 1) забезпечення рівності сторін під час дистанційного провадження (гарантування рівних цифрових прав учасників процесу з упередженням можливих ризиків застосування цифрових технологій для права особи на справедливий судовий розгляд)[1]; 2) створення додаткових гарантій для вразливих учасників процесу[2]; 3) забезпечення баланс у доступі учасників провадження до електронного кримінального провадження (балансу між конфіденційністю розслідування, правом потерпілого та сторони захисту на інформацію). При цьому зробимо зауваження про те, що неодмінною умовою цифрової рівності учасників кримінального провадження є забезпечення державою фундаментального права особи на доступ до Інтернету[3] та якості інформації, що надається у цифровому просторі[4].

[1] *Примітка.* У Посібнику, підготовленому у 2020 році Бюро демократичних інститутів і прав людини ОБСЄ за результатом спостереження за особливостями функціонування судів в умовах пандемії COVID-19 [*The Functioning of Courts in the Covid-19 Pandemic. Primer* (OSCE, ODIHR, October 2020) 53 <https://www.osce.org/files/f/documents/5/5/469170.pdf> (дата звернення:)] висловлено низку занепокоєнь, які стосується ефективності забезпечення достовірної оцінки показань свідків та права на захист. Через те, що, наприклад, відеоконференції позбавляють сторони та суддю можливості спостереження за невербальними сигналами та за судовою залою загалом, це перешкоджає орієнтуванню та оцінці довіри до свідків. Ефективна та конфіденційна комунікація між сторонами та їхніми адвокатами під час слухання також є проблематичною, якщо взагалі можливою. Розгляд можливостей для використання платформ, які дозволяють об'єднуватися в окремі кімнати для проведення обговорень між адвокатами/клієнтами, може запропонувати рішення в деяких випадках; однак, об'єднання в окремі кімнати не забезпечує справжньої конфіденційності. Проведення слухань онлайн також може викликати труднощі у залученні перекладачів, в тому числі для конфіденційного спілкування сторін та їхніх адвокатів. Виникають також інші труднощі з тим, як перевірити особу сторін та свідків (особливо з огляду на можливості проникнення у технології), як подати та перевірити докази, як запобігти підгляданню свідків або сторін у «шпаргалки» або впливу на них чи отриманню сигналів третіми особами під час давання показань, а також як забезпечити належне проведення перехресного допиту та право (а в деяких юрисдикціях – дотримання законодавчої вимоги щодо права) обвинуваченого бути присутнім під час допиту свідка. Наприклад, ЄСПЛ визнав, що «важко зрозуміти, як» право особи, яка обвинувачується у вчиненні кримінального правопорушення, «особисто захищатися», допитувати свідків та отримувати допомогу перекладача, за потреби, можна здійснювати без фізичної присутності [Марсело Віола (№ 2), Заява № 45106/04, рішення від 5 січня 2007 року, п. 51;]. Також була поставлена під сумнів здатність оцінювати вразливість підсудних та її вплив на спроможність брати участь у дистанційному судочинстві [Інклюзивне правосуддя: система, розроблена для всіх, Комісія з питань рівності та прав людини, Сполучене Королівство, червень 2020 року. Див. також Захист права на справедливий суд під час пандемії коронавірусу: дистанційне провадження у кримінальному судочинстві, FairTrials.org, 3 квітня 2020 року].

[2] *Примітка.* Як наголошується у п. 19 Висновків РЄ повна, достовірна та своєчасна інформація з питань здійснення судочинства є основним аспектом, що гарантує доступ до правосуддя, як це зазначено в Статті 6 ЄКПЛ. Судді мають переконатися, що кожна особа, яка бере участь в судовому процесі, має доступ до достовірної інформації. Така інформація повинна містити дані або вимоги, дотримання яких необхідне в судовому процесі. Зазначені заходи потрібні для забезпечення рівності сторін в засобах захисту своїх прав.

[3] *Примітка.* Як наголошено у п. 4 Інструментарію діджиталізації Ради ЄС, процес цифровізації має повністю враховувати потреби незахищених груп населення. Цифрові технології стають все більш зручними та доступними для переважної більшості, незалежно від віку, рівня освіти та доступними для людей з обмеженими можливостями. Водночас інституційні, організаційні та технічні заходи повинні забезпечити повний доступ до правосуддя незахищеним групам і людям у вразливому становищі, таким як діти або люди похилого віку, які можуть не мати необхідних засобів або цифрових навичок. Жертви злочинів також повинні мати можливість користуватися цифровими інструментами відповідно до конкретних потреб кожної жертви.

[4] *Примітка.* Право на доступ до Інтернету є найпершим та найфундаментальнішим правом у Хартії прав людини та принципів Інтернету. У 2007 році Комітет міністрів Ради Європи у «Рекомендації щодо підвищення цінності Інтернету як суспільної служби» наголосив, що «доступ до Інтернету, здатність та можливість користуватися ним мають розглядатися як невід'ємні компоненти повноцінного здійснення прав людини та основоположних свобод в інформаційному суспільстві» [Селезньова О. М. 'Інтернет право і його місце в системі інформаційного права' (2013) 2–2 Вчені записки Таврійського національного університету ім. В. Вернадського 236–240.< http://www.juris.vernadskyjournals.in.ua/journals/2013/2-2_2013/35.pdf> (дата звернення: 11.04.2024)].

ЄСПЛ також визнав, що доступ до інтернет контенту є фундаментальним правом людини, яке може бути обмежене лише у виняткових випадках. Так, у рішенні ЄСПЛ Yildirim v. Turkey зазначено, що «Інтернет став одним з основних засобів здійснення права на свободу вираження поглядів та свободи інформації». Натомість як відмічає Л. Тарасенко у законодавстві України немає відповідних правових норм щодо права на доступ до Інтернету, тож законодавець жодним чином не гарантує громадянам можливості використовувати Інтернет на рівні спеціального законодавства.

Втім на справедливе зауваження автора, право на доступ до Інтернету охоплює не лише технічну та економічну, а й правову складову. Правові умови включають в себе такі складові: 1. держава повинна визнавати, що кожен має право на доступ до Інтернету, та гарантувати здійснення цього права; 2. держава повинна забезпечити можливість провайдерам працювати на ринку цих послуг (забезпечення доступу провайдерів на ринок). 3. держава не повинна втручатися у відносини «користувач Інтернету – провайдер». При цьому до принципів доступу до Інтернету він відносить, зокрема рівність доступу до Інтернету (доступ до Інтернету має надаватися за розумну ціну і бути недискримінаційним. Держава повинна створити

11. Останнім принципом ЦКП виступає вимога узгодженості темпів цього процесу із рівнем цифрової компетентності уповноважених осіб органів кримінальної юстиції.

Враховуючи, що цифрова компетентність є новим поняттям для юридичної науки перше за все хотілося б звернутися до термінологічного апарату, адже в літературі зустрічається такі терміни як «цифрова компетентність» та «цифрова компетенція». У цьому сенсі ми поділяємо думку М. С. Головань, який на підставі дослідження етимологічного визначення понять «компетенція» та «компетентність» зазначає, що «Компетенція – це певна норма, досягнення якої може свідчити про можливість правильного вирішення якогонебудь завдання, а компетентність – це оцінка досягнення (або недосягнення) цієї норми. Компетентність виступає в українській мові як якість, характеристика особи, яка дозволяє їй (або навіть дає право) вирішувати певні завдання, виносити рішення, судження у певній галузі. Основою цієї якості є знання, обізнаність, досвід соціально-професійної діяльності людини. Цим самим підкреслюється інтегративний характер поняття «компетентність».[1] На підставі вище викладеного вважаємо, що в контексті нашого дослідження більш правильним є використання поняття «цифрова компетентність».

Цілком зрозуміло, що неодмінною умовою цифрової трансформації кримінального провадження є формування цифрової компетентності працівників органів кримінальної юстиції, на що звертається окрема увага міжнародною спільнотою. Так у Висновку №14 КРЕС підкреслено, що нове законодавство з питань діджиталізації має набрати чинності тільки після того, як системи ІТ будуть адаптовані до нових вимог, а кадровий персонал суду буде навчений відповідним чином…. Судді та апарат суду мають право та зобов'язані пройти первинний курс навчання з використання ІТ, а також наступні курси підвищення кваліфікації (п. 39). Європейська комісія попередила про те, що судді та працівники суду можуть недостатньо добре володіти електронними платформами для доступу до документів, здійснення електронного управління справами, включаючи подання в електронному вигляді та електронні підписи, електронне управління справами та опції для проведення відеоконференцій. Обробка конфіденційної інформації в електронній формі означає, що судді та судовий персонал *повинні покращити свою обізнаність щодо засобів захисту даних та гарантій конфіденційності, включаючи відповідне національне законодавство та міжнародні стандарти.* Також було б корисним навчання з проведення дистанційних слухань» (п. 31 Висновків).[2] Тож формування цифрової компетентності має стати окремим напрямом у навчанні та підвищенні кваліфікації правника.

Висновки. Пошук оптимальних меж цифровізації кримінального провадження вимагає формулювання (виокремлення) та розгляд основних положень принципового характеру, сукупність яких є необхідною для врахування в перебігу здійснення цифровізації. Такі принципи своєю чергою є основою для формулювання похідних від них більш конкретних вимог практичного характеру – стандартів цифровізації кримінального провадження.

Проведене дослідження надає підстави виокремити такі стандарти ЦКП: верховенство права; правова визначеність; пріоритетність цифрового формату; гнучкість процесу цифровізації; застосування ризикоорієнтованого підходу; збереження провідної ролі людського фактора при прийнятті кримінальних процесуальних рішень; є прозорість використання цифрових технологій в кримінальному провадженні; покладення відповідальності за ризики, супутні їх застосуванню під час кримінальної процедури, на представників органів кримінальної юстиції; забезпечення інформаційної безпеки (кібербезпеки) кримінального провадження; вимога узгодженості темпів процесу цифровізації з рівнем цифрової компетентності уповноважених осіб органів кримінальної юстиції. Підкреслимо, що кожен з визначених нами принципів (стандартів) ЦКП є напрямом окремого предметного дослідження під кутом зору відшукання оптимальних меж цифровізації кримінального прова-

умови кожному громадянинові незалежно від раси, кольору шкіри, статі, національності для доступу до мережі Інтернет). [Тарасенко Л 'Право на доступ до інтернету' (2020) 71 Вісник Львівського університету. Серія юридична. 53–61].

[1] Головань М. С. 'Компетенція і компетентність: досвід теорії, теорія досвіду' (2008) 3 Вища освіта України 23–30 <https://core.ac.uk/download/pdf/324272272.pdf> (дата звернення: 16.01.2024)

[2] Висновок №14 (2011) Консультативної ради європейських суддів до уваги Комітету міністрів Ради Європи про правосуддя та інформаційні технології (ІТ) URL: https://rm.coe.int/opinion-n-14–2011-on-justice-and-information-technologies-it-/16806a1fc0 (дата звернення: 12.03.2024)

дження. Втім лише комплексне їх дотримання здатне забезпечити права та законні інтереси особи та досягти бажаного результату цифровізації кримінального провадження.

REFERENCE

List of legal documents

Legislations

1. Access to justice: seizing the opportunities of digitalisation. Council Conclusions 11599/20. Council of the European Union. Brussels, 2020. URL: https://data.consilium.europa.eu/doc/document/ST-11599–2020-INIT/en/pdf (in English)
2. Artificial Intelligence Act P9_TA(2024)0138 (COM(2021)0206 – C9-0146/2021–2021/0106(COD)) European Parliament 19.4.2024 URL: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL–COR01_EN.pdf (in English)
3. Digitalisation of justice in the European Union: A toolbox of opportunities» European Commission. COM/2020/710 final. Brussels, 2020.. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020DC0710 (in English)
4. European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment / Adopted at the 31st plenary meeting of the CEPEJ (Strasbourg, 3–4 December 2018). URL: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699 (in English)
5. Vysnovok Konsultatyvnoi rady yevropeiskykh suddiv do uvahy Komitetu ministriv Rady Yevropy pro pravosuddia ta informatsiini tekhnolohii (IT) № 14 (2011) URL: https://rm.coe.int/opinion-n-14–2011-on-justice-and-information-technologies-it-/16806a1fc0 (in Ukrainian)
6. Vysnovok Konsultatyvnoi rady yevropeiskykh sudiv: Rukhaiuchys vpered: vykorystannia asystyvnykh tekhnolohii u sudochynstvi № 26 (Strasburh, 1 hrudnia 2023 roku). URL: https://hcj.gov.ua/page/vysnovky-kryes (in Ukrainian)

Cases

7. AFFAIRE XAVIER LUCAS c. FRANCE (Requête no 15567/20) ARRÊT Cour européenne des droits de l'homme 9 juin 2022 URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001–217615%22]} (in French)
8. Sprava «Sandi Taims» (The Sunday Times) proty Spoluchenoho Korolivstva» (Zaiava № 6538/74) : Rishennia Yevropeiskoho sudu z prav liudyny vid 26 kvit. 1979 r. URL: http://hudoc.echr.coe.int/rus?i=001–57584 (in Ukrainian)
9. Sprava «Maestri proty Italii» (Zaiava № 39748/98) : Rishennia Yevropeiskoho sudu z prav liudyny vid 17 liut. 2004 r. URL: http://hudoc.echr.coe.int/rus?i=001–61638 57584 (in Ukrainian)

Bibliography

Authored books

1. Hmyrko V. P. *Dokazuvannia v kryminalnomu protsesi: diialnisna paradyhma. Teoretychnyi analiz. Problematyzatsiia. SMD-reprezentatsiia: monohrafiia* [Evidence in the criminal process: an activity paradigm. Theoretical analysis. Problematization. SMD-representation: monograph] (Akad. mytnoi sluzhby Ukrainy, 2010) 179 (in Ukrainian)
2. Lutsyk V V, Samarin V I, *Suchasnyi kryminalnyi protses krain Yevropy : monohrafiia* [Modern criminal process in European countries: monograph] (Pravo, 2018) 792 (in Ukrainian)

Edited books

3. Kaplinoi O. V., Shylo O. H. (red) *Kryminalnyi protses: pidruchnyk* [Criminal process: a textbook] (Pravo, 2019) 584 (in Ukrainian)
4. Shylo O. H. (red) *Kontseptualni osnovy pobudovy suchasnoho kryminalnoho protsesu Ukrainy* [Conceptual foundations of construction of the modern criminal process of Ukraine] (NDI VPZ imeni akad. V. V. Stashysa NAPrNU, 2016) 264 (in Ukrainian)
5. Tolubko V. B. (red) *Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt: pidruchnyk* [Information and cyber security: socio-technical aspect: a textbook] (DUT, 2015) 288

Non-authored books

6. *The Functioning of Courts in the Covid-19 Pandemic. Primer* (OSCE, ODIHR, October 2020) 53 <https://www.osce.org/files/f/documents/5/5/469170.pdf> (in English)
7. *Posibnyk zi statti 6 Konventsii – Pravo na spravedlyvyi sud (kryminalno-protsesualnyi aspekt)* [Guide to Article 6 of the Convention – Right to a fair trial (criminal procedural aspect)] <https://www.echr.coe.int/Documents/Guide_Art_6_criminal_UKR.pdf> (in Ukrainian)

Part of the books

8. Murzanovska A V 'Osnovni tendentsii rozvytku nauky kryminalnoho protsesu v Ukraini v suchasnykh umovakh' *Legal science and education in Ukraine and EU countries: a paradigm shift: Collective monograph* («Baltija Publishing», 2021) 285–310 <http://www.baltijapublishing.lv/omp/index.php/bp/catalog/book/159> (in Ukrainian)

Journal aticles

9. Holovan M. S. 'Kompetentsiia i kompetentnist: dosvid teorii, teoriia dosvidu' [Компетенция и компетентность: опыт теории, теория опыта] (2008) 3 Vyshcha osvita Ukrainy 23–30 <https://core.ac.uk/download/pdf/324272272.pdf>
10. Kalancha I. H. 'Informatsiina bezpeka elektronnoho kryminalnoho provadzhennia Ukrainy' [Information security of electronic criminal proceedings of Ukraine] (2018) 3 Naukovyi chasopys Natsionalnoi akademii prokuratury Ukrainy 11–22 (in Ukrainian)
11. Kamenieva T. 'Mozhlyvosti ta mezhi vykorystannia tsyfrovykh tekhnolohii v sferi kryminalno-protsesualnoi diialnosti' [Protection of individual rights in the aspect of digitalization of criminal proceedings] (2020) 8 (193) Hromadska dumka pro pravotvorennia 17–21 <http://nbuviap.gov.ua/images/dumka/2020/8.pdf> (in Ukrainian)
12. Kislenko D. P. 'Zakhyst prav osoby v aspekti didzhytalizatsii kryminalnoho provadzhennia' [Possibilities and limits of the use of digital technologies in the field of criminal procedural activity] (2021) 29 Naukovi zapysky Lvivskoho universytetu biznesu ta prava. 114–119 (in Ukrainian)
13. Klepka D. I. 'Zdiisnennia sudovoho kontroliu pid chas dosudovoho rozsliduvannia v poriadku dystantsiinoho sudovoho provadzhennia: analiz sudovoi praktyky' [Implementation of judicial control during pre-trial investigation in the order of remote judicial proceedings: analysis of judicial practice.] (2022) 45 Pytannia borotby zi zlochynnistiu 88–97 (in Ukrainian)
14. Pavlova T. O. 'Didzhytalizatsiia yak napriam transformatsii kryminalnoho provadzhennia' [Digitization as a direction of transformation of criminal proceedings] (2021) 41 Pravova derzhava 96 <http://pd.onu.edu.ua/article/view/225612> (in Ukrainian)
15. Tarasenko L 'Pravo na dostup do interenetu' [The right to access the Internet] (2020) 71 Visnyk Lvivskoho universytetu. Seriia yurydychna. 53–61 (in Ukrainian)
16. Tsyhaniuk Yu. V. 'Hermenevtyka sudovykh rishenn u kryminalnomu provadzhenni' [Hermeneutics of court decisions in criminal proceedings] (2021) 4 Dniprovskyi naukovyi chasopys publichnoho upravlinnia, psykholohii, prava. 38–39 <https://chasopys-ppp.dp.ua/index.php/chasopys/article/view/98/89> (in Ukrainian)
17. Seleznova O. M. 'Internet pravo i yoho mistse v systemi informatsiinoho prava' (2013) 2–2 Vcheni zapysky Tavriiskoho natsionalnoho universytetu im. V. Vernadskoho [Internet law and its place in the system of information law] 236–240.< http://www.juris.vernadskyjournals.in.ua/- journals/2013/2-2_2013/35.pdf> (in Ukrainian)

Conference paper

18. Hlynska N. V., Drozdov O. M., 'Ievrointehratsiinyi vektor tsyfrovizatsii kryminalnoho provadzhennia: vyklyky ta shliakhy realizatsii Perspektyvni napriamy rozvytku kryminalnoi yustytsii v tsyfrovu eru : materialy Vseukr. zaoch. nauk.-prakt. konf. (m. Kharkiv, 24 lyp. 2023 r.) 104–117. <https://ivpz.kh.ua/wp-content/uploads/2023/10/Zbirnyk-tez_Perspektyvni-napriamy_2023.pdf> (in Ukrainian)

Websites

19. Kennedy Rónán 'AI: why installing 'robot judges' in courtrooms is a really bad idea' (The Conversation) <https://theconversation.com/ai-why-installing-robot-judges-in-courtrooms-is-a-really-bad-idea-208718> (in English)
20. 'Shtuchnyi intelekt u pravosuddi' [Artificial intelligence in justice] (Tsentr demokratii ta verkhovenstva prava) <https://cedem.org.ua/analytics/shtuchnyj-intelekt-pravosuddia/> (in Ukrainian)

Глинська Н. В., Клепка Д. І.
Принципи визначення розумних меж цифровізації кримінального провадження України

У статті досліджуються засадничі основи процесу цифровізації кримінального провадження. Авторами визначається поняття меж цифровізації кримінального провадження, під якими запропоновано розуміти зумовлені низкою чинників певні «кордони» цифрового оснащення кримінальної процедури та необхідний рівень нормативної адаптації цієї царини до діджиталсередовища. Пошук таких оптимальних меж цифровізації кримінального провадження вимагає формулювання (виокремлення) та розгляд основних положень принципового характеру, сукупність яких є необхідною для врахування в перебігу здійснення цифровізації. Такі принципи своєю чергою

є основою для формулювання похідних від них більш конкретних вимог практичного характеру – стандартів цифровізації кримінального провадження.

На підставі дослідження міжнародних актів та доктринальних напрацювань авторами виокремлено такі стандарти цифровізації кримінального провадження верховенство права; правова визначеність; пріоритетність цифрового формату; гнучкість процесу цифровізації; застосування ризикоорієнтованого підходу; збереження провідної ролі людського фактора при прийнятті кримінальних процесуальних рішень; є прозорість використання цифрових технологій в кримінальному провадженні; покладення відповідальності за ризики, супутні їх застосуванню під час кримінальної процедури, на представників органів кримінальної юстиції; забезпечення інформаційної безпеки (кібербезпеки) кримінального провадження; вимога узгодженості темпів процесу цифровізації з рівнем цифрової компетентності уповноважених осіб.

У висновку зазначається що кожен з визначених нами принципів (стандартів) ЦКП є напрямом окремого предметного дослідження під кутом зору відшукання оптимальних меж цифровізації кримінального провадження. Втім лише комплексне їх дотримання здатне забезпечити права та законні інтереси особи та досягти бажаного результату цифровізації кримінального провадження.

Ключові слова: *кримінальне провадження, цифровізація, права людини, стандарти цифровізації кримінального провадження.*

Glynska N. V., Klepka D. I.

Principles of determining reasonable limits of the digitalization of criminal proceedings in Ukraine

In the article, to examine the basics of the process of digitization of criminal proceedings. The authors define the concept of the limits of the digitalization of criminal proceedings, under which it is proposed to understand certain «borders» of digital equipment of the criminal procedure determined by a number of factors and the necessary level of regulatory adaptation of this area to the digital environment. The search for such optimal limits of digitalization of criminal proceedings requires the formulation (identification) and consideration of the main provisions of a principled nature, the totality of which is necessary to take into account in the course of digitalization. Such principles, in turn, are the basis for the formulation of more concrete requirements derived from them of a practical nature – standards for digitalization of criminal proceedings.

Based on the study of international acts and doctrinal developments, the authors have singled out the following standards of digitalization of criminal proceedings: the rule of law; legal certainty; priority of digital format; flexibility of the digitization process; application of a risk-oriented approach; preservation of the leading role of the human factor in making criminal procedural decisions; there is transparency in the use of digital technologies in criminal proceedings; assigning responsibility for the risks associated with their application during criminal proceedings to representatives of criminal justice bodies; ensuring information security (cyber security) of criminal proceedings; the requirement that the pace of the digitization process be consistent with the level of digital competence of authorized persons.

In the conclusion, it is noted that each of the principles (standards) of the CCP that we have determined is the direction of a separate thematic study from the point of view of finding the optimal limits of digitalization of criminal proceedings. However, only their comprehensive observance can ensure the rights and legitimate interests of a person and achieve the desired result of digitalization of criminal proceedings.

Keywords: *criminal proceedings, digitalization, human rights, standards of digitalization of criminal proceedings.*

Стаття надійшла до редакції:10.05.2024 р.
Прийнята до друку: 20.05.2024 р.