ЗАГАЛЬНІ ПРИНЦИПИ ЩОДО ПРОВЕДЕННЯ ДИСТАНЦІЙНИХ СУДОВИХ ЗАСІДАНЬ

ПОСІБНИК

cepej

European Commission for the Efficiency of Justice

Commission européenne pour l'efficacité de la justice

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

ЗАГАЛЬНІ ПРИНЦИПИ ЩОДО ПРОВЕДЕННЯ ДИСТАНЦІЙНИХ СУДОВИХ ЗАСІДАНЬ

Посібник

Київ
2023

Посібник підготували експерти CEPEJ за підтримки Проєкту Ради Європи «Підтримка судової влади України в забезпеченні кращого доступу до правосуддя», який впроваджує Відділ програм співробітництва Департаменту імплементації стандартів прав людини, правосуддя та правової співпраці:

Джуліо Борсарі (Giulio Borsari) — IT-менеджер, колишній директор Управління з координації технологій, Міністерство юстиції *(Італія)*;

Доктор Александр Паланко (Alexandre Palanco) — доцент Католицького інституту Ліону, юридичний факультет, співавтор Керівництва CEPEJ щодо проведення судових проваджень у режимі відеоконференції *(Франція)*;

Доктор Марек Свєрчинський (Marek Świerczyński) — професор Інституту правових наук Університету кардинала Стефана Вишинського у Варшаві, адвокат, співавтор Керівництва CEPEJ щодо проведення судових проваджень у режимі відеоконференції *(Польща)*.

Цитуючи матеріали цього посібника, необхідно зазначати як джерело «Загальні принципи щодо проведення дистанційних судових засідань», який підготували експерти CEPEJ, Рада Європи, 2023.

Наведену в посібнику інформацію не слід вважати офіційною точкою зору Ради Європи.

Зміст

Додаткові матеріали

ПЕРЕЛІК СКОРОЧЕНЬ

У посібнику терміни мають такі значення:

CEPEJ — Європейська комісія з питань ефективності правосуддя;

Відеоконференція — телекомунікаційна технологія інтерактивної взаємодії двох і більше дистанційних учасників судового процесу з можливістю обміну аудіо- та відеоінформацією в режимі реального часу;

Керівництво CEPEJ — Керівні принципи, ухвалені Європейською комісією з питань ефективності правосуддя (CEPEJ) на її 36-му пленарному засіданні (червень 2021 р.), щодо проведення судових засідань у режимі відеоконференції;

Керівні принципи ODR — Керівні принципи, ухвалені Комітетом міністрів Ради Європи 16 червня 2021 року, щодо механізмів онлайн вирішення спорів у цивільному та адміністративному провадженні;

Керівні принципи щодо електронних доказів — Керівні принципи, ухвалені Комітетом міністрів Ради Європи 30 січня 2019 року, щодо електронних доказів у цивільному та адміністративному провадженні;

Конвенція — Конвенція про захист прав людини і основоположних свобод (Європейська конвенція з прав людини);

Посібник — посібник «Загальні принципи щодо проведення дистанційних судових засідань».

МЕТА ТА СФЕРА ЗАСТОСУВАННЯ

Метою посібника є запровадження ефективних механізмів проведення дистанційних судових засідань, зокрема у разі надзвичайної ситуації та під час воєнного стану. Посібник не встановлює обов'язкових правових стандартів, а містить рекомендації, опис найкращої практики, яку суди можуть застосовувати на власний розсуд.

Посібник може бути використано у цивільному, адміністративному, господарському та кримінальному судочинстві для допомоги в організації дистанційного судового засідання та для забезпечення ефективної реалізації права на справедливий суд, як це визначено Конвенцією.

Оскільки положення законодавства щодо здійснення судочинства в умовах надзвичайної ситуації та під час воєнного стану мають тимчасовий характер, необхідно проводити періодичний перегляд посібника, ураховуючи коментарі відповідних зацікавлених сторін, зокрема представників судової системи, адвокатури, громадянського суспільства, неурядових організацій.

Посібник має таку структуру: перша частина охоплює процедурні питання, що стосуються всіх видів судових проваджень, — у ній зосереджено увагу на особливостях кримінального провадження; друга частина містить організаційні та технічні вимоги до проведення судових засідань у режимі відеоконференції.

У додатках подано перелік кращої практики і відповідні ресурси, що встановлюють європейські принципи стосовно прав людини і стандарти дистанційного правосуддя.

ОСНОВНІ ПРИНЦИПИ

A. Режим надзвичайного стану не позбавляє сторону гарантій справедливого суду.

B. Жодна сторона не повинна бути позбавлена визначеної законом можливості бути заслуханою судом або стежити за процесом. Жодна сторона не повинна перебувати у суттєво невигідному становищі порівняно з іншою стороною.

C. Важливість юридичного представництва має вирішальне значення для справедливого розгляду справи. Суд повинен захищати право сторони на ефективну допомогу адвоката під час усіх судових проваджень, зокрема конфіденційність спілкування.

D. Особливу увагу необхідно приділити дотриманню права на захист у кримінальному провадженні.

Частина І
ПРОЦЕДУРНІ АСПЕКТИ РЕЖИМУ ВІДЕОКОНФЕРЕНЦІЇ З ТОЧКИ ЗОРУ ПРАВА НА СПРАВЕДЛИВИЙ СУД

Керівництво щодо всіх судових проваджень

Рішення про проведення дистанційного судового засідання

Правило 1. Держави повинні забезпечити законодавчу базу, яка надає судам достатні підстави для вирішення питання про те, чи можна або чи потрібно в кожному конкретному випадку проводити дистанційне судове засідання.

1. Суд вирішує питання про можливість проведення судового засідання в режимі відеоконференції за наявності відповідних технічних можливостей.
2. Розглядаючи можливість розгляду справи в дистанційному режимі, суд повинен ураховувати технічні можливості суду, сторін та їх представників, інших учасників.
3. Суд повинен ураховувати обставини груп учасників процесу, які перебувають у вразливому становищі (неповнолітні, особи з інвалідністю тощо), що може перешкоджати особі брати самостійну та/або повноцінну участь у судовому засіданні за допомогою засобів відеоконференцзв'язку.
4. Суд має знати про фізичне місцезнаходження учасників процесу, зокрема про те, чи беруть вони участь у судовому засіданні з території іншої держави або з тимчасово окупованої території України, території проведення воєнних дій.
5. Із міркувань безпеки суд повинен розглянути можливість використання безпечних місць для безпечного підключення як альтернативи фізичної присутності в залах засідання суду. Такі місця, як відділ

поліції, державні адміністративні установи та інші заздалегідь внесені до переліку місця, можуть приймати як усіх учасників судового засідання, так і суддю/працівників суду.

Правило 2. Суд має визначити, ґрунтуючись на положеннях законодавства держави, чи є проведення дистанційного судового засідання розумним та доцільним з урахуванням конкретних обставин справи, та обґрунтувати своє рішення.

Правило 3. Сторони повинні мати можливість обмінятись із судом інформацією з таких питань: i) чи можливо або чи необхідно проводити дистанційне судове засідання у справі; ii) яких конкретних заходів потрібно вжити для проведення дистанційного судового засідання; iii) вирішення проблем безпеки сторін; iv) можливість звернутися до суду з проханням провести судове засідання з особистою присутністю із зазначенням причин.

1. Секретар судового засідання повинен забезпечити належну підготовку до проведення дистанційного судового засідання, а саме:
    a. Перевірити наявність в учасників необхідних технічних можливостей для участі в судовому засіданні;
    b. Надіслати учасникам інформацію про те, як користуватися платформою, а також контактні дані у разі виникнення технічних питань або проблем із доступом до дистанційного судового засідання, якщо такі відомості не були зазначені в судовому рішенні, яким призначено проведення судового засідання в режимі відеоконференції, або якщо сторона, інший учасник справи чи їх представник до моменту проведення судового засідання не отримав відповідного судового рішення;
    c. Завчасно надіслати форми електронною поштою (наприклад, для складання присяги) та облікові дані для підключення до судового засідання, якщо необхідно;
    d. Запропонувати учасникам перевірити з'єднання перед проведенням судового засідання, зокрема провести пробний сеанс зв'язку в день судового засідання;
    e. Попросити всіх учасників приєднатися до сеансу зв'язку або увійти в обліковий запис за короткий час до початку судового засідання.
2. Суд повинен:
    a. Розглянути питання про скорочення днів судових засідань з урахуванням різних часових поясів і врахувати, що дистанційні судові засідання потребують підвищеної концентрації уваги від учасників;

b. Розглянути можливість робити перерви, щоб сторони й адвокати, які фізично не знаходяться в одному місці, могли провести приватну консультацію;

c. Визначити порядок, у якому будуть заслуховувати свідків та експертів, а також час і спосіб запрошення їх до дистанційної зали судових засідань.

3. Перед початком судового засідання учасник провадження повинен надати суду всі необхідні документи для розгляду справи, зокрема копію документа, що посвідчує особу, документи, які підтверджують повноваження представника його інтересів, якщо їх не містять матеріали справи.

Правило 4. Рішення повинно підлягати перегляду компетентним органом відповідно до національного законодавства.

1. Згідно з національним законодавством рішення про проведення дистанційного судового засідання не підлягає перегляду окремо від рішення, ухваленого по суті справи.

Право на ефективну участь

Правило 5. Суд має надати учасникам можливість перевірити якість звуку та зображення або до початку судового засідання (наприклад, виконавши самоперевірку), або на його початку, щоб кожен учасник міг ознайомитися з особливостями платформи для проведення відеоконференції.

1. Технічні засоби та технології, які використовують суд та учасники, повинні мати належну якість зображення та звуку, а також забезпечувати інформаційну безпеку.

2. Учасники судового процесу повинні мати можливість чути й бачити хід судового засідання, ставити запитання та отримувати на них відповіді, реалізовувати інші процесуальні права й обов'язки.

3. Стислість і точність мають вирішальне значення під час дистанційних судових засідань. Сторонам рекомендується максимально викладати свої доводи та аргументи письмово, особливо у випадку складної доказової бази.

Правило 6. Під час дистанційного судового засідання суд повинен мати змогу постійно відстежувати якість зображення та звуку відеозв'язку, щоб звести до мінімуму кількість технічних несправностей, які можуть вплинути на право сторін брати активну участь у провадженні.

1. Суд повинен уважно стежити за тим, щоб усі учасники були присутні в судовому засіданні й могли стежити за його перебігом, наприклад, перевіряти, чи не переривається зв'язок (завис екран), і швидко та належним чином реагувати, якщо виникають проблеми.

2. Секретар судового засідання здійснює поточний контроль якості звуку та зображення, а також контролює роботу технічних засобів відеозапису шляхом спостереження за їх роботою.

3. На вимогу судді/головуючого судді відповідальний працівник суду повинен вимикати мікрофон.

Правило 7. Суд має забезпечити можливість бачити й чути трансляцію для всіх учасників провадження, а також для представників громадськості, якщо судове провадження проводиться у відкритому форматі.

1. Якщо в суду виникнуть побоювання, що якість зв'язку негативно впливає на судове засідання, про цю ситуацію слід негайно повідомити учасників.

2. У суду може виникнути потреба повторити те, що щойно відбулося, якщо учасник не міг стежити за процесом. Якщо якість звуку чи відео значно погіршується під час запитання чи надання аргументів, може знадобитися їх повторення, тому процес набагато легше провести за допомогою стислих запитань чи аргументів.

3. Суд має попросити сторони повідомляти про будь-які проблеми щодо організації або проведення дистанційного судового засідання.

Правило 8. Під час ухвалення рішення про проведення дистанційного судового засідання і його практичних аспектів суд має враховувати обставини та труднощі осіб, які перебувають у вразливому становищі, як-от діти, мігранти або особи з інвалідністю.

1. Під час судового засідання слід подбати про захист осіб, які перебувають у вразливому становищі, зокрема осіб із вадами психічного розвитку, з урахуванням поваги до їхньої гідності та інтересів.

2. Суд повинен урахувати, наскільки система відеоконференцзв'язку доступна для осіб з інвалідністю (наприклад, з вадами зору, слуху, психічними розладами тощо) або інших уразливих осіб.

3. Під час розгляду справи в закритому судовому засіданні (наприклад, у сімейних справах) мають бути присутніми лише сторони та інші особи, яким суд надав дозвіл бути присутніми.

Правило 9. Суд має оголосити перерву в судовому засіданні в разі виникнення технічної несправності до моменту її усунення, залежно від її характеру. Таке зупинення має бути відображено в протоколі дистанційного судового засідання.

1. Відповідно до національного законодавства учасник справи, який подав відповідне клопотання, несе ризик відсутності технічної можливості підключитись до дистанційного судового засідання поза приміщенням суду, переривання підключення тощо.
2. На початку дистанційного судового засідання суд повинен повідомити учасникам, як саме вони можуть повідомляти про виникнення непередбачених технічних проблем під час дистанційного судового засідання й до кого мають звертатися в такому разі.
3. У разі переривання зв'язку має бути встановлена процедура, за якою всі, кого це стосується, зокрема свідки й експерти, можуть за допомогою додаткових засобів повідомити суд про проблему, що виникла (наприклад по телефону, через текстове повідомлення, електронну пошту).

Ідентифікація та приватність

Правило 10. Усі учасники дистанційного судового засідання мають бути ідентифіковані судом. Засоби ідентифікації мають бути чітко визначені в законодавстві й не бути надмірно інтрузивними або обтяжливими.

1. Кожна особа повинна представитися, повідомити, чи присутні з нею в приміщенні інші особи, а також сповістити, якщо вони чи будь-які інші особи увійдуть у приміщення або вийдуть із нього. Суд може розглянути можливість надання учасниками скан-копії документа, що посвідчує особу, перед початком судового засідання.
2. Відповідно до національного законодавства особа учасника справи підтверджується за допомогою електронного підпису, а якщо особа не має такого підпису, то у порядку, визначеному Законом України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» або Державною судовою адміністрацією України (частина четверта статті 197 Господарського процесуального кодексу України).
3. Суд має розглянути різні варіанти перевірки особи учасників дистанційного судового засідання, такі як:
    a. Показати на камеру документ, що посвідчує особу, або паспорт. Якщо є сумніви або документ чітко не видно, судове засідання не слід продовжувати, поки проблему не буде вирішено.

b. Попросити учасників надіслати суду скан-копії документів, що посвідчують особу, або паспортів до початку судового засідання. Далі їх можна порівняти з документами, які учасники показують на камеру на початку судового засідання, що дасть суду змогу порівняти та підтвердити відповідні версії документів. За подачу неправдивих документів особи, які їх подають, несуть відповідальність, установлену законом.

c. Попередня реєстрація з використанням відповідного документа, що посвідчує особу. Учасник може зареєструватися онлайн за допомогою електронного підпису, через національну базу даних або іншу цифрову платформу. Після верифікації особи судове засідання можна продовжити. У такому разі кожен учасник дистанційного судового засідання окремо приєднується до судового засідання в режимі відеоконференції поза межами приміщення суду з використанням власних технічних засобів та електронного підпису.

d. Підтвердження з офісу нотаріуса/адвоката або іншого органу. Учасник може бути присутнім на дистанційному судовому засіданні з офісу адвоката. Це рішення забезпечує як підтвердження особи, так і безпечне середовище для участі особи в судовому засіданні.

e. Ідентифікація поліцією. Поліція може ідентифікувати учасника, який перебуває вдома, наприклад, на початку дистанційного судового засідання.

f. Впізнання сторонами або свідками. За відсутності іншого способу ідентифікації в розпорядженні суду інші учасники, за можливості, можуть ідентифікувати особу та підтвердити її. Неправдиві заяви караються законом. Кожен має право заявити, що в судовому засіданні присутня інша особа (поставити проведену ідентифікацію під сумнів).

Правило 11. Приватність учасників дистанційного судового засідання має бути належно захищена і суд має вживати заходів для зниження ризиків для неї. Потрібно вжити всіх необхідних заходів щодо усунення будь-якого ризику порушення права сторін на повагу до приватності.

1. Приватність і безпека є невід'ємними умовами справедливого судового розгляду.

2. Суд має дозволяти участь у дистанційному судовому засіданні лише особам із затвердженого або попередньо зареєстрованого списку за умови дотримання заздалегідь узгоджених умов щодо публічного характеру судового засідання.

3. Список учасників, їхні ПІБ, професійна належність і відомості про місця, із яких вони братимуть участь у судовому засіданні, мають бути заздалегідь узгоджені та надані сторонам.

4. Якщо судове засідання є відкритим і/або його висвітлюватимуть медіа, учасників слід заздалегідь повідомити про це.

5. Секретар судового засідання повинен переконатися у відсутності осіб, які незаконно (несанкціоновано) підключилися до дистанційного судового засідання, переглянути список підключених осіб і перевірити його відповідність списку учасників судового процесу та осіб, яких допущено до спостереження за судовим засіданням, а також їхню кількість.

Публічність і запис

Правило 12. Суд має зберегти публічний характер дистанційного судового засідання через створення цілісної процедури участі громадськості. Публічність дистанційного судового засідання можна забезпечити, наприклад, дозволивши громадськості приєднатися до дистанційного судового засідання в реальному часі або розмістивши його записи на вебсайті суду.

1. Доступ громадськості, якщо він передбачений національним законодавством, має бути забезпечений навіть під час надзвичайного стану. Суд має враховувати як вимоги законодавства, так і технічні можливості для проведення відкритого судового засідання.

2. Дистанційне спостереження має бути дозволеним, якщо це відповідає інтересам правосуддя; воно не може дозволятись, якщо це шкодить правосуддю у справі, яку розглядає суд. Суди повинні враховувати існування таких ризиків у справі, яка розглядається, і заздалегідь оцінити, чи буде віддалений доступ в інтересах правосуддя. Це має бути відображено в судових рішеннях і в змісті будь-яких настанов, які він надає.

3. Представники медіа можуть допомогти з онлайн-доступом до судового засідання. Суд також може розглянути можливість створення безпечного каналу підключення для журналістів, які зможуть у такий спосіб стежити за судовим засіданням.

Правило 13. Заборонено фотографування, записування, транслювання чи в інший спосіб поширення будь-якої частини дистанційного судового засідання (разом із аудіозаписами) без попереднього дозволу суду.

1. На початку судового засідання суд повинен пояснити спостерігачам, зокрема громадськості та медіа, що несанкціонований запис або трансляція судового засідання є незаконним.

Свідки та експерти

Правило 14. У межах, дозволених національним законодавством, допит свідків та експертів під час дистанційного судового засідання має проводитися в порядку, максимально наближеному до практики їх допиту в залі засідання суду.

1. Суд повинен залишатися пильним, активним і чуйним до потреб і проблем свідків, які дають показання дистанційно.
2. Свідок або експерт може брати участь у судовому засіданні за допомогою відеозв'язку тільки із зали судових засідань (приміщення) суду.
3. Якщо свідки перебувають у вразливому становищі, суд повинен розглянути можливість присутності осіб, які можуть запропонувати їм професійну підтримку.
4. Якщо немає достатніх гарантій безпечності середовища для свідка, суд також повинен розглянути можливість зупинити або відкласти судове засідання.
5. Якщо зв'язок поганий, суд має розглянути можливість припинити надання показань і відкласти судове засідання, доки з'єднання не стане безпечним і стабільним.
6. Присяги, урочисті заяви чи декларації можна проводити за допомогою відеозв'язку. Особа, яка складає присягу, робить урочисту заяву чи декларацію, і повинна підписати документ. Документ можна відсканувати або сфотографувати й надіслати до суду в електронній формі.
7. Під час допиту свідків та експертів суд повинен дотримуватися Керівних принципів щодо електронних доказів, викладених у розділі щодо отримання усних показань за допомогою дистанційного зв'язку (керівні принципи 1–5).

Правило 15. Слід ретельно продумати відповідні організаційні заходи, щоб забезпечити цілісність дистанційних засідань та уникнути тиску або впливу на свідків чи експертів під час таких засідань.

1. Якщо учасник, який бере участь у судовому засіданні дистанційно, є свідком, суд повинен розглянути автентичність, надійність і достовірність показань свідка, а також відсутність впливу з боку інших осіб.
2. Якщо суд має сумніви щодо втручання в показання свідка, суд може розпорядитися про надання свідком показань з офіційно зареєстрованого місця, наприклад з приміщення суду, іншого відповідного державного органу, офісу адвокатів відповідної сторони або посередників.

3. Суд може використати такі варіанти для зменшення ризику неправомірного втручання в оцінку достовірності показань свідка.

   a. Попросити свідка «показати» приміщення, у якому він перебуває, повернувши камеру на своєму пристрої. За потреби цю процедуру можна повторювати протягом судового засідання.

   b. Попросити свідка дати показання з приміщення, у якому є лише одні двері, а потім подбати про те, щоб під час судового засідання камера була сфокусована на цих дверях. У такому разі суд зможе закликати будь-яку особу, яка увійде до приміщення, негайно його залишити.

   c. Попросити свідка сісти подалі від екрана, щоб він не міг читати будь-які матеріали з комп'ютера. Якщо існує ризик того, що свідок міг читати з підготовленого сценарію, суд може поставити йому запитання, щоб з'ясувати, чи це так.

   d. Надати свідку можливість конфіденційно спілкуватися в чаті, по мобільному телефону чи за допомогою іншого електронного пристрою, щоб у разі виникнення ризику того, що свідок міг читати з підготовленого сценарію, свідок міг безпосередньо спілкуватися з судом.

   e. Використовувати окремі «кімнати» на платформі, у яких свідки можуть очікувати, перш ніж суд дозволить їм «увійти» до судового засідання.

   f. Пояснити, як саме свідки й інші учасники можуть привернути увагу суду під час судового засідання (наприклад, за допомогою жестів рук, за допомогою функції «чат», ставлячи запитання безпосередньо суду тощо).

Докази

Правило 16. Суд має надати вказівки щодо процедури, яких учасники повинні дотримуватися для подання документів або інших матеріалів під час дистанційного судового засідання.

1. За потреби суд повинен надати сторонам вказівки щодо процедури й забезпечити технічні умови для обміну такими доказами та їх використання.

2. Доступ до доказів, які подають та зберігають у цифровій формі, має бути контрольованим, а точки доступу до них — обмеженими.

3. Суд має бути обізнаним у питаннях, пов'язаних з електронними доказами, як сторони мають подати суду відомості в безпечний спосіб.

4. Дотримання належної практики поводження з електронними доказами є важливим для забезпечення захисту доказів як від навмисної, так і від ненавмисної зміни.

Правило 17. Слід вжити організаційних заходів, щоб забезпечити можливість для всіх учасників бачити та/або чути матеріали, подані під час дистанційного судового засідання.

1. Докази та відповідні матеріали мають бути надані сторонам у доступний і належний спосіб.
2. Суд має дозволити подання електронних доказів в електронній формі.

Правило 18. Подання нових заяв, аргументів та/або доказів під час дистанційного судового засідання має відповідати принципу змагальності, суд має забезпечити право подання зустрічних доказів.

1. Опрацювання нових заяв, аргументів та/або доказів не має бути невигідним для сторін або надавати несправедливу перевагу одній з них.
2. Суд повинен завжди оцінювати достовірність доказів, зокрема їх джерело.
3. Електронні докази повинні оцінюватися так само, як і інші види доказів, зокрема щодо їх належності, допустимості, достовірності, вірогідності, точності та цілісності.

Перекладачі

Правило 19. Якщо під час дистанційного судового засідання виникає потреба в перекладачеві, перевага віддається присутності перекладача поряд із учасником, який не володіє мовою суду.

1. Слід докласти зусиль для постійного залучення перекладачів, коли вимагається використання їхніх послуг, та впевненого висловлення ними проблем, що виникають. Перекладач має право ставити запитання для уточнення перекладу.
2. Суд має вирішити питання щодо конфіденційних і відокремлених каналів зв'язку до початку дистанційного судового засідання.

Правило 20. Перекладач повинен мати належний візуальний контакт з особою, мовлення якої перекладає, протягом усього судового засідання.

1. Особа, чиє мовлення перекладають, повинна підтримувати зоровий контакт із камерою та сидіти на такій відстані від неї, щоб її було добре видно. Не слід сидіти спиною до вікна чи іншого джерела світла.

Окремі правила щодо кримінальних проваджень

Легітимна мета

Правило 21. Якщо законодавство не вимагає отримання вільної інформованої згоди обвинуваченого, рішення суду щодо його або її участі в дистанційному судовому засіданні повинно мати легітимну мету.

1. Оскільки національне законодавство не вимагає отримання вільної інформованої згоди обвинуваченого, рішення суду щодо його або її участі в дистанційному судовому засіданні повинно мати легітимну мету.

Правило 22. Легітимна мета проведення дистанційного судового засідання у межах кримінального провадження має ґрунтуватися на таких цінностях, як охорона громадського порядку, охорона здоров'я, запобігання вчиненню правопорушень і захист права на життя, свободу, захист свідків і потерпілих від злочинів. Суд може розглядати питання дотримання права на справедливий розгляд справи упродовж розумного строку, зокрема, на наступних стадіях провадження після розгляду справи в суді першої інстанції.

1. Мета проведення дистанційного судового засідання може бути визнана легітимною у зв'язку з надзвичайним і воєнним станом у випадку:
   a. Збереження здоров'я та життя учасників у разі бомбардування або ризику бомбардування.
   b. Збереження життя представників влади та ув'язнених шляхом уникнення переміщення.
   c. Руйнування судової інфраструктури.
   d. Руйнування дорожньої інфраструктури.
   e. Відсутності обладнання або людських ресурсів для забезпечення безпечного переміщення.
2. У кожному окремому судовому рішенні стосовно проведення дистанційного судового засідання в кримінальному провадженні має бути зазначена причина такого вибору. Сторони мають бути проінформовані про ці причини.
3. Дистанційні судові засідання можуть обмежуватися досудовим провадженням або апеляційним судовим провадженням за умови, що можуть проводитися очні засідання.

Активна участь обвинуваченого

Правило 23. Відеозв'язок, що забезпечується, має давати обвинуваченому змогу бачити й чути учасників дистанційного засідання, зокрема інші сторони, суддів, свідків та експертів. Учасники повинні мати змогу бачити й чути обвинуваченого.

1. Суд повинен забезпечити під час дистанційного судового засідання таке:
    a. Можливість бачити й чути трансляцію для всіх учасників провадження, а також для представників громадськості, якщо судове засідання проводять у відкритому форматі.
    b. Можливість для обвинуваченого бачити й чути учасників дистанційного судового засідання, зокрема інші сторони, суддів, свідків та експертів.
    c. Можливість для учасників бачити й чути обвинуваченого.
2. Під час дистанційного судового засідання слід застосовувати такі принципи щодо зображення:
    a. Обличчя особи, яка говорить (суддя, обвинувачений, перекладач, адвокат), завжди має бути видно на екрані.
    b. Кадрування має бути чітким та якісним щодо обвинуваченого (наприклад, слід уникати неприємних ракурсів, контурного освітлення або спотворень, через які обличчя особи не видно).
    c. І захисник, і обвинувачений можуть у будь-який час висловити зауваження щодо кадрування та вимагати внесення змін.
3. Вимоги, викладені в пунктах 1 і 2, передбачають:
    a. Використання високоякісного обладнання (наприклад, камера й мікрофон) або, якщо є, спеціального обладнання (наприклад, камера автоматичного відстеження, мікрофон із заглушенням фонового шуму).
    b. Регулярне тестування поза судовим засіданням, а також перед кожним судовим засіданням.
    c. Участь кваліфікованого персоналу.

Правило 24. Суд має реагувати на технічні несправності, про які повідомляє обвинувачений. Перед початком дистанційного судового засідання обвинувачений має бути поінформований про порядок повідомлення головуючому судді про технічні несправності.

1. Можуть бути обрані різні процедури, які дають обвинуваченому чи його захиснику змогу повідомляти про технічну несправність, але їх

потрібно пояснити обвинуваченому чи його захиснику перед початком судового засідання. Наприклад:

a. Повідомлення про несправність безпосередньо до суду.

b. Призначення відповідальної посадової особи, яка перебуватиме поряд з обвинуваченим.

c. Сигнальна кнопка сповіщення в інтерфейсі засобу відеозв'язку.

2. Усі повідомлення обвинувачених про технічні несправності вносять до протоколу судового засідання.

3. Кожну технічну несправність фіксують у протоколі судового засідання із зазначенням таких відомостей:

a. Характер несправності.

b. Тривалість несправності.

c. Характер втручання.

4. У разі виникнення технічної несправності суд має розглянути такі варіанти подальших дій:

a. Відновити судове засідання (якщо несправність буде усунена в розумний строк).

b. Перенести судове засідання (якщо несправність не усунена).

Це рішення також фіксують у протоколі судового засідання.

Правило 25. У разі постійної неприйнятної поведінки обвинуваченого суд має спершу повідомити йому про право суду вимкнути звук, перервати або призупинити сеанс відеозв'язку з обвинуваченим, перш ніж ухвалювати рішення про це.

1. Суд повинен забезпечити дотримання учасниками загальних правил судового етикету й належної практики, зокрема, таких їх аспектів:

a. Як звертатися до судді та інших учасників.

b. Як попросити надати слово.

c. Правила щодо формату та послідовності проведення судового засідання.

2. Слід нагадати сторонам про загальні правила, зокрема, правила прийнятної поведінки та судовий етикет.

3. Суд повинен попередити учасників про наслідки неприйнятної поведінки, перш ніж застосовувати санкції.

4. Якщо обвинувачений поводиться неналежним чином, суд повинен повідомити йому про таке:

a. Можливість застосування санкцій.

b. Санкції, які можуть бути застосовані (повноваження вимкнути звук з мікрофона обвинуваченого, призупинити його участь у сеансі відеозв'язку або відключити його).

Якщо обвинувачений продовжує поводитися неналежним чином незважаючи на попередження суду, можна застосувати санкції.

Правило 26. У разі вимкнення звуку від обвинуваченого суд має забезпечити його захиснику можливість і надалі реалізовувати право на правничу допомогу під час дистанційного судового засідання і провадження загалом.

1. Перед вимкненням звуку, призупиненням участі обвинуваченого або відключенням його від сеансу відеозв'язку суд повинен гарантувати, що право обвинуваченого на правничу допомогу не буде суттєво й безповоротно порушено.
2. Будь-які санкції, застосовані до обвинуваченого, мають бути пропорційними його поведінці, а також мають бути внесені до протоколу судового засідання.
3. У своєму рішенні про вимкнення звуку, призупинення участі обвинуваченого в сеансі відеозв'язку або його відключення суд повинен ураховувати таке:
   a. Той факт, що обвинувачений уже дав або ще не дав показання під час судового засідання чи на попередньому етапі провадження.
   b. Той факт, що обвинувачений може або не може продовжувати приватне спілкування зі своїм захисником.
4. Якщо обвинувачений не має захисника, суд повинен призначити йому захисника і відкласти судове засідання на строк, необхідний для того, щоб захисник міг підготуватися до захисту обвинуваченого.

Представництво інтересів

Правило 27. Обвинувачений повинен мати ефективний доступ до представництва своїх інтересів перед початком дистанційного судового засідання і під час його проведення, разом із правом до початку судового засідання конфіденційно спілкуватися зі своїм захисником.

Правило 28. Суд має перенести або призупинити дистанційне судове засідання в разі відсутності захисника обвинуваченого і вжити всіх необхідних заходів щодо забезпечення дотримання права обвинуваченого на захист, разом із можливим призначенням захисника *ex officio*.

1. За відсутності захисника обвинуваченого під час судового засідання змішаного типу може бути застосовано такі варіанти (коли всі учасники, крім обвинуваченого, присутні в залі судового засідання):
    a. Обвинуваченому допомагає один захисник, який фізично присутній у залі засідання суду. У цьому разі обвинувачений повинен мати можливість спілкуватися зі своїм захисником через захищену лінію зв'язку.
    b. Обвинуваченому допомагають два захисники: один — фізично присутній на судовому засіданні, другий — поряд з обвинуваченим, щоб допомагати йому.
2. Якщо обвинувачений перебуває у вразливому становищі (наприклад, є особою з інвалідністю, неповнолітньою особою, не володіє мовою суду), слід віддати перевагу другому варіантові.
3. Якщо судове засідання проводять повністю в дистанційному режимі, перевагу слід віддавати фізичній присутності захисника поряд з обвинуваченим.
4. Захисник завжди повинен мати можливість фізично зустрітися з обвинуваченим перед судовим засіданням.

Правило 29. Обвинувачений повинен мати право радитися із захисником і обмінюватися конфіденційною інформацією без нагляду. Присутність інших осіб у приміщенні, у якому обвинувачений перебуває під час такого обміну, не допускається.

1. Присутність співобвинувачених, співкамерників, тюремних охоронців або будь-якої іншої третьої особи під час спілкування обвинуваченого та його захисника через захищену лінію зв'язку є порушенням права на конфіденційність такого спілкування.
2. Дотримання цих вимог має передбачати:
    a. Наявність приміщення, спеціально обладнаного для того, щоб залишити обвинуваченого наодинці в повній безпеці.
    b. Положення, що передбачає покарання за перехоплення такої розмови, незалежно від її змісту або дати виявлення перехоплення.

Правило 30. Обвинувачений повинен мати право спілкуватися із захисником за допомогою захищеної системи. Слід забезпечити конфіденційність такого спілкування обвинуваченого. Використання захищеної лінії зв'язку, яка є окремою від лінії відеозв'язку, за допомогою якої проводять дистанційне судове засідання, має бути захищене привілеєм на збереження адвокатської таємниці.

1. Слід сприяти спілкуванню між обвинуваченим і його/її захисником під час дистанційних судових засідань і забезпечувати його захист.
2. Слід віддавати перевагу спілкуванню через захищену лінію зв'язку, яка є окремою від лінії відеозв'язку, за допомогою якої проводять судове засідання (наприклад, по телефону або через іншу платформу, ніж та, яку використовує суд). В іншому разі обвинувачений може мати достатні підстави почуватися некомфортно під час спілкування зі своїм адвокатом.
3. Якщо обрано використання тих самих платформ, вони повинні мати відповідні функції для забезпечення приватного спілкування, такі як кімната для обговорення (яка може мати функцію таймера або кнопку сповіщення, щоб повідомити обвинуваченого та його/її представника про відновлення судового засідання).
4. Не слід віддавати перевагу варіанту, за якого суд просто оголошує коротку перерву, під час якої інші учасники мають залишити платформу. У разі використання цього варіанта обвинувачений може мати вагоміші підстави вважати, що розмову можуть перервати, відстежувати або записувати.
5. Під час судового засідання можна додатково надати обвинуваченому і його/її захиснику можливість спілкуватися в приватному чаті.

Правило 31. Слід вжити спеціальних організаційних заходів щодо забезпечення захисту конфіденційності спілкування між обвинуваченим і захисником у разі використання послуг перекладача під час такого спілкування.

1. Слід віддавати перевагу присутності перекладача поруч з обвинуваченим, який не володіє мовою суду, щоб зберегти конфіденційність спілкування між обвинуваченим і його/її захисником.

Частина II
ОРГАНІЗАЦІЙНІ ТА ТЕХНІЧНІ АСПЕКТИ РЕЖИМУ ВІДЕОКОНФЕРЕНЦІЇ

Основні вимоги

Фінансування та ресурси

Правило 32. Державам рекомендовано надавати достатнє фінансування та ресурси для забезпечення ефективного проведення судових проваджень у режимі відеоконференції.

1. Залежно від типу обраної інфраструктури (загальнодоступне хмарне середовище або технічне рішення з локальним розташуванням) фінансування та ресурси повинні передбачати витрати на таке:
   a. Програмна платформа.
   b. Аудіовізуальні пристрої (мікрофони, колонки, відеокамери тощо) для окремих учасників та для залів засідань суду.
   c. Пропускна здатність з'єднання.
   d. Навчання та допомога.
   e. Апаратна інфраструктура (якщо технічне рішення розміщене локально).
   f. Експлуатація та обслуговування інфраструктури (якщо технічне рішення розміщене локально).
2. Програмна платформа для дистанційних судових засідань повинна відповідати таким вимогам:
   a. Простота використання.
   b. Надійність.
   c. Забезпечення належного зображення судді, зали засідань суду та учасників на екрані комп'ютера.

d. Бути достатньо безпечною з точки зору порушень безпеки.

e. Надання спеціальних інструментів, за допомогою яких суддя може контролювати процедури та запобігати зловживанням.

f. Надання кожній стороні рівних можливостей для участі.

g. Надання судді та сторонам змоги контролювати процес допиту свідка.

h. Можливість керувати дистанційними судовими засіданнями кількома мовами (існують значні технічні проблеми і не всі платформи мають таку можливість).

3. Під час вибору платформи також може бути корисно враховувати таке:

a. Чи надає вона суду аналогічні способи керування процесом або більшу їх кількість, ніж недистанційне судове засідання.

b. Яка потужність сервера потрібна для ефективної роботи.

c. Які вона має функції для запису сеансів зв'язку.

d. Чи створюється окремий файл після кожної паузи, зокрема, чи дає програма змогу призупиняти та продовжувати запис.

e. Де зберігають записи (на локальному комп'ютері чи в хмарі).

f. Спосіб запрошення учасників (наприклад, електронною поштою).

g. Чи існує можливість вимкнути та ввімкнути звук мікрофонів окремих учасників.

h. Чи існує функція чату.

i. Час, на який можна запланувати судове засідання (наприклад, заздалегідь мінімальний/максимальний час).

j. Наскільки вона є доступною для осіб з інвалідністю (наприклад, з вадами зору, слуху, психічними розладами тощо) або для інших осіб уразливих категорій.

k. Як надають послуги транскрибування, письмового перекладу й усного перекладу.

l. Чи може платформа забезпечувати пряму трансляцію чи вебтрансляцію під час судових засідань, які вважаються відкритими, і чи має вона засоби для передачі трансляції медіа.

Реалістичність судового засідання

Правило 33. Держави мають забезпечувати максимально наближене до реалістичного проведення судових засідань, зокрема повноцінне спілкування та взаємодію всіх сторін процесу з особою, яку вони мають вислухати.

1. Усі учасники дистанційного судового засідання, зокрема суд, сторони та їхні представники, повинні мати технічні можливості для повноцінної участі в ньому.
2. Потрібно підтвердити, що учасники мають доступ до необхідних технічних засобів, щоб забезпечити їхню повноцінну участь. Основні елементи:
    a. Пропускна здатність: швидкість підключення до інтернету (відображається в обсязі даних, які можна передати за фіксований проміжок часу).
    b. Аудіообладнання: мікрофон і колонки.
    c. Візуальне обладнання: відеокамера.
3. Зала засідання суду повинна бути належним чином обладнана високошвидкісним підключенням і високоякісними пристроями, щоб кожного з учасників можна було добре чути й бачити без перешкод.
4. Щодо підключення рекомендовано виділити для відеоконференцій достатню пропускну здатність внутрішньої мережі, у той же час аудіовізуальні пристрої повинні дозволяти чітко чути й бачити того, хто говорить у відповідний момент. Для цієї останньої мети мікрофони, колонки та відеокамери мають бути належної якості.

    Стосовно учасників, які беруть участь у засіданні дистанційно, слід ураховувати таке правило:

Правило 34. Суд має попросити учасників забезпечити надійний відеозв'язок достатньої якості та належну видимість і освітлення для ефективної участі в дистанційному судовому засіданні.

1. Якщо в учасника, який бере участь у судовому засіданні дистанційно, виникають проблеми або в нього немає необхідного технічного обладнання, слід знайти альтернативи, наприклад скористатися приміщенням адвокатської фірми чи іншими обладнаними залами засідань суду.
2. Якщо під час судового засідання поганий зв'язок, суддя повинен розглянути можливість зупинити судове засідання та відкласти його до того часу, поки з'єднання не стане надійним і стабільним.

Інструкції для учасників

Чіткі правила, інструкції та/або навчальні матеріали

Правило 35. Суд має надати учасникам чіткі правила, інструкції та/або навчальні матеріали щодо використання засобів відеозв'язку та проведення дистанційного судового засідання. Рекомендовано підготувати інформаційні матеріали не лише в текстовому форматі, а й у вигляді коротких відео. Слід розглянути можливість створення індивідуальних навчальних матеріалів або курсів щодо використання платформи. Учасникам слід нагадати, що вони постають перед судом і повинні поводитися належним чином згідно з вимогами чинного законодавства, належною практикою і судовим етикетом, які потрібно адаптувати для застосування під час дистанційних судових засідань.

1. Деякі учасники можуть бути недостатньо обізнаними з програмним забезпеченням чи іншими технічними елементами, тож можуть не розуміти, як брати участь у судовому засіданні. Тому вкрай важливо чітко поінформувати їх перед початком судового засідання, щоб уникнути запитань і проблем під час судового засідання або принаймні звести їх до мінімуму.
2. Інструкції мають бути загальнодоступними (наприклад, розміщуватися на вебсайті суду), а також супроводжуватися навчальними відео.

Завчасне повідомлення

Правило 36. Суд має завчасно повідомити учасників про технічні вимоги, зокрема дату, час (з урахуванням різних часових поясів), місце та умови проведення дистанційного судового засідання.

1. Зазвичай виклик на судове засідання містить повістка або інший офіційний документ, створений у системі керування справами. У цьому разі виклик має містити додаткову інформацію щодо проведення дистанційного судового засідання, а саме:
   a) Вказівки, зокрема, щодо таких аспектів:
      - Процедура входу, а також процедура попередньої реєстрації, якщо застосовується.
      - Чи перед входом є кімната очікування.
      - Процедура ідентифікації: наприклад, учасника можуть попросити заздалегідь надати відсканований документ, що посвідчує особу.
      - Дата й час пробного сеансу.

- Коли потрібно завчасно приєднатися до судового засідання.
- Як попросити надати слово.
- Спілкування між учасниками провадження.

b) Технічні вимоги, наприклад:

- Бажано, щоб учасники приєднувалися з використанням стабільного підключення до інтернету через локальну мережу LAN/Ethernet, а не через Wi-Fi, про що їх слід попередити заздалегідь.
- Суд має попросити учасників забезпечити наявність надійного відеозв'язку достатньої якості та належну видимість і освітлення для ефективної участі в дистанційному судовому засіданні.

c) Правила поведінки та етикету, наприклад, щодо:

- Належного зовнішнього вигляду (особливо для учасників, які приєднуються з дому).
- Офіційної мови та фраз, які слід використовувати.

d) Відповідні попередження та застереження, наприклад, щодо:

- Використання функції вимкнення звуку, щоб припинити перебивання або непристойну/неналежну поведінку.
- Запис і стенограмування.

e) Обмеження, наприклад, щодо несанкціонованого запису або транслювання, разом із зображеннями.

f) Посилання для підключення до дистанційного судового засідання.

g) Контактні дані у разі виникнення технічних питань чи інших проблем перед початком судового засідання або під час нього.

2. Для показань свідків слід передбачити спеціальні вказівки, наприклад:

a. Для уникнення надмірного впливу або втручання.

b. Щоб у приміщенні більше нікого не було: можна дати вказівку «показати» приміщення, у якому перебуває особа, утримуючи та повертаючи камеру на своєму пристрої, і встановити камеру так, що вона була сфокусована на одних дверях.

c. Сидіти подалі від екрана, щоб особа не могла читати готовий сценарій.

d. Щодо вжиття спеціальних заходів для захисту конфіденційності (спотворення голосу, розмиття/викривлення/дезактивація зображення тощо), а також щодо дозволу свідку безпосередньо та приватно спілкуватися із суддею, якщо в нього виникли сумніви.

e. Про те, як надати показання в письмовій формі.

3. Якщо запрошення надсилають електронною поштою, необхідно зібрати електронні адреси всіх учасників; якщо учасник не має електронної адреси, його/її можна попросити створити й надати її. Також необхідно перевірити правильність доставки електронних листів одержувачам.

4. Призначаючи час судового засідання, суд має враховувати ту обставину, що сторони можуть приєднуватись з інших часових поясів або інших юрисдикцій.

5. Що стосується тривалості судового засідання, слід пам'ятати, що технічні проблеми, затримки, необхідність пояснювати процедуру, потреба повторювати заяви в разі погіршення зв'язку, необхідність робити часті перерви — це чинники, які можуть вплинути на час.

6. Якщо доступ у режимі реального часу можливий і дозволений для широкої громадськості та медіа, слід надати відповідні вказівки. Є два можливих варіанти:

    a. Через прямі трансляції в потоковому режимі з використанням комерційних онлайн-платформ, які зазвичай не вимагають автентифікації. Цей режим забезпечує ефективне використання пропускної здатності, а також має перевагу, оскільки надає творцю матеріалів більше контролю над його/її інтелектуальною власністю (після відтворення відеоданих медіаплеєр видаляє їх).

    b. Надання доступу до платформи для проведення відеоконференцій, зазвичай шляхом надання посилання з гостьовим або автентифікованим доступом і можливості для організатора створити кімнату очікування. В останньому випадку необхідно надати чіткі інструкції.

7. Альтернативою публічному доступу в реальному часі є відкладений доступ, що означає, що широка громадськість і медіа можуть переглянути та/або прослухати запис судового засідання на вебсайті. Доступ до запису можна отримати через завантаження або потокове відтворення. У разі потокового відтворення матеріал надсилається безперервним потоком даних, який відтворюється залежно від надходження. Користувачі можуть ставити на паузу, перемотувати назад або вперед, як із завантаженим файлом.

8. Важливо завчасно повідомити громадськість і медіа про проведення судового засідання, щоб забезпечити дотримання вимог і запобігти його несанкціонованому зриву чи неналежному використанню відеозапису.

Пробний сеанс

Правило 37. Якщо це можливо й необхідно, суд має призначити пробну відеоконференцію перед початком дистанційного судового засідання, щоб дати пояснення, як саме відбуватиметься дистанційне судове засідання, які технології використовуватимуться, та стосовно будь-яких інших пов'язаних із цим питань.

1. Перед початком судового засідання рекомендовано перевірити та протестувати обладнання і програмні платформи.
2. Попередня перевірка також буде корисною для тих учасників, хто не ознайомлений із обраною платформою, а також для користувачів, які ознайомлені з нею, але використовують інший вид підключення до інтернету та/або інші аудіовізуальні пристрої.

Завчасне приєднання

Правило 38. Суд та учасники мають приєднатися до відеоконференції завчасно перед початком дистанційного судового засідання, щоб вирішити всі технічні проблеми.

1. Технічні проблеми, як-от поганий зв'язок, можуть виникнути несподівано і з різних непередбачуваних причин, тому рекомендовано провести останню перевірку безпосередньо перед початком судового засідання, виділивши достатньо часу для діагностики та вирішення проблем.

Повідомлення про труднощі

Правило 39. Суд має повідомити всіх учасників судового засідання про можливі технічні й інші труднощі, які можуть виникнути, та нагадати про те, що не слід говорити надто багато, а також потрібно вимикати мікрофон, коли вони не говорять.

1. На початку судового засідання суддя повинен переконатися в тому, що всі учасники отримали та зрозуміли вказівки, а також у тому, що вони знають про свої обов'язки, обмеження та ознайомлені з манерою поведінки. Суддя має повторити правила на початку судового засідання, чітко й детально пояснивши, як проводитиметься судове засідання і які наслідки його зриву.

Місце, з якого беруть участь у судовому засіданні

Правило 40. Залежно від вимог національного законодавства, учасники можуть брати участь у судовому засіданні, що проводиться в режимі відеоконференції, перебуваючи в залах суду, місцях позбавлення волі, приміщеннях юридичних фірм або інших безпечних місцях. Обстановка судового засідання, зокрема обладнання, має гарантувати цілісність заяв усіх учасників, особливо тих, які перебувають у вразливому становищі.

1. Відповідно до конкретних потреб слід передбачити можливість надання технологічних засобів та обладнання учасникам, які в іншому разі не матимуть дистанційного доступу до судового засідання, зокрема належних пристосувань для осіб з інвалідністю (аналогічних пристосуванням і коригуванням, якими зазвичай вони були б забезпечені у разі присутності в судовому засіданні в залі суду).

Безпека

Уразливість

Правило 41. Слід завчасно вжити організаційних заходів щодо пом'якшення ризику вразливості обладнання, програмного забезпечення і з'єднання для відеоконференції до несанкціонованого доступу, як-от зламування, чи іншого виду незаконного доступу.

1. Якщо платформа розміщена локально, відповідні завдання з технічного обслуговування повинні забезпечувати безпеку шляхом своєчасного оновлення та керування виправленнями, із застосуванням конкретних угод про рівень обслуговування, якщо ці завдання покладено на стороннього постачальника послуг.
2. У разі використання хмарної платформи постачальник повинен забезпечити постійний моніторинг безпеки системи та своєчасно повідомляти про проблеми чи порушення та вжиті контрзаходи.

Плани дій в екстрених ситуаціях

Правило 42. Потрібно розробити плани дій в екстрених ситуаціях, щоб ефективно вирішувати такі проблеми, як-от несподівані технічні несправності, відключення зв'язку, вимкнення електропостачання (альтернативні канали зв'язку та технічна підтримка) або порушення безпеки даних.

1. Якщо платформа розміщена локально, потрібно підготувати, затвердити та виконати аналіз ризиків і комплексний план аварійного відновлення (або план забезпечення безперервної діяльності), зокрема

провести випробування часу відновлення ефективності. Потрібно врахувати всі необхідні аспекти, як-от використання системи резервного копіювання, резервних пристроїв, резервних каналів підключення тощо. Необхідно укласти конкретні угоди про рівень обслуговування, якщо керування системою доручено сторонньому постачальнику послуг, щоб забезпечити своєчасне виконання плану в разі надзвичайної ситуації.

2. У разі використання хмарної платформи слід укласти конкретні угоди про рівень обслуговування, щоб забезпечити мінімальний щомісячний рівень доступності.

Захист персональних даних у разі використання послуг хмарного зберігання

Правило 43. Послуги хмарного обчислення, що використовують під час дистанційних судових засідань, і потенційні сховища даних мають відповідати вимогам законодавства щодо захисту персональних даних.

1. Хмарна платформа для проведення відеоконференцій, а також для зберігання інформації повинна забезпечувати шифрування каналу зв'язку та збережених персональних даних.

2. Обмін файлами через платформу для проведення конференцій або платформу хмарного сховища є більш безпечним, ніж використання електронної пошти. Однак:

   a. Завжди слід ураховувати конфіденційний характер інформації, тип судового засідання та необхідний рівень безпеки.

   b. Електронна пошта є загальнодоступною, але вона може бути недостатньо безпечним способом передачі конфіденційної інформації. Електронні листи можуть містити помилки, як-от неправильна тема, неможливість прикріплення бажаного файла або прикріплення зовсім не пов'язаного файла. Дата надсилання та отримання може призвести до плутанини щодо найновішої версії. Крім того, з точки зору безпеки електронні листи є звичайними точками проникнення руйнівних вірусів і шкідливих програм.

3. Доступ до доказів, які подаються та зберігаються в цифровій формі, має бути контрольованим, а точки доступу до них — обмеженими. До електронних контрольних журналів аудиту потрібно вносити інформацію про те, коли і хто здійснював доступ до файлів. Керівні принципи щодо електронних доказів містять корисні вказівки щодо зберігання, збереження та архівування даних:

a. Електронні докази мають зберігатися так, щоб була забезпечена їхня зрозумілість, доступність, цілісність, автентичність, надійність і, за потреби, конфіденційність та секретність.

b. Електронні докази слід зберігати в оригінальному форматі (тобто не як роздруківки) і відповідно до вимог законодавства.

c. Зрозумілість і доступність збережених електронних доказів повинні бути гарантовані з плином часу, ураховуючи еволюцію інформаційних технологій.

d. Цілісність електронних доказів має бути забезпечена на всіх етапах.

e. Суди повинні архівувати електронні докази згідно з вимогами національного законодавства. Електронні архіви повинні відповідати всім вимогам безпеки та гарантувати цілісність, автентичність, конфіденційність і якість даних, а також повагу до приватності.

Технічна несправність, яку неможливо усунути

Правило 44. У разі виникнення технічної несправності, яку неможливо усунути, дистанційне судове засідання слід перенести або призупинити.

Технічні стандарти

Дотримання стандартів

Правило 45. Обладнання та програмне забезпечення для відеоконференцій має відповідати мінімальним галузевим стандартам, щоб забезпечити сумісність з будь-якими видами засобів проведення відеоконференцій, а також мінімізувати затримки трансляції відео- й аудіоданих.

Правило 46. Державам слід переглядати технічні стандарти, пов'язані з проведенням відеоконференцій.

1. Основні стандарти, яким повинна відповідати система для проведення відеоконференцій:

   a. H.323 (стандарт Міжнародної спілки електрозв'язку) — для передачі звуку та відеозображення через мережу з пакетною передачею (IP-LAN і загальнодоступний інтернет). SIP — стандарт IETF для передачі звуку та відеозображення через IP-мережі. Деякі системи для проведення відеоконференцій можуть обслуговувати клієнтів H.323 і SIP водночас. H.323 забезпечує взаємодію з

комерційними хмарними платформами (через кінцеві точки H.323) та IP-телефонами.

b. Для стиснення відео основними кодексами ITU є H.263 і H.264; другий із них є удвічі менш вимогливим до пропускної здатності, ніж перший.

c. H.239 розподіляє пропускну здатність між відеоконференцзв'язком та другим джерелом відео. Завдяки цьому учасники можуть підключатися до другого відеопотоку й ділитися зображеннями з екранів своїх комп'ютерів під час конференції.

Технологічна нейтральність

Правило 47. Державам слід розглянути можливість розробити правила щодо відеоконференцій технологічно нейтральними й не вимагати використання певного виду технологій, а також не створювати сприятливих умов для цього.

Якість обладнання

Правило 48. Обладнання та програмне забезпечення для відеоконференцій має забезпечувати трансляцію зображення та звуку достатньої якості, щоб підтримувати постійний належний аудіовізуальний зв'язок, який дає учасникам змогу дотримуватися процедури провадження і брати в ньому активну участь.

Правило 49. Усі учасники дистанційного судового засідання, зокрема суддя, повинні мати можливість водночас бачити й чути особу, яка ставить запитання або робить заяви під час заслуховування, а також реакцію інших учасників.

1. Мікрофони, колонки та відеокамери мають бути належної якості. Для певних учасників, зокрема судді, який підключається дистанційно, мають бути дотримані такі вимоги та рекомендації:

   a. Роздільна здатність екрана: не менш ніж 1280 x 720 пікселів (рекомендовано: 1920 x 1080 пікселів).

   b. Вебкамера з високою роздільною здатністю: не менш ніж 720 p.

   c. Рекомендовано використовувати якісний зовнішній мікрофон або гарнітуру (замість вбудованого в ноутбук або вебкамеру); бажано використовувати шумопоглинаючий пристрій.

   d. Рекомендується підключення через дротову мережу (не Wi-Fi).

2. У разі використання великої зали засідань суду слід віддати перевагу професійному комплекту пристроїв: найкращим рішенням є мікрофони з автоматичним вмиканням лише для активного мовця та роботизовані камери, які автоматично дають його зображення широким планом.
3. У разі використання невеликої зали засідань суду доцільним є рішення щодо круглого столу (сумісне з програмною платформою), оскільки у такий спосіб забезпечується панорамне відеозображення всіх тих, хто сидить за столом, зображення активного мовця з високою роздільною здатністю та перемикання між різними учасниками, коли вони говорять.

Технічна допомога

Правило 50. Судді, сторони, працівники апарату суду та інші учасники під час дистанційних судових засідань повинні мати доступ до ІТ-підтримки, щоб уникнути затримок і технічних труднощів під час використання систем для проведення відеоконференцій.

1. Підтримка може бути надана через центральну (дистанційну) службу підтримки.
2. Локальна підтримка може бути надана для однієї або кількох зал засідань суду, у яких присутні багато осіб, які беруть участь у дистанційних судових засіданнях.

Підготовка та краща практика

Підготовка

Правило 51. Держави мають забезпечити для суддів, працівників апарату суду та юристів-практиків належну підготовку з питань ІТ-рішень і міжнародних стандартів захисту прав людини.

1. Залучені органи влади відповідають за підготовку суддів та інших працівників суду до проведення дистанційного судового засідання.
2. Необхідно організувати навчальні курси (також вебінари) і надати доступ до навчальних відеоматеріалів для різних типів користувачів.

Додатки
КРАЩА ПРАКТИКА

Італійська система проведення відеоконференцій у кримінальних справах

Проведення судового засідання у кримінальній справі за допомогою відеоконференцзв'язку відбувається за присутності судді, прокурора та адвоката в судовій залі, тоді як обвинувачений приєднується до судового засідання зі спеціально обладнаної кімнати в пенітенціарній установі.

Система має найвищий рівень безпеки та не підключена до інтернету, тому громадськість може тільки фізично бути присутньою в залі судових засідань. У справах з високим рівнем суспільного значення, коли очікується залучення великої кількості спостерігачів та медіа, інша судова зала, яка підключена до тієї ж системи, може бути використана для розміщення спостерігачів.

Захисники можуть спілкуватись конфіденційно зі своїми підзахисними, які знаходяться в пенітенціарній установі, через лінію VOIP: телефони встановлено як у залі судових засідань, так і в спеціальних кабінах у кімнатах установи.

Свідки можуть приєднуватись з різних місць — або з іншої зали судових засідань, або із спеціально обладнаної зали пенітенціарної установи. У разі якщо необхідно зберігати в таємниці місцезнаходження свідка з міркувань його захисту, на екрані таке місцезнаходження не зазначають. Викривлення голосу або розмивання/ретушування картинки не застосовують.

Італійська система має центральний пункт управління, у якому розміщують належну кількість операторів та експертів, які можуть контролювати всі прилади (камери, мікрофони, динаміки) під час сесій, а також те, що видно на екранах: попередньо пункт управління попереджають про залучення свідків під захистом для того, щоб забезпечити спеціальні налаштування.

Використовують такі практичні налаштування:

- за 30 хвилин до початку судового засідання оператор пункту управління, якого призначили до засідання, проводить контрольну перевірку аудіо- та відеоякості;

- оператор пункту управління здійснює моніторинг якості під час судового засідання;
- пункт управління діє як пункт допомоги у разі виникнення проблем та негайно втручається для їх усунення;
- систему встановлено у двох дата-центрах для забезпечення заміщення: у разі припинення роботи одного негайно починає працювати другий;
- система діє в спеціально призначеній приватній мережі через Intranet Міністерства юстиції Італії, а отже, є захищеною від втручання;
- для забезпечення якості цій мережі надано належну пропускну можливість;
- система створена так, що кожна сесія записується та будь-яка дія реєструється. Записи та журнал реєстрації зберігаються певний період часу. У такий спосіб забезпечується можливість надавати інформацію у відповідь на запит;
- у пенітенціарних установах є переносні місця (тобто рухомі, обладнані всім необхідним устаткуванням, місця для приєднання) як запасний варіант у разі, якщо стаціонарне обладнання не працюватиме.

Польська система проведення відеоконференцій у цивільному судочинстві

Більшість дистанційних судових засідань у Польщі проводять за допомогою двох IT-систем Міністерства юстиції Польщі — Equinox (колишня Avaya Scopia) та Jitsi. Обидві системи адаптовано до спеціальних вимог цивільної процедури та електронного протоколу (електронний запис судового засідання). Учасників дистанційного судового засідання завчасно повідомляють про дату дистанційного судового засідання та надсилають їм посилання для підключення. Вони також отримують детальні інструкції щодо доступу до судового засідання та як використовувати функціональні можливості вказаної системи (Посібник для учасників судового засідання з використанням відеоконференції).

Див.: https://www.wroclaw.sa.gov.pl/wideokonferencje,m,mg,385).

Система *Avaya Scopia* 3 вересня 2022 року була замінена на *Equinox* — нову систему, що є більш зрозумілою та зручною для використання учасниками. *Avaya Scopia* потребувала завантаження спеціального застосунку на мобільний прилад, що було доволі проблематичним для більшості учасників дистанційного судового засідання.

Тепер обидві системи, рекомендовані Міністерством юстиції Польщі — *Jitsi and Equinox,* дають змогу приєднуватись до судового засідання з

використанням посилання, яке надсилає працівник суду або суддя, безпосередньо через інтернет-браузер, не вдаючись до завантаження або встановлення будь-якої програми.

На сьогодні Апеляційний суд у місті Вроцлаві, який визначено відповідальним за розвиток та підтримку ІТ-систем для судової гілки влади в Польщі, працює над удосконаленням та імплементацією нових функцій систем відеоконференції (*Equinox and Jitsi*).

Заплановано удосконалити такі функції:

1) Можливість подати клопотання щодо дистанційного судового засідання у своїй справі — клопотання буде надсилатись через спеціальну ІТ-систему.

2) ПІН-код (ID) верифікація — використовуючи ПІН-код, кожен може верифікувати свою особу та після успішного її проходження учасник автоматично долучається до віртуальної кімнати очікування.

3) Модерування кімнати очікування — управління здійснюється через окрему систему, надаючи модератору зустрічей можливість погоджувати певних осіб та допускати їх до обраної ним віртуальної зали судових засідань. Наприклад, якщо заслуховують свідків, кожен свідок може заходити до віртуальної зали судових засідань один за одним. Це забезпечується з огляду на те, що відповідно до національного законодавства Польщі свідки не можуть бути присутніми в залі суду, коли дає свідчення інший свідок. Учасник, обраний модератором (працівник суду або суддя), очікує у віртуальній кімнаті очікування.

4) Можливість надсилати учасникам, які очікують у віртуальній кімнаті очікування, повідомлення про затримку дистанційного судового засідання або технічні проблеми. Ця функція була розроблена у відповідь на численні прохання адвокатів та представників сторін, які скаржились на те, що в багатьох випадках вони не отримували жодної інформації про затримку дистанційного судового засідання.

5) Зміни щодо участі слухачів — особи, які зацікавлені в участі в судовому засіданні як слухачі, повинні отримати індивідуальний ПІН-код, який дає змогу верифікувати особу. Після успішної верифікації учасник автоматично під'єднується до системи, у якій транслюється дистанційне судове засідання. Такі учасники не можуть використовувати мікрофон або камеру, вони також не можуть брати активної участі в дистанційному судовому засіданні.

РЕСУРСИ

Керівництво CEPEJ щодо проведення судових проваджень у режимі відеоконференції

https://rm.coe.int/cepej-2021–4-guidelines-videoconference-en/1680a2c2f4

Керівні принципи Комітету міністрів Ради Європи щодо електронних доказів у цивільних та адміністративних судочинстві

https://www.coe.int/en/web/cdcj/activities/digital-evidence

Керівні принципи Комітету міністрів Ради Європи щодо механізмів онлайн вирішення спорів у цивільному та адміністративному судочинстві

https://www.coe.int/en/web/cdcj/online-dispute-resolution-mechanisms

Справа «Джаллоу проти Норвегії» (Jallow v. Norway)

ДОДАТКОВІ МАТЕРІАЛИ

cepej
European Commission for the Efficiency of Justice
Commission européenne pour l'efficacité de la justice
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Страсбург, 30 червня 2021 року

CEPEJ(2021)4REV4

ЄВРОПЕЙСЬКА КОМІСІЯ З ПИТАНЬ ЕФЕКТИВНОСТІ ПРАВОСУДДЯ (СЕРЕЈ)

Керівництво щодо проведення судових проваджень у режимі відеоконференції

Документ затверджено СЕРЕЈ на 36-му пленарному засіданні (16–17 червня 2021 року)

КЕРІВНИЦТВО

МЕТА ТА СФЕРА ЗАСТОСУВАННЯ

Керівництво[1] містить основні заходи, яких мають вживати держави й суди під час проведення судових провадження у режимі відеоконференції, щоб запобігти порушенню права на справедливий судовий розгляд, яке гарантується статтею 6 Європейської конвенції з прав людини (далі — ЄКПЛ), і забезпечити дотримання вимог Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних. Метою є надання державам системи настанов, що покликана усунути будь-які ризики порушення прав сторін під час проведення дистанційних судових засідань, зокрема їхнього права бути вислуханими та брати активну участь у провадженні, а також права на захист. Керівництво стосується всіх судових проваджень і можуть також застосовуватися mutatis mutandis до діяльності органів прокуратури у разі внесення відповідних змін.

Структура документа: у першій частині розглянуто процедурні аспекти всіх видів судових проваджень і зосереджено увагу на особливостях кримінальних проваджень; у другій частині акцентовано на технічних і організаційних вимогах до проведення судових проваджень у режимі відеоконференції. Додаток містить контрольний список основних вимог до проведення відеоконференцій у судовій практиці.

ВИЗНАЧЕННЯ

У контексті Керівництва перелічені нижче терміни мають такі значення:

i. **відеоконференція —** система, що дає змогу здійснювати одночасну двосторонню передачу зображення та звуку й у такий спосіб забезпечує візуальну, аудіальну та вербальну взаємодію під час дистанційного судового засідання;

ii. **дистанційне слухання —** слухання, що проводять у режимі відеоконференції;

iii. **суд —** орган судової влади, який у межах виконання своїх функцій забезпечує організацію дистанційного судового засідання.

ОСНОВНІ ПРИНЦИПИ

A. Всі передбачені в ЄКПЛ гарантії справедливого суду застосовують до дистанційних судових засідань у межах усіх судових проваджень.

1. Керівництво розроблено на основі Проєкту, що його підготували фахівці CEPEJ: Марек Свєрчинський (Marek Świerczyński) (Польща) та Александр Паланко (Alexandre Palanco) (Франція).

Основними елементами є право на ефективний доступ до суду, справедливість провадження, змагальність сторін, рівність сторін, належне поводження з доказами, час на підготовку матеріалів і доступ до них, ухвалення судом рішення протягом розумного строку, захист даних і управління ризиками.

B. Державам слід створити законодавче регулювання, яке забезпечувало б чіткі підстави для проведення судами дистанційних судових засідань у межах судових проваджень.

C. Саме суд має вирішувати в межах чинного законодавства, чи слід певне судове засідання проводити в дистанційному режимі, щоб забезпечити загальну справедливість провадження.

D. Суд має забезпечити дотримання права сторони на ефективну допомогу адвоката під час усіх судових проваджень, зокрема конфіденційність їхнього спілкування.

Частина I

ПРОЦЕДУРНІ АСПЕКТИ РЕЖИМУ ВІДЕОКОНФЕРЕНЦІЇ З ТОЧКИ ЗОРУ ПРАВА НА СПРАВЕДЛИВИЙ СУД

Керівництво щодо всіх видів судових проваджень

Рішення про проведення дистанційного судового засідання

1) Державам слід забезпечити, щоб законодавство давало судам достатні підстави у кожному конкретному випадку вирішувати, чи може або повинно судове засідання бути проведено дистанційно.

2) З огляду на чинне законодавство суд має визначити, з урахуванням конкретних обставин справи, чи є розумним проведення дистанційного судового засідання, а також належним чином обґрунтувати своє рішення.

3) Сторонам слід надати можливість обговорити з судом такі питання: i) чи можна або чи слід проводити дистанційне судове засідання; ii) яких конкретних заходів потрібно вжити для організації дистанційного судового засідання; iii) щодо безпеки сторін та їх побоювань щодо цього; iv) можливість звернутися до суду з проханням провести дистанційне судове засідання з особистою присутністю із наведенням причин.

4) Рішення повинно підлягати оскарженню в компетентному органі влади відповідно до національного закону.

Право на активну участь

5) Суд має надати учасникам можливість перевірити якість звуку та зображення до початку дистанційного судового засідання (наприклад, виконавши самоперевірку), або на його початку, щоб кожен учасник міг ознайомитися з функціями платформи проведення відеоконференцій.

6) Під час дистанційного засідання суд повинен мати можливість постійно відстежувати якість зображення та звуку відеозв'язку, щоб звести до мінімуму кількість технічних несправностей, які можуть вплинути на право сторін брати активну участь у провадженні.

7) Суд має забезпечити можливість бачити й чути трансляцію для всіх учасників провадження, а також для представників громадськості, якщо провадження проводять у відкритому форматі.

8) Під час ухвалення рішення про проведення дистанційного судового засідання і його практичних аспектів суд має враховувати обставини та труднощі осіб, які перебувають у вразливому становищі, як-от діти, мігранти або особи з інвалідністю.

9) Суд має призупинити проведення дистанційного судового засідання в разі виникнення технічної несправності до моменту її усунення, залежної від характеру такої несправності. Це призупинення має бути задокументоване в протоколі дистанційного судового засідання.

Ідентифікація та приватність

10) Суд має ідентифікувати всіх учасників дистанційного судового засідання. Засоби ідентифікації мають чітко відповідати чинному законодавству й не бути надмірними або обтяжливими.

11) Приватність учасників дистанційного судового засідання має бути належно захищена і суд має вживати заходів для зниження ризиків для неї. Потрібно вжити всіх необхідних заходів для усунення будь-якого ризику порушення права сторін на приватність.

Публічність і запис

12) Суд має зберегти публічний характер дистанційного судового засідання, створивши цілісну процедуру участі громадськості. Публічність дистанційного судового засідання можна забезпечити, наприклад, дозволивши громадськості приєднатися до дистанційного судового засідання в реальному часі або розмістивши відповідні записи на вебсайті суду.

13) Без попереднього дозволу суду може бути заборонене фотографування, записування, транслювання чи інше поширення будь-якої частини дистанційного судового засідання (разом із аудіозаписами).

Свідки та експерти

14) У межах, дозволених національною правовою системою, допит свідків та експертів під час дистанційного судового засідання має проводитися в порядку, максимально наближеному до практики їх допиту в залі засідань суду.

15) Слід приділити особливу увагу відповідним організаційним заходам, щоб забезпечити цілісність дистанційних судових засідань та уникнути тиску або впливу на свідків чи експертів під час таких засідань.

Докази

16) Суд має надати вказівки щодо процедури, якої учасники повинні дотримуватися для подання документів або інших матеріалів під час дистанційного судового засідання.

17) Слід вжити організаційних заходів, щоб забезпечити можливість для всіх учасників бачити та/або чути матеріали, надані під час дистанційного судового засідання.

18) Подання нових заяв, аргументів та/або доказів під час дистанційного судового засідання має відповідати принципу змагальності, водночас суд має забезпечити право подання доказів протилежною стороною.

Перекладачі

19) У разі потреби в залученні перекладача під час дистанційного судового засідання перевагу слід надавати присутності перекладача поряд з учасником, який не розмовляє мовою суду.

20) Перекладач повинен мати належний візуальний контакт з особою, мовлення якої перекладає, протягом усього дистанційного судового засідання.

Окреме керівництво щодо кримінальних проваджень

Легітимна мета

21) Якщо законодавство не вимагає отримання вільної інформованої згоди обвинуваченого, рішення суду щодо його або її участі в дистанційному судовому засіданні повинно мати легітимну мету.

22) Легітимна мета дистанційного судового засідання в межах кримінального провадження має ґрунтуватися на таких цінностях, як охорона громадського порядку, охорона здоров'я, запобігання вчиненню правопорушень і захист права на життя, свободу, захист свідків і потерпілих від злочинів. Суд може розглядати питання дотримання права на судовий розгляд протягом розумного строку, зокрема, на наступних етапах провадження після першої інстанції.

Активна участь обвинуваченого

23) Через відеозв'язок обвинувачений повинен мати змогу бачити й чути учасників дистанційного судового засідання, зокрема інших сторін, суддів, свідків та експертів. Учасники повинні мати змогу бачити й чути обвинуваченого.

24) Суд має реагувати на технічні несправності, про які повідомляє обвинувачений. Перед початком дистанційного судового засідання обвинувачений має бути поінформований про порядок повідомлення головуючому судді про технічні несправності (наприклад, через призначення офіційного відповідального представника, який перебуватиме поряд з обвинуваченим, або використання сигнальної кнопки в інтерфейсі засобу відеозв'язку).

25) У разі постійної неприйнятної поведінки обвинуваченого суд має спершу повідомити йому про право суду вимкнути звук, перервати або призупинити сеанс відеозв'язку з обвинуваченим, перш ніж ухвалювати рішення про це.

26) У разі вимкнення звуку від обвинуваченого суд має забезпечити представнику його інтересів можливість і надалі реалізовувати право на правничу допомогу під час дистанційного судового засідання і провадження загалом.

Представництво інтересів

27) Обвинувачений повинен мати ефективний доступ до представництва своїх інтересів перед початком дистанційного судового засідання і під час його проведення, разом із правом до початку судового засідання конфіденційно спілкуватися зі своїм захисником.

28) Суд має перенести або призупинити дистанційне судове засідання за відсутності захисника обвинуваченого. У такому разі суд має вжити всіх необхідних заходів щодо забезпечення дотримання права обвинуваченого на захист, разом із можливим призначенням захисника *ex officio*.

29) Обвинувачений повинен мати право радитися із захисником і обмінюватися конфіденційною інформацією без нагляду. Присутність інших осіб у приміщенні, у якому обвинувачений перебуває під час такого обміну, не допускається.

30) Обвинувачений повинен мати право спілкуватися із захисником за допомогою захищеної системи. Слід забезпечити конфіденційність такого спілкування обвинуваченого. Використання захищеної лінії зв'язку, яка є окремою від лінії відеозв'язку, за допомогою якою проводять дистанційне судове засідання, має бути захищене привілеєм на збереження адвокатської таємниці.

31) Слід вжити спеціальних організаційних заходів, щоб забезпечити захист конфіденційності спілкування між обвинуваченим і захисником у разі використання послуг перекладача під час такого спілкування.

Частина II

ОРГАНІЗАЦІЙНІ ТА ТЕХНІЧНІ АСПЕКТИ РЕЖИМУ ВІДЕОКОНФЕРЕНЦІЇ

Основні вимоги

32) Державам рекомендується виділяти достатнє фінансування та ресурси для забезпечення ефективного проведення судових проваджень у режимі відеоконференції.

33) Держави мають забезпечувати максимально наближене до реалістичного проведення дистанційних судових засідань, зокрема повноцінне спілкування та взаємодію всіх сторін процесу з особою, яку вони мають вислухати.

34) Проведення дистанційного судового засідання має ґрунтуватися на принципах справедливості, ефективності, доцільності провадження, співпраці, безпеки та законності обробки персональних даних.

Інструкції для учасників

35) Суд має надати учасникам чіткі правила, інструкції та/або навчальні матеріали щодо використання засобів відеозв'язку та проведення дистанційного судового засідання. Рекомендується підготувати інформаційні матеріали не лише в текстовому форматі, а й у форматі коротких відео. Слід розглянути можливість створення індивідуальних навчальних матеріалів або курсів щодо використання платформи. Суд повинен нагадати учасникам, що вони постають перед судом і повинні поводитися належним чином згідно з вимогами чинного законодавства, належною практикою і судовим етикетом, які потрібно адаптувати для застосування під час дистанційних судових засідань.

36) Суд має завчасно надіслати учасникам повідомлення про технічні вимоги, зокрема дату, час (з урахуванням різних часових поясів), місце та умови проведення дистанційного судового засідання.

37) Суд має попросити учасників забезпечити надійний відеозв'язок достатньої якості, належну видимість і освітлення для ефективної участі в дистанційному судовому засіданні.

38) Якщо це можливо і в цьому виникає потреба, перед початком дистанційного судового засідання суд має призначити тестову відеоконференцію, щоб дати пояснення стосовно того, як саме буде проводитись

дистанційне судове засідання, які технології використовуватимуться та з інших пов'язаних із цим питань.

39) Суд та учасники мають приєднатися до відеоконференції завчасно до початку дистанційного судового засідання для вирішення всіх технічних питань.

40) Суд має повідомити всіх учасників про можливі технічні чи інші складнощі, що можуть виникнути, та нагадати, що не слід говорити надто багато, а також потрібно вимикати мікрофон, коли вони не говорять.

41) Залежно від вимог національного законодавства учасники можуть брати участь у судовому засіданні, що проводиться в режимі відеоконференції, перебуваючи в залах суду, місцях позбавлення волі, приміщеннях юридичних фірм або інших безпечних місцях. Обстановка судового засідання, зокрема обладнання, має забезпечувати цілісність заяв усіх учасників, особливо тих, які перебувають у вразливому становищі.

Безпека

42) Слід завчасно вжити організаційних заходів для пом'якшення ризику вразливості обладнання, програмного забезпечення і з'єднання для відеоконференції від несанкціонованого доступу, як-от зламування чи іншого виду незаконного доступу.

43) Потрібно розробити плани дій в екстрених ситуаціях, щоб ефективно вирішувати такі проблеми, як несподівані технічні несправності, відключення зв'язку, вимкнення електропостачання (альтернативні канали зв'язку та технічна підтримка) або порушення безпеки даних.

44) Послуги хмарного обчислення, що використовують під час дистанційних судових засідань, і потенційні сховища даних мають відповідати вимогам законодавства щодо захисту даних.

45) Використання технологій, особливо інструментів і послуг на основі штучного інтелекту, має зміцнювати автономність суду, а не обмежувати її.

46) Використання інструментів на основі штучного інтелекту, таких як електронні фільтри звуку та зображення, має бути під контролем суду.

47) У разі виникнення технічної несправності, яку не вдається усунути, дистанційне судове засідання слід перенести або призупинити.

Технічні стандарти

48) Обладнання та програмне забезпечення для відеоконференцій має відповідати мінімальним галузевим стандартам, щоб забезпечити сумісність з будь-якими видами засобів проведення відеоконференцій, а також мінімізувати можливу затримку трансляції відео- й аудіоданих.

49) Державам слід розглянути можливість розроблення правил щодо проведення відеоконференцій, які будуть технологічно нейтральними і не віддаватимуть переваг використанню певного виду технологій.

50) Обладнання та програмне забезпечення для відеоконференцій має забезпечувати трансляцію зображення та звуку достатньої якості, щоб підтримувати постійний належний аудіовізуальний зв'язок, який дає змогу учасникам стежити за перебігом судового розгляду і брати в ньому активну участь.

51) Усі учасники дистанційного судового засідання, зокрема суддя, повинні мати можливість водночас бачити й чути особу, яка ставить запитання або робить заяви під час заслуховування, а також реакцію інших учасників.

52) Система для проведення відеоконференцій, яку надає суд, має бути безкоштовною для всіх учасників, простою та зручною у користуванні. Ця система має працювати на стандартному обладнанні й забезпечувати захист даних.

53) Державам слід переглядати технічні стандарти, пов'язані з проведенням відеоконференцій.

Технічна допомога

54) Судді, сторони, працівники апарату суду та інші учасники під час дистанційних судових засідань повинні мати доступ до ІТ-підтримки, щоб уникнути затримок і технічних труднощів під час використання системи відеоконференцзв'язку.

Підготовка та передова практика

55) Державам слід забезпечити для суддів, працівників апарату суду та юристів-практиків належну підготовку з питань ІТ-рішень і відповідних міжнародних стандартів захисту прав людини.

56) Державам слід заохочувати суди ділитися кращою практикою проведення відеоконференцій для скорочення витрат і підвищення ефективності.

Додаток

Контрольний список основних вимог до проведення відеоконференцій у судовій практиці

- Безпека: бажаний рівень безпеки, що відповідає виду процедури
  - авторизація
    - присутніми можуть бути тільки визначені (запрошені) учасники
  - автентифікація особи
    - підтвердження особи учасників
  - приватність (забезпечення приватності конференції)
    - шифрування
  - приватна та публічна інфраструктури
    - публічна інфраструктура (хмара, хостинг)
    - рішення, розміщене локально (IT-рішення)
    - приватна інфраструктура
  - керування правами користувачів
    - автентифікація учасників
- Запис
  - голос
  - голос і зображення
  - багатоканальний голос
- Доступність
  - обладнання
  - програмне забезпечення
  - універсальність (зручність використання)
- Якість
  - роздільна здатність
  - пропускна здатність
  - чутливість
  - обладнання

- екрани
- роздільна здатність камери
- якість мікрофона
- кількість доріжок (мікрофонів і камер)

- Тип ліцензії:
  - пропрієтарна або на ПЗ з відкритим кодом
- Обладнання для відеоконференції
  - професійне (встановлене в залах суду на постійній основі)
  - професійне (мобільне)
  - напівпрофесійне (конференц-зали з екранами й камерами)
  - побутова електроніка (вебкамери з колонками, гарнітури з мікрофоном)
  - мобільні пристрої (планшети, мобільні телефони)
- Видимість
  - зала суду: екрани, колонки дають змогу всім учасникам стежити за ходом провадження
  - свідок або експерт
- Стандарти
  - відкриті або
  - пропрієтарні
- Сумісність
  - стандартні протоколи (стандарт MCE)
  - IP-to-IP
- Обмін документами
  - камера для документів (для документів у паперовій формі)
  - спільний екран (для документів у електронній формі)
- Робота камери
  - статична (фіксована) камера
  - ручний нахил/поворот/наближення/фокус
  - автоматична (контроль голосом)
  - дистанційне керування
- Захист свідків

- окреме приміщення для свідків (можливо в іншому місці)
- спотворення голосу
- розмивання/спотворення/відключення зображення

♦ Приватні сесії
- консультації сторін з адвокатами

♦ Переклад
- перекладачі в іншому місці
- синхронний переклад

♦ Використання штучного інтелекту
- автоматичне субтитрування
- визначення особи, яка говорить
- перетворення голосу на текст
- фільтри

♦ Планування відеоконференції
- використання системи резервування для відеоконференцій (календарні графіки) — залу суду можна зарезервувати залежно від його технічного оснащення
- технічний спеціаліст — бажано завчасно протестувати, налаштувати обладнання для відеоконференції в режимі очікування

cepej

European Commission for the Efficiency of Justice

Commission européenne pour l'efficacité de la justice

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 30 June 2021

CEPEJ(2021)4REV4

EUROPEAN COMMISSION FOR THE EFFICIENCY OF JUSTICE (CEPEJ)

Guidelines on videoconferencing in judicial proceedings

Document adopted by the CEPEJ at its 36th plenary meeting (16 and 17 June 2021)

GUIDELINES

PURPOSE AND SCOPE

These Guidelines provide a set of key measures that states and courts should follow to ensure that use of videoconferencing in judicial proceedings does not undermine the right to a fair trial as enshrined in Article 6 of the European Convention on Human Rights (ECHR) and meets the requirements of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. The purpose is to provide states with a framework aiming at eliminating any risk of a violation of the parties' rights during remote hearings, in particular their right to be heard and to actively participate in proceedings, and the right of defence. The Guidelines cover all judicial proceedings and can also be applicable mutatis mutandis to the public prosecution services.

The document is structured as follows: In the first part, the guidelines address procedural issues concerning all types of judicial proceedings, emphasising the particularities of criminal proceedings. In the second part, the guidelines address the technical and organisational requirements for videoconferencing in judicial proceedings. The appendix contains a checklist of the basic requirements for the implementation of videoconferencing in judicial practice.

DEFINITIONS

For the purposes of these guidelines, the terms below shall be defined as follows:

i. **videoconferencing** refers to a system that allows two-way and simultaneous communication of image and sound enabling visual, audio and verbal interaction during the remote hearing;

ii. **remote hearing** refers to a hearing that is held through videoconferencing;

iii. the term **"court"** refers to the judicial authority that organises remote hearings, in the exercise of its functions.

FUNDAMENTAL PRINCIPLES

A. All guarantees to a fair trial under ECHR apply to remote hearings in all judicial proceedings. The key elements are the right to effective access to a court, fairness of the proceedings, adversarial character of the process, equality of arms, proper administration of evidence, time to prepare and access to materials, the court's decision in a reasonable time, data security and risk management.

B. States should establish a legal framework that provides a clear basis for allowing courts to hold remote hearings in judicial proceedings.

C. It is for the court to decide, within the applicable legal framework, whether a certain hearing should be held remotely, with the aim of ensuring the overall fairness of the proceedings.

D. The court should safeguard the right of a party to be effectively assisted by a lawyer in all judicial proceedings, including confidentiality of their communication.

Part I —

PROCEDURAL ISSUES ON VIDEOCONFERENCING IN RESPECT OF THE RIGHT TO A FAIR TRIAL

Guidelines on all judicial proceedings

Decision to hold a remote hearing

1) States should ensure that the legal framework provides the courts with sufficient grounds to decide whether a remote hearing can or should be held in a particular case.

2) Based on the legal framework provided by the state, the court should determine whether holding a remote hearing is reasonable and appropriate under the specific circumstances of the case and reason its decision.

3) The parties should have the opportunity to consult with the court: i) on whether a remote hearing can or should be held in the case, ii) on the specific arrangements for such a remote hearing, iii) to address any security concerns of the parties, and iv) to request the court to hold a hearing in person, stating their reasons.

4) The decision should be open to possible review before a competent authority in accordance with national law.

Right to participate effectively

5) The court should give the participants the opportunity to test the audio and video quality, either prior, for example through self-testing, or at the start of the hearing allowing each participant to familiarise themselves with the features of the videoconferencing platform.

6) During the remote hearing, the court should be able to continuously monitor the quality of the image and sound of the video link in order to minimize technical incidents that may affect the right of the parties to participate effectively in the proceedings.

7) The court should ensure that the transmission can be seen and heard by those involved in the proceedings and by members of the public where the proceedings are held in public.

8) The court should consider the situation and challenges of persons in vulnerable positions, such as children, migrants, or persons with disabilities in the decision to have a remote hearing and its modalities.

9) The court should suspend the hearing in case of a technical incident until it has been corrected, depending on its nature. Such a suspension should be registered in the minutes of the remote hearing.

Identification and privacy

10) All participants of the remote hearing should be identified by the court. The measures of identification should be clearly within the applicable legal framework and not excessively intrusive or burdensome.

11) The privacy of the remote hearing's participants should be protected and respective risks to their privacy should be mitigated by the court. All necessary measures should be taken in order to eliminate any risk of a violation of the parties right to privacy.

Publicity and recording

12) The court should preserve the public nature of remote hearing by creating a comprehensive procedure for public participation. The publicity of the remote hearing can be ensured, for example, by allowing the public to join the remote hearing in real time or uploading the recordings to the court's website.

13) No photographing, recording, broadcasting or any other form of dissemination of any part of the remote hearing (including the audio track) may be made unless previously authorised by the court.

Witnesses and experts

14) As far as a national legal system permits, the examination of the witnesses and experts during the remote hearing should follow as closely as possible the practice adopted when a witness or expert is present in the courtroom.

15) The respective arrangements should be given special consideration in order to ensure the integrity of remote hearings and avoid pressure or influence on the witnesses or experts during such hearings.

Evidence

16) The court should provide instructions on the procedure the participants need to follow to present documents or any other materials during the remote hearing.

17) Practical arrangements should be made to ensure that all participants can see and/or hear the material presented during the remote hearing.

18) The presentation of new allegations, arguments and/or evidence during a remote hearing should follow the adversarial principle and the court should ensure the right to counter-evidence.

Interpreters

19) When an interpreter is needed during the remote hearing, the presence of the interpreter alongside the participant who does not speak the language of the court should be preferred.

20) At any time during the hearing, the interpreter should have appropriate visual contact with the person whose speech is being interpreted.

Guidelines specifically for criminal proceedings

Legitimate aim

21) If legislation does not require the free and informed consent of the defendant, the court's decision for his or her participation in the remote hearing should serve a legitimate aim.

22) The legitimate aim of remote hearing in criminal proceedings should be based on such values as the protection of public order, public health, the prevention of offences, and the protection of the right to life, liberty, and security of witnesses and victims of crimes. Compliance with the right to a trial within a reasonable time can be considered by the court in particular at stages in the proceedings subsequent to the first instance.

Effective participation of the defendant

23) The video link provided should enable the defendant to see and hear the participants of the remote hearing, including the other parties, judges, witnesses and experts. The participants should be able to see and hear the defendant.

24) The court should react to technical incidents reported by the defendant. Prior to the remote hearing, the defendant should be informed of the procedure for reporting technical incidents to the presiding judge (e.g. through designation of a responsible official agent near the defendant or an alert button on the video link interface).

25) In case of the defendant's continuous improper conduct, the court should inform the defendant of its power to mute, interrupt or suspend the defendant's video link, before actually making this decision.

26) In case the defendant was muted, the court should ensure that the legal representative of the defendant is still able to exercise the right to legal assistance during the remote hearing and the proceedings as a whole.

Legal representation

27) The defendant should have effective access to legal representation before and during the remote hearing, including the right to communicate with their lawyer confidentially before the beginning of the hearing.

28) The court should adjourn or suspend the remote hearing in the absence of the defendant's legal representative. In such circumstances, the court should take all necessary measures to ensure the right to legal representation of the defendant, including possible appointment of an *ex officio* defence counsel.

29) The defendant should be able to confer with their legal representative and exchange confidential instructions without surveillance. The presence of other persons sharing the same room as the defendant during such exchanges should be excluded.

30) The defendant should be able to communicate with their legal representative over a secured system. The defendant should be assured of the confidentiality of such communications. The use of a secured line, different from the video link provided for the remote hearing, should be privileged.

31) Specific arrangements should be taken to ensure that the interpretation of communication between the defendant and their legal representative does not undermine its confidentiality.

Part II —
ORGANISATIONAL AND TECHNICAL ISSUES OF VIDEOCONFERENCING

Key requirements

32) States are encouraged to allocate adequate public funding and resources to enable effective videoconferencing in judicial proceedings.

33) States should ensure as much as possible a true-to-life hearing experience including full communication and interaction of all the parties to the procedure with the person to be heard.

34) Conduct of the remote hearing should be based on the principles of fairness, efficiency, expedience of proceedings, co-operation, security and legality of personal data processing.

Instructions for the participants

35) The court should provide the participants with clear rules, instructions, and/or tutorials on the use of videoconferencing and conduct of the remote hearing. It is recommended to prepare information materials not only in text format, but also as short videos. Made-to-measure tutorials or training sessions on the use of the platform should be considered. The participants should be reminded that they appear before the court and should therefore behave suitably in compliance with applicable laws, good practices, and court etiquette, which should be adapted in any case to remote hearings.

36) Sufficient notice about technical requirements, including the date, time (considering different time zones), place and the conditions of the remote hearing should be given in advance by the court to the participants.

37) The court should request participants to secure a reliable video connection of sufficient quality and ensure adequate visibility and lighting in order to be able to participate effectively in the remote hearing.

38) If possible and required, the court should schedule a test videoconferencing session prior to the remote hearing to allow guidance to be given on how the remote hearing will be conducted, the technology to be used, and any other relevant issues.

39) The court and participants should join the videoconferencing session in good time before the remote hearing is due in order to resolve any technical issues.

40) All participants should be informed by the court of possible technical and other difficulties that could be experienced by others and reminded to avoid over-speaking and mute their microphones when they are not speaking.

41) Depending on national law, the participants can attend a hearing by videoconference from courtrooms, detention facilities, law firms, or other safe places. The hearing's setting, including equipment, should guarantee the integrity of statements of every participant, in particular the vulnerable ones.

Security

42) Practical arrangements should be made in advance to mitigate the risk that the videoconferencing hardware, software and connections are vulnerable to improper access, such as hacking or other illicit access.

43) Contingency plans should be in place in order to effectively deal with issues such as sudden technical failures, disconnections, power outages (alternative communication channels and technical support), or data security breaches.

44) Cloud computing services used during remote hearings, and potential data storage, should comply with data protection laws.

45) The court's autonomy should be strengthened and not restricted by the use of technology, in particular by the use of artificial intelligence tools and services.

46) Use of artificial intelligence tools, such as sound or video e-filters, should be under the control of the court.

47) If there is a technical failure that cannot be fixed, then the remote hearing should be adjourned or suspended.

Technical standards

48) The videoconferencing hardware and software should meet minimum industry standards to facilitate interoperability, regardless of the type of videoconferencing used, and to reduce delays in video and audio data transmission.

49) States should consider making videoconferencing rules technology-neutral and not impose, or discriminate in favour of, a particular type of videoconferencing technology.

50) The videoconferencing hardware and software should provide video and audio of sufficient quality to hold continuous and adequate audio-visual

connectivity, enabling parties to follow the proceedings and effectively participate in them.

51) All participants to the remote hearing, in particular the judge, should be able to see and hear both the speaker asking questions or making statements when heard, and the reaction of the other participants.

52) The videoconferencing system provided by the court should be free of charge for all participants, easily accessible and user friendly, operate on standard hardware, and ensure data protection.

53) States should keep technical standards related to videoconferencing under review.

Technical assistance

54) The judges, parties, court staff, and other participants should be able to access IT support during remote hearings in order to avoid delays and technical difficulties while using a videoconferencing system.

Training and good practices

55) States should provide judges, court staff, and legal practitioners with sufficient training in IT solutions and related international standards of human rights protection.

56) States should encourage the courts to share best videoconferencing practices in order to reduce costs and increase efficiency.

Appendix

Checklist for conducting videoconferences in judicial practice

- Security: the desired level of security derived from the type of procedure
  - authorisation
    - only desired (invited) participants attending
  - authenticity
    - ensuring the identity of the participant
  - privacy (keeping the conference private)
    - encryption
  - private or public infrastructure
    - public infrastructure (cloud, hosting)
    - solution hosted on-site
    - private infrastructure
  - user management
    - authentication of participants
- Recording
  - voice
  - voice & video
  - multi-channel voice
- Accessibility
  - equipment
  - software
  - versatility (ease of use)
- Quality
  - resolution
  - bandwidth
  - sensitivity
  - equipment

- screens
- camera resolution
- microphone quality
- number of tracks (microphones and cameras)

- Licence type:
  - proprietary or open source
- Videoconferencing equipment
  - professional (permanently installed in courtrooms)
  - professional (mobile)
  - semi-professional (meeting rooms with screens and cameras)
  - consumer electronics (webcams with speakers, headsets with microphone)
  - mobile devices (tablets, mobile phones)
- Visibility
  - courtroom: screens, speakers enable all parties to follow the proceedings
  - witness or expert
- Standards
  - open vs.
  - proprietary
- Interoperability
  - standard protocols (ITU standard)
  - IP-to-IP
- Sharing documents
  - document camera (documents in physical form)
  - screen sharing (any digital content)
- Camera operation
  - static (fixed) camera
  - manuel tilt/turn/zoom/focus
  - automatic (voice controlled)
  - remote operation
- Witness protection

- separate witness rooms (possible off-site)
- voice distortion
- picture blur/distortion/deactivation

- Private sessions
  - parties consulting with their lawyers
- Interpretation
  - interpreters off-site
  - simultaneous interpretation
- Use of AI
  - automatic subtitling
  - speaker identification
  - speech to text
  - filters
- Planning a videoconference
  - using a booking system for videoconferencing (calendaring) — a courtroom can be booked depending on its technical equipment
  - technician — test beforehand, establish the videoconference, stand-by

COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES

1949.2019

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

ЗАСТУПНИКИ МІНІСТРІВ | Документи Комітету міністрів | **CM(2018)169-add1final** | 30 січня 2019 року

Керівні принципи Комітету міністрів Ради Європи щодо електронних доказів у цивільному та адміністративному судочинстві

(ухвалено Комітетом міністрів 30 січня 2019 року на 1335-му засіданні заступників міністрів)

Комітет міністрів,

беручи до уваги, що метою Ради Європи є досягнення більшої єдності між державами-членами, зокрема через сприяння прийняттю спільних правил щодо правових питань;

ураховуючи необхідність надання практичних рекомендацій щодо обробки електронних доказів у цивільних та адміністративних провадженнях судам та іншим компетентним органам, які виконують судові функції; фахівцям, зокрема юристам-практикам; а також сторонам провадження;

беручи до уваги, що метою цих керівних принципів є забезпечення спільної основи, а не гармонізація національного законодавства держав-членів;

ураховуючи необхідність поважати різноманітність у правових системах держав-членів;

визнаючи прогрес, якого досягли держави-члени стосовно цифровізації своїх судових систем;

відзначаючи, тим не менш, перешкоди для ефективного управління електронними доказами в системах правосуддя, такі як відсутність єдиних стандартів і різноманітність та складність процедур збирання доказів;

підкреслюючи необхідність сприяння використанню електронних доказів у правових системах та в судовій практиці;

визнаючи необхідність вивчення державами-членами сучасних недоліків використання електронних доказів та визначення сфер можливого запровадження чи поліпшення принципів і практики використання електронних доказів;

відзначаючи, що метою цих керівних принципів є надання практичних рішень для усунення існуючих недоліків у законодавстві та практиці,

приймає ці керівні принципи, які будуть практичним інструментом для держав-членів, що покликаний допомогти їм адаптувати функціонування своїх судових та інших механізмів урегулювання спорів для вирішення питань, які виникають у зв'язку з електронними доказами у цивільному та адміністративному провадженнях , і пропонує їм поширювати ці керівні принципи для їхньої імплементації відповідальними чи іншими зацікавленими особами.

Мета та сфера застосування

Керівні принципи стосуються:

- усних доказів, що отримано за допомогою засобів дистанційного зв'язку;
- використання електронних доказів;
- збирання, вилучення та передання доказів;
- відповідності;
- достовірності;
- зберігання та збереження;
- архівування;
- підвищення обізнаності, перегляду, навчання та освіти.

Керівні принципи не потрібно тлумачити як такі, що визначають доказову цінність для певних типів електронних доказів, а потрібно застосовувати лише в частині, у якій вони не суперечать вимогам національного законодавства.

Ці керівні принципи мають за мету полегшення використання й управління електронними доказами у правових системах і судовій практиці.

Визначення

Для цілей цих керівних принципів:

Електронні докази

Термін «електронні докази» — це будь-які докази, що містяться або які виробляє будь-який пристрій, функціонування якого залежить від

програмного забезпечення або даних, що зберігаються або передаються через комп'ютерну систему або мережу.

Метадані

Термін «метадані» — це електронна інформація про інші електронні дані, що можуть виявити ідентифікаційні ознаки, походження або історію доказів, а також відповідні дати й час.

Довірчі послуги

Термін «довірчі послуги» — це електронна послуга, що охоплює:

a. створення, верифікацію та підтвердження електронних підписів, електронних печаток чи електронних позначок часу, електронних зареєстрованих служб доставки та сертифікатів, пов'язаних із цими послугами; або

b. створення, верифікацію та підтвердження сертифікатів для автентифікації на вебсайтах; або

c. збереження електронних підписів, печаток або сертифікатів, пов'язаних із цими послугами.

Суд

Термін «суд» — це будь-який компетентний орган, що виконує судові функції та використовує електронні докази.

Основні принципи

Питання вирішення потенційної доказової цінності електронних доказів є відповідальністю судів згідно з вимогами національного законодавства.

Електронні докази повинні оцінюватися так само, як і інші види доказів, зокрема в частині, що стосується їхньої допустимості, достовірності, точності та цілісності.

Використання електронних доказів не повинно бути невигідним для сторін або надавати несправедливу перевагу одній із них.

Керівні принципи

Усні докази, отримані за допомогою засобів дистанційного зв'язку

1. Усні докази можуть бути отримані дистанційно, з використанням технічних пристроїв, якщо природа доказів дає таку можливість.
2. Під час вирішення питання про те, чи можуть усні докази бути отримані дистанційно, суди повинні розглядати, зокрема, такі фактори:

- значущість доказів;
- статус особи, яка надає докази;
- безпека та цілісність відеозв'язку, за допомогою якого передають докази;
- витрати та труднощі доставлення відповідної особи до суду.

3. Під час дистанційного отримання доказів необхідно забезпечити, щоб:
   a. передання усних доказів могли бачити і чути особи, які беруть участь у судовому процесі, та представники громадськості, якщо судове засідання відкрите; і
   b. особа, яку заслуховують дистанційно, може бачити та чути провадження тією мірою, якою це необхідно для забезпечення його здійснення справедливо та ефективно.
4. Процедура та технології, що застосовують для отримання усних доказів дистанційно, не повинні компрометувати допустимість таких доказів та здатність суду провести ідентифікацію зацікавлених осіб.
5. Незалежно від того, чи передають усні докази за допомогою засобів приватного або публічного каналу зв'язку, слід забезпечити належну якість відеоконференції та зашифрувати відеосигнал для захисту від перехоплення.

Використання електронних доказів

6. Суди не повинні відмовляти у прийнятті електронних доказів і не повинні заперечувати їхню юридичну силу лише тому, що вони були зібрані та (або) подані в електронній формі.
7. Загалом суди не повинні заперечувати юридичну силу електронних доказів виключно через те, що вони не мають розширеного, кваліфікованого або аналогічного захищеного електронного підпису.
8. Суди повинні розуміти доказову цінність метаданих та потенційні наслідки їх невикористання.
9. Сторонам має бути дозволено подавати електронні докази у вихідній електронній формі без необхідності надавати роздруківки.

Збирання, вилучення та передання

10. Електронні докази потрібно збирати в належний, убезпечений спосіб та подавати до судів з використанням надійних сервісів, таких як довірчі послуги.

11. Ураховуючи вищий ризик потенційного знищення або втрати електронних доказів порівняно з доказами не в електронній формі, держави-члени повинні встановити процедури для безпечного вилучення та збирання електронних доказів.

12. Суди повинні бути обізнані щодо окремих питань, які виникають під час розгляду питання про вилучення та збирання електронних доказів за кордоном, зокрема в транскордонних справах.

13. Суди повинні співпрацювати під час транскордонного отримання доказів. Суд, який отримав запит, повинен повідомити суд, який надіслав такий запит, про всі умови, разом із обмеженнями, згідно з якими доказ може прийняти суд, який отримав запит.

14. Збирання, структурування й управління електронними доказами має відбуватися так, щоб це полегшувало їхнє передання іншим судам, зокрема апеляційному.

15. Передання електронних доказів за допомогою електронних засобів слід заохочувати й полегшувати для підвищення ефективності судового розгляду.

16. Системи та пристрої, що використовують для передання електронних доказів, мають забезпечувати збереження цілісності таких доказів.

Відповідність

17. Суди повинні брати активну участь в управлінні електронними доказами, зокрема для уникнення надмірного або спекулятивного їх надання чи вимоги їх надання.

18. Суди можуть вимагати проведення експертами аналізу електронних доказів, особливо коли виникають складні доказові питання, або коли йдеться про маніпулювання електронними доказами. Суди мають вирішувати, чи мають такі особи достатній досвід у цьому питанні.

Достовірність

19. Стосовно достовірності суди повинні враховувати всі фактори, пов'язані з джерелом і автентичністю електронних доказів.

20. Суди мають бути обізнані щодо цінності довірчих послуг для встановлення достовірності електронних доказів.

21. Тією мірою, якою це не суперечить вимогам національного законодавства, за умови надання дискреційних повноважень суду вирішувати прийнятність конкретного доказу, електронні дані потрібно приймати як докази, якщо їх автентичність не оскаржує одна зі сторін.

22. Тією мірою, якою це не суперечить вимогам національного законодавства, за умови надання дискреційних повноважень суду вирішувати прийнятність конкретного доказу, достовірність доказу презюмується за умови, що особу підписувача може бути підтверджено, а цілісність даних забезпечено, якщо не буде обґрунтованих сумнівів у протилежному.

23. Якщо чинне національне законодавство встановлює спеціальний захист для вразливих категорій осіб, закон повинен мати пріоритет над цими керівними принципами.

24. Якщо нормами національної правової системи це визначено, електронні докази, які державний орган передає незалежно від сторін, мають переконливий зміст, якщо не буде доведено протилежне.

Зберігання та забезпечення збереження

25. Електронні докази потрібно зберігати так, щоб було забезпечено їх зрозумілість, доступність, цілісність, автентичність, достовірність і, за потреби, конфіденційність та повагу до приватності.

26. Електронні докази потрібно зберігати зі стандартизованими метаданими, щоб були зрозумілими обставини їх створення.

27. Мають бути гарантовані зрозумілість і доступність збережених електронних доказів зі сплином часу, ураховуючи розвиток інформаційних технологій.

Архівування

28. Суди повинні архівувати електронні докази відповідно до вимог національного законодавства. Електронні архіви повинні відповідати всім вимогам безпеки та гарантувати цілісність, автентичність, конфіденційність і якість даних, а також повагу до приватності.

29. Архівування електронних доказів мають забезпечувати кваліфіковані фахівці.

30. Дані необхідно переписувати на нові носії для зберігання, коли це буде потрібно для забезпечення доступності електронних доказів.

Підвищення рівня обізнаності, моніторинг, професійна підготовка та навчання

31. Держави-члени повинні сприяти підвищенню рівня обізнаності про переваги та цінність електронних доказів у цивільному та адміністративному провадженнях.

32. Держави-члени повинні постійно переглядати технічні стандарти, пов'язані з електронними доказами.

33. Усі фахівці, які мають справу з електронними доказами, повинні мати можливість проходити необхідне міждисциплінарне навчання щодо того, як працювати з такими доказами.

34. Судді та юристи-практики мають бути обізнані про розвиток інформаційних технологій, які можуть впливати на доступність електронних доказів та їх цінність.

35. Освітні програми в галузі права повинні містити модулі про електронні докази.

COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES

1949.2019

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

ЗАСТУПНИКИ МІНІСТРІВ	Документи Комітету міністрів	**CM(2018)169-add2**	17 грудня 2018 року[1]

1335-те засідання, 30 січня 2019 року

10. Правові питання

10.1. Європейський комітет з правового співробітництва (CDCJ)

Керівні принципи Комітету міністрів Ради Європи щодо електронних доказів у цивільному та адміністративному судочинстві — Пояснювальна записка

Питання для розгляду GR-J на засіданні 17 січня 2019 року

Зміст

1. Цей документ був класифікований як документ з обмеженим доступом до розгляду Комітетом міністрів Ради Європи.

Відповідність

Достовірність

Зберігання і забезпечення збереження

Архівування

Підвищення рівня обізнаності, моніторинг, професійна підготовка та навчання

Бібліографія та інші ресурси

Загальні коментарі

Навіщо нам новий документ?

1. Суди дедалі частіше звертаються до електронних доказів або надають дозвіл сторонам та іншим особам, які беруть участь у цивільному та адміністративному провадженнях, на створення електронних даних.
2. На сьогодні існує кілька стандартів, застосовних до електронних доказів на міжнародному, європейському чи національному рівнях. Законодавство та практика, які застосовують електронні докази, містять суттєві недоліки.
3. Мета цих керівних принципів щодо електронних доказів полягає не в тому, щоб установити обов'язкові правові стандарти, а в тому, щоб слугувати практичним інструментом для держав — членів Ради Європи в адаптації роботи їхніх судових та інших механізмів вирішення спорів для вирішення питань, що виникають у зв'язку з електронними доказами. У цьому питанні керівні принципи мають за мету підвищити ефективність та якість правосуддя.
4. Електронні докази переважно відрізняються від інших видів доказів і під час роботи з електронними доказами в судах та інших компетентних органах із судовими функціями виникають специфічні проблеми. Ці проблеми вказують на необхідність у підвищенні рівня знань про електронні докази та удосконалення роботи з електронними доказами у цивільному та адміністративному провадженнях.

Метод роботи і процес проєктування

5. Питання щодо електронних доказів належить до компетенції Європейського комітету з правового співробітництва (CDCJ), який є міжурядовим органом Ради Європи, що відповідає за діяльність із встановлення стандартів Ради Європи в галузі цивільного та адміністративного права.

6. Керівні принципи розробила редакційна група; вони ґрунтуються на пропозиціях, що їх внесли члени CDCJ і призначені експерти та підготували під час зустрічей, що відбулися у 2018 році. У цих зустрічах також брали участь відповідні органи Ради Європи, які мають досвід та обов'язки у цій галузі.

7. Редакційна група врахувала досвід роботи механізмів електронного правосуддя, що існують у державах — членах Ради Європи.

Приклади держав-членів

– Електронну систему правосуддя [«Lietuvos teismų informacinė sistema» (LITEKO)] було запроваджено в **Литві** у 2004 році. LITEKO скорочує кількість паперових файлів та дає сторонам провадження можливість подавати всі процесуальні документи й контролювати хід провадження у справі в режимі онлайн.

– **Хорватія** розробляє електронний комерційний реєстр, електронний земельний реєстр та інтегровану систему відстеження справ (eSpis). Ця система дасть змогу встановлювати зв'язок між учасниками судового процесу та судом у режимі онлайн.

Структура і зміст

8. Керівні принципи є не лише декларацією принципів, вони також мають за мету надання практичних порад.

Преамбула

9. У преамбулі надано пояснення стосовно того, що керівні принципи повинні застосовуватись лише тією мірою, якою вони не суперечать національному законодавству. Керівні принципи є інструментом, що не має обов'язкової сили. Вони не мають за мету гармонізацію національного законодавства держав-членів. Керівні принципи не слід тлумачити як такі, що надають конкретну юридичну цінність певним електронним доказам. Вони мають бути доволі загальними, щоб враховувати відмінності правових систем держав-членів, чия різноманітність визнається повністю.

Мета та сфера застосування

10. Керівні принципи мають за мету вирішення конкретних проблем, що пов'язані з електронними доказами, а саме: потенційна доказова цінність метаданих, легкість маніпуляції, знищення або видалення електронних доказів, а також участь третіх сторін, зокрема постачальників довірчих послуг, у збиранні й вилученні електронних доказів. Керівні принципи застосовують до вирішення спорів у цивільному та адміністративному провадженнях.

Приклади держав-членів

У **Словаччині** адміністративні органи приймають електронні докази, спираючись на загальне правило, відповідно до якого будь-що, що має доказову цінність для визначення фактичного стану справ, може бути подано як докази, якщо їх не отримано з порушенням закону.

Визначення

Електронні докази

11. Термін «електронні докази» (також існує інша назва — «цифрові докази») у цьому документі вжито в широкому значенні. Електронний доказ може мати форму тексту, відео, фото або звукозапису. Дані можуть походити з різних носіїв або способів доступу, таких як мобільні телефони, вебсторінки, бортові комп'ютери або GPS-реєстратори, зокрема дані, що зберігаються у сховищі поза межами контролю сторони. Електронні повідомлення (електронна пошта) є типовим прикладом електронних доказів, оскільки це докази, що надходять з електронного пристрою (комп'ютера або подібного до комп'ютера пристрою) і містять відповідні метадані (див. визначення «метаданих» нижче).

Метадані

12. Термін «метадані» — це дані, що характеризують або пояснюють інші дані. Іноді їх називають «цифровим відбитком» електронних доказів. Вони можуть містити важливі доказові дані, такі як дата й час створення чи зміни файла чи документа, або ім'я автора, а також дату й час надсилання даних. До метаданих зазвичай немає прямого доступу.

Довірчі послуги

13. Довірчі послуги відіграють важливу роль в ідентифікації, автентифікації та для безпеки онлайн-транзакцій. Визначення «довірча послуга» сформульовано відповідно до статті 3 (16) Регламенту (ЄС) № 910/2014 Європейського парламенту та Ради від 23 липня 2014 року (Регламент eIDAS). У цих керівних принципах також ідеться про конкретні довірчі послуги, пов'язані з «простими», «розширеними» або «кваліфікованими» електронними підписами й сертифікатами, що передбачає можливе застосування інших визначень, що їх ужито в Регламенті eIDAS.

Суд

14. Термін «суд» вжито в широкому значенні, що охоплює всі органи, які мають повноваження вирішувати правові спори між сторонами цивільного та адміністративного провадженнях. До них належать суди, трибунали та адміністративні органи.

Основні принципи

15. Перший принцип пояснює, що остаточне рішення стосовно потенційної доказової сили електронних доказів належить судам незважаючи на важливу роль експертів в їх оцінці. Водночас суди можуть керуватись презумпціями чинного законодавства (наприклад, надання конкретної доказової сили певному типу електронних доказів).

16. Згідно з другим принципом до електронних доказів не повинно бути дискримінаційного ставлення, їм не потрібно надавати переваги порівняно з іншими видами доказів. Щодо цього суди повинні застосовувати технологічно нейтральний підхід. Це означає, що має сприйматись будь-яка технологія, що дає змогу встановити автентичність, точність і цілісність даних.

Практика Європейського суду з прав людини

«Хоча стаття 6 Європейської конвенції з прав людини гарантує право на справедливий судовий розгляд, вона не встановлює жодних правил щодо допустимості доказів або способу їх оцінки, які, в першу чергу, є питаннями, що регулюються національним законодавством і національними судами» (див. *García Ruiz v. Spain*, no. 30544/96, п. 28).

17. Третій принцип стосується рівності сторін і надання рівних умов сторонам процесу щодо електронних доказів. Використання електронних доказів не повинно ставити сторони у цивільному чи адміністративному провадженні в невигідне становище. Наприклад, сторона повинна мати можливість оскаржити достовірність доказів. Якщо суд вимагає від сторони надати роздруківки електронних доказів, така сторона не повинна бути позбавлена можливості подати відповідні метадані.

Практика Європейського суду з прав людини

«Принцип рівності сторін вимагає надання кожній стороні розумної можливості представляти свою справу, включно з доказами, за таких умов, які не ставлять її у суттєво невигідне становище порівняно з протилежною стороною» (див. *Letinčić v. Croatia*, no. 7183/11, п. 48).

Керівні принципи

Докази в усній формі, що їх отримано за допомогою засобів дистанційного зв'язку

18. Докази, що їх отримано в усній формі за допомогою засобів дистанційного зв'язку, є електронними доказами для цілей цих керівних принципів (див. визначення «електронні докази» вище). Але цей розділ керівних принципів не стосується попередньо записаних усних

доказів, а стосується доказів в усній формі, які передані за допомогою відеоконференцзв'язку (передання синхронізованого зображення та звуку в режимі реального часу). Не всі усні докази можна отримати за допомогою віддаленого зв'язку. Слід також приділяти увагу технічним пристроям, які використовують для передання усних доказів. Дистанційно отримати докази можна за допомогою аналогових або цифрових технічних пристроїв, що забезпечують передання даних за допомогою електронного зв'язку, зокрема двостороннього зв'язку, який дозволяє передання зображення та звуку в режимі реального часу. Якщо показання потребують конфіденційності, може виникнути потреба в заходах або технічних рішеннях, за допомогою яких отримати доступ до зрозумілої форми комунікації можуть лише авторизовані особи. Пристрої, що можуть забезпечити цілісність телекомунікацій, дадуть суду та сторонам процесу адекватну та належну можливість викликати та допитати «віддаленого» свідка.

Приклади ЄС та національних правил

- Стаття 10(4) Регламенту Ради (ЄС) № 1206/2001 від 28 травня 2001 року про співпрацю між судами держав-членів у збиранні доказів у цивільних або комерційних справах передбачає, що суд, який звертається із запитом, може попросити суд, до якого надійшов запит, використовувати комунікаційні технології для отримання доказів, зокрема відеоконференцзв'язок.
- Стаття 803(3) Цивільного процесуального кодексу **Литви** встановлює, що «суди Литовської Республіки можуть просити іноземний суд використати комунікаційні технології (такі як відеоконференції) для отримання доказів».

19. Важливими чинниками для отримання усних доказів за допомогою дистанційного зв'язку є економічні міркування (наприклад, зменшення витрат), практичні складнощі (наприклад, хвороба, особа з інвалідністю) та намагання забезпечити процесуальну ефективність, щоб уникнути надмірної тривалості судового провадження. Якщо особа проживає в іншій державі, доцільним є отримання доказів за допомогою дистанційного зв'язку. Це стосується також групи осіб з віддаленим місцем проживання від судового округу того суду, який розглядає справу. Якщо особа є ключовим свідком, то для надання доказів доцільно забезпечити його/її фізичну присутність у суді. Інші фактори, які мають враховувати суди, стосуються участі перекладачів та пов'язаних із цим витрат. Важливо, щоб судді, правники, зокрема юристи-практики і працівники суду, знали про можливі відмінності між свідченнями, наданими безпосередньо в залі судових засідань, і свідченнями, наданими дистанційно. Наприклад, складно спостерігати за поведінкою свідків та тлумачити її під час надання доказів дистанційно.

20. Керівні принципи вимагають звернути увагу на процес, за допомогою якого докази надають дистанційно. Важливо переконатися, особливо стосовно доказів, що мають принципове значення для розгляду справи, що використовувані технології дають змогу поставити запитання під час надання доказів (якщо правила процедури це встановлюють). Цю вимогу навряд чи можна виконати через поганий інтернет-зв'язок або якщо доступ сторін до технічних засобів є обмеженим. У цьому разі одна зі сторін матиме суттєву перевагу в такому процесі. Слід використовувати всі можливі технічні засоби, аби дистанційне отримання доказів відбувалось так само, як і безпосередньо в залі суду.

21. Методи, які використовують, повинні належним чином захищати передання зображення або звуку від знищення, спотворення або несанкціонованого доступу. Суд може перевірити особу, яка дає показання, вимагаючи від неї/нього пред'явити відповідний документ, наприклад, дійсне посвідчення особи, паспорт або права водія.

22. Усі доступні системи зв'язку, як публічні, так і приватні, повинні забезпечувати щонайменше якість відеоконференції та шифрування відеосигналу для захисту від перехоплення. Можна отримувати докази через приватні засоби зв'язку, якщо це дозволяє національне законодавство, за умови, що використовувані рішення забезпечують достатню технічну безпеку та дотримання процесуальних гарантій. Приватні засоби зв'язку в цьому контексті — це система зв'язку, яка не є офіційною державною системою, спеціально створеною для отримання доказів у суді.

Використання електронних доказів

23. Суди повинні усвідомлювати важливість електронних даних, наданих сторонами як доказ у їх оригінальному форматі. У разі подання роздруківки електронного доказу суд, за клопотанням сторони або з власної ініціативи, може зобов'язати відповідну особу надати оригінал електронного доказу. Прикладом електронних доказів, які можуть мати важливе значення для вирішення спірного питання, за умови, що їх надано в оригінальному форматі, є дані геолокації. Більшість держав у всьому світі вже встановили у своєму законодавстві таке використання електронних доказів під час судового розгляду. Приклади таких положень наведено в Регламенті eIDAS.

Приклади держав-членів

Верховний Суд **Хорватії** (справа no. I Kž 696/04–7) підтвердив, що SMS-повідомлення можуть бути використані як докази в судовому провадженні, оскільки вони є джерелом інформації, рівнозначним будь-якому іншому письмовому контенту, що зберігається на інших носіях.

Приклад технології, яка буде спеціально використана для забезпечення доказів, — блокчейн.

Блокчейн — це нова технологія, яка може підвищити довіру до електронних доказів та їхню безпеку. Його можна визначити як розподілений реєстр, що посилається на список записів (блоків), які пов'язані й захищені криптографією та записані в децентралізованій одноранговій мережі. За структурою блокчейн є стійким до модифікації даних. Після запису дані в будь-якому окремому блоці не можуть бути змінені ретроспективно без зміни всіх наступних блоків, що потребує узгодженості більшості мереж. Це робить блокчейн зручним для отримання доказів.

У **США** пункт 1913 Правил про докази штату Вермонт передбачає: «(1) Цифровий запис, електронно зареєстрований у блокчейні, повинен бути автентифікований відповідно до Правил про докази штату Вермонт 902, якщо він супроводжується письмовою заявою кваліфікованої особи, наданою під присягою, із зазначенням кваліфікації особи для сертифікації та містить: (a) дату та час, коли запис було введено до блокчейну; (b) дату та час отримання запису з блокчейну; передбачає, що: (c) запис було збережено у блокчейні як регулярний вид діяльності; та (d) запис було зроблено в ході регулярно проведеної діяльності як звичайна практика».

У **Китаї** Інтернет-суд Ханчжоу 28 червня 2018 року підтвердив, що електронні дані, що ґрунтуються на блокчейні, можуть використовуватися як докази в правових спорах. Використання сторонньої блокчейн-платформи, яка є надійною і без конфлікту інтересів, стало юридичною підставою для доказу щодо порушення права інтелектуальної власності.

(http://www.xinhuanet.com/2018–06/28/c_1123051280.htm).

24. Для цілей керівного принципу 7 «розширений електронний підпис» — це електронний підпис, що відповідає вимогам, викладеним у статті 36 Регламенту eIDAS, а саме: a) унікально поєднаний із підписантом; b) дає можливість ідентифікувати підписанта; c) створений за допомогою використання даних, які підписант з великим ступенем конфіденційності може використовувати тільки під особистим контролем; та d) пов'язаний із даними, які підписуються, у такий спосіб, що подальша зміна даних може бути виявлена. Поняття «кваліфікований електронний підпис» означає розширений електронний підпис, створений за допомогою пристрою для створення кваліфікованого електронного підпису. Такий пристрій має надавати кваліфікований сертифікат електронного підпису. Це сертифікат, який надає фізична або юридична особа, що надають одну або більше кваліфіковану довірчу послугу («надавач кваліфікованої довірчої послуги») та мають відповідний дозвіл наглядового органу.

25. На сьогодні більшість електронних даних не мають будь-яких розширених або кваліфікованих електронних підписів і не захищені будь-яким іншим способом. Незважаючи на це, суди мають розглядати їх як електронні докази (хоча доказова цінність доказів може змінюватися

залежно від конкретного випадку), ураховуючи, наприклад, різноманітні довірчі послуги, пов'язані з електронним управлінням документами та ідентифікацією підписувачів, які доступні по всьому світові. Прикладом є біометричний підпис, спосіб отримання електронної версії власноручного підпису, коли особа наносить власноручний підпис на електронному пристрої за допомогою спеціальної ручки та блокнота. Залежно від чинного законодавства суд може визнати такий біометричний підпис рівноцінним власноручному підписові на папері.

26. Метадані забезпечують необхідний контекст для оцінки доказів (даних) так само, як поштова марка надає контекст для оцінки звичайного (паперового) листа та його змісту. Електронні докази зазвичай містять метадані й суди повинні знати про їх потенційну доказову цінність. Вони можуть використовуватись для відстеження та ідентифікації джерела та адресата повідомлення, даних про пристрій, який створив електронні докази, дати, часу, тривалості та типу доказів. Метадані можуть бути відповідними або як непрямі докази (наприклад, вказуючи на найбільш релевантну версію документа), або як прямі докази (наприклад, у разі маніпулювання даними файла). Керівні принципи також стосуються втрачених метаданих.

Приклади судової практики щодо метаданих в ***Ірландії***

Метадані вважалися важливими для автентифікації походження документів/матеріалів, створених в електронній формі *[Koger Inc. & Koger (Dublin) Ltd v O'Donnell & Others (2010) IEHC 350]*.

http://www.courts.ie/Judgments.nsf/0/1F8979ED6FCCF69C802577CB003B6360

Ірландські суди постановили, що зобов'язання розкриття доказів, що зберігаються в електронній формі, передбачає розкриття метаданих первинних документів, якщо це було б доречно *[Sretaw v. Craven House Capital PLC (2017) IEHC 580; Gallagher v RTE (2017) IEHC 237]*.

http://www.courts.ie/Judgments.nsf/0/D5847A097092C099802581C40045290E

27. Роздруківками електронних доказів можна легко маніпулювати, оскільки вони не містять метаданих або інших прихованих даних. Це означає, що коли сторона надає роздруківку з екрана веббраузера, таку роздруківку навряд чи можна визнати достовірним електронним доказом. Роздруківка — це копія зображення на екрані, яку можна змінити дуже легко, адже для цього не потрібні спеціальні вимоги до програмного чи апаратного забезпечення.

Приклади держав-членів

Апеляційний суд **Литви** вирішив, що моментальні копії екрана комп'ютера (скріншоти) не викликають довіри (27 квітня 2018 р., справа No. e2A-226–516/2018).

http://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=fbf43bd0–2c01–41a5–9f69–3be0c2ef3acb

Збирання, вилучення та передання

28. Електронні докази за своєю природою є вразливими: можуть бути змінені, пошкоджені або знищені внаслідок неналежного поводження з ними або дослідження. З огляду на це може бути вжито спеціальних запобіжних заходів для належного збирання таких доказів. Невиконання цієї вимоги може зробити їх непридатними для використання або призвести до неправильного висновку. Сторони відповідають за належне збирання електронних доказів у цивільному та адміністративному судочинстві. Для різних типів даних можуть знадобитися різні способи збирання. Заходи, яких ужито для захисту та збирання електронних доказів, не повинні впливати на цілісність цих доказів. У дуже важливих справах сторони повинні розглянути можливість збирання електронних доказів за допомогою IT-фахівця або нотаріальних служб. Судді, правники, зокрема юристи-практики, повинні знати, що дані часто зберігаються в мережевих службах. Це стосується як хмарних обчислень, так і надання послуг онлайн.

29. Хоча судді, правники, зокрема юристи-практики, покращили свої знання і досвід роботи з електронними доказами, але конкретних стандартів досі немає. Для збирання та вилучення електронних доказів у держав-членів може виникнути потреба в спеціальних інструментах і процедурах. Водночас судді, правники, зокрема юристи-практики, повинні прагнути забезпечити цілісність, конфіденційність і безпеку таких даних. Це передбачає збереження захищених резервних копій у разі відмови одного із засобів зберігання. Електронні дані необхідно зберігати в їх оригінальному форматі.

30. Хоча використання даних може мати суто національний характер, дедалі ймовірним є те, що воно може мати транскордонний характер за участю інших держав. Прикладом є розташування в іншій державі інфраструктури, яка використовується для оброблення або зберігання даних, або розташування постачальника, який забезпечує зберігання або оброблення даних. Слід заохочувати пряму співпрацю між судами та постачальниками довірчих чи хмарних послуг у транскордонних справах. У роботі з електронними доказами судді, правники, зокрема юристи-практики, можуть ураховувати такі фактори, як

місце розташування постачальника послуг, місце оброблення даних і місцеві закони, що регулюють доступ до даних.

Приклад транскордонної технології

Спільне використання даних (хмари) — це зберігання різних частин бази даних на різних серверах, які можуть знаходитись у різних фізичних місцях. Це стало звичною технікою безпеки. Глобальний характер інтернету та дедалі ширше використання хмарних сервісів все менше припускають, що доступ до даних має суто внутрішній характер.

31. Між національними процесуальними правилами щодо збирання доказів існують суттєві відмінності. Суди, які використовують отримані за кордоном докази, повинні брати до уваги ці відмінності. Рекомендовано, щоб суди тісно співпрацювали у цьому питанні під час транскордонного отримання електронних доказів. Суд, який надіслав запит, повинен бути проінформований про процесуальні правила, які використовує суд, який отримав запит, щоб адаптувати свою оцінку електронних доказів, якщо це доцільно. Зокрема, отримання доказів за кордоном не повинно призводити до порушення основних принципів і норм процесуального права, таких як рівність сторін.

32. Ефективність провадження підвищується, коли є можливість передавати електронні докази до інших судів в оригінальному форматі, а не роздруковувати їх та надсилати. Передані електронні дані повинні супроводжуватися метаданими. Це передбачає використання додаткових метаданих, створених судами для належного управління даними та їх безперебійного передання іншим судам. Наявність структурованих метаданих дає судам контроль над доказами. Копія електронного доказу в ідеалі повинна використовуватися для передання до іншого суду.

33. Передання електронних доказів за допомогою електронних засобів можна стимулювати і прискорювати через впровадження спільних технічних стандартів, форматів файлів та оцифрування національних судових та адміністративних систем. З огляду на вищий ризик знищення електронних доказів необхідно на національному рівні визначити процедури, що забезпечуватимуть безпечне передання електронних доказів.

34. Під час передання доказів слід ураховувати цілісність, збереженість і безпеку даних. Надійні послуги, такі як довірчі послуги, можуть бути важливими для забезпечення належного передання електронних доказів. Якщо передання вимагає конфіденційності, може виникнути потреба у вжитті певних заходів або застосуванні технічних рішень, таких як шифрування, що забезпечуватимуть доступ до безпечного зв'язку лише авторизованим особам.

Відповідність

35. Сторона може легко надати непотрібну велику кількість електронних даних, що ускладнить або унеможливить ефективне опрацювання їх судом та іншими учасниками. Отже, активне управління судом електронними доказами для обмеження їх надання лише суворою необхідністю вирішення справи має важливе значення. Під час активного управління даними слід дотримуватися принципу пропорційності. Кожен запит на надання електронних доказів слід розглядати по суті, зокрема, з точки зору його корисності для цілей доказування. Сторони повинні мати право висловити заперечення стосовно таких запитів.

36. Судді та працівники судової системи, зокрема юристи-практики, повинні знати про можливу потребу в технічній експертизі та розуміти, де можуть знадобитися подальші дослідження або додаткові спеціальні знання, такі як висновок експерта. Експерти повинні бути компетентними та мати достатню підготовку для виконання поставленого завдання.

Достовірність

37. Відокремлення цифрової ідентичності від фізичної може призводити до виникнення проблем, пов'язаних із достовірністю доказів. Суди мають прагнути насамперед ідентифікувати особу автора електронних даних. Якщо у чинному законодавстві не зазначено способу встановлення особи, її можна визначити у будь-який об'єктивний спосіб, наприклад, за допомогою електронного підпису або перевірки електронної адреси, з якої було надіслано документ.

38. Довірчі служби можуть надавати технологічні механізми, що забезпечують достовірність доказів. Наприклад, сертифікати електронних підписів, які іноді називають «цифрові ідентифікатори» особи (digital ID), можуть гарантувати як автентичність, так і цілісність даних. Якщо особа підписувача, який накладає електронний підпис, викликає сумніви, суд може вимагати від постачальника послуг, пов'язаних з електронним підписом, надати пояснення з питань, щодо яких він має право надавати докази. Позначка часу (сертифікація часу) може бути не менш важливою для підтвердження цілісності електронних даних.

Приклад довірчих послуг

Позначка часу — це механізм, що дає змогу довести цілісність даних. Він демонструє, що дані існували в певний момент і не були змінені. Позначка часу надає цінність електронним доказам, оскільки містить відповідні метадані про момент їх створення.

39. Наскільки дозволяє чинне законодавство та на розсуд суду, заохочується та рекомендується судам приймати як докази всі види електронних доказів. У разі виникнення спору сторони зазвичай визначають питання, які необхідно вирішити, і якщо сторона не порушує питання щодо автентичності електронних доказів, суду не потрібно порушувати це питання з власної ініціативи. Лише якщо сторона оскаржує електронні докази, від сторони, яка бажає покладатися на докази, можна вимагати продемонструвати їх автентичність, наприклад, через подання метаданих або запиту на відповідне доручення для отримання додаткових даних від інших осіб, таких як постачальники довірчих послуг.

40. Конкретне посилання на дискреційні повноваження суду в керівних принципах 21 і 22 підкреслює важливу роль дискреційних повноважень суду стосовно предмета цих керівних принципів.

41. Як і з будь-якими іншими доказами, сторона судового провадження може оскаржити докази. У такому разі сторона може просити суд виключити докази, наприклад, через те, що автора даних неможливо належним чином ідентифікувати. Достовірність електронних даних може бути доведена в будь-який спосіб, наприклад, за допомогою кваліфікованого електронного підпису або іншого подібного методу ідентифікації та забезпечення цілісності даних. Проте застосовне законодавство має визначити юридичну силу електронних підписів, наприклад, забезпечивши, що лише кваліфікований електронний підпис повинен мати юридичну силу, еквівалентну власноручному підпису (вологими чорнилами). Наприклад, застосовне законодавство може вимагати, щоб пристрої, які використовують для генерування підписів, перебували під виключним контролем підписувача.

Кваліфікований електронний підпис у ЄС

Для забезпечення цілісності даних суди не повинні проводити спеціального аналізу технології, яку використовують для створення кваліфікованих електронних підписів. Достатньо перевірити реєстр сертифікованих постачальників довірчих послуг ЄС.

42. Керівний принцип 23 стосується тягаря доказування. Більш уразливі категорії осіб, такі як споживачі та діти, можуть технічно та/або економічно не мати можливості надати електронні докази. Якщо вони отримують перевагу від законодавчих положень, які полегшують або скасовують тягар доказування, ці законодавчі положення мають перевагу над керівними принципами. Суди повинні відігравати активну роль у справах, у яких залучені вразливі категорії осіб.

43. Залежно від національної правової системи слід поважати доказову цінність публічних (офіційних) електронних систем, які генерують

електронні докази. Наприклад, дані з електронних публічних реєстрів можуть розглядатися як офіційний документ, що призводить до презумпції їхньої достовірності. Електронний запис іншого провадження може розглядатися як достовірне відображення фактів без ризику людської помилки (наприклад, порівнюючи його із вмістом, який суддя продиктував для внесення до протоколу).

Приклади публічних довірчих послуг у державах-членах

Існують конкретні види довірчих послуг, які надають на національному рівні, такі як «Довірчий профіль» (Trusted Profile) (**Польща**), «Електронне архівування та цифровізація» (Electronic archiving and digitalization) (**Бельгія**), «Довгострокове збереження інформації/документів, Платформа LEXNET для обміну інформацією між судовими органами та широким колом юридичних операторів» (Information/documents long term preservation, LEXNET Platform for exchanging information between the Judicial Bodies and a wide range of legal operators) (**Іспанія**).

Зберігання і забезпечення збереження

44. Зберігання в розумінні цих керівних принципів стосується тривалості цивільного чи адміністративного провадження. Електронні докази можуть зберігатися в судах протягом періоду судового провадження, наприклад, на портативних пристроях (картах пам'яті), серверах, системах резервного копіювання та інших місцях зберігання даних (хмарні обчислення). Суди повинні зберігати електронні докази в їх оригінальній формі (не як роздруківки) відповідно до чинного законодавства. Важливим є також питання кібербезпеки, що означає, що суди повинні застосовувати проактивні підходи для захисту цілісності електронних доказів від кіберзагроз, зокрема від пошкоджень або несанкціонованого доступу. Зосереджуючись на запобіганні, суди можуть попередити вплив кіберзагроз на цілісність електронних доказів і зменшити загальні ризики кібербезпеки. Не можна надавати доступ до електронних доказів особам, які не мають відповідного дозволу, незалежно від способу зберігання.

45. Збережені електронні докази можуть бути пов'язані зі стандартизованими метаданими, що описують контекст їх створення, а також з існуючими зв'язками з іншими електронними записами. Впровадження міжнародних стандартів для метаданих забезпечує рівень узгодженості під час зберігання електронних доказів. Оскільки створення стандартизованих метаданих може бути складним і займати багато часу, суди можуть використовувати інструменти, які допомагають створити стандартизовані метадані.

Приклад рішення, що використовується для стандартизованих метаданих

Існує ряд інструментів для створення стандартизованих метаданих. Наприклад, інструмент управління метаданими може створити файл XML (розширювана мова розмітки), що містить метадані, пов'язані з електронними доказами. Робота з файлами XML не потребує сучасного програмного забезпечення. Такий формат є водночас стандартизованим і доволі гнучким для застосування в різних інформаційних системах. Це може спростити як зберігання, так і пошук електронних доказів.

З огляду на це має бути дотримано міжнародних стандартів, які застосовують до метаданих, наприклад, ідеться про ті з них, що опублікували міжнародні спільноти з питань стандартизації, такі як ISO (Міжнародна організація стандартизації).

46. Керівний принцип 27 щодо збереження електронних доказів застосовують як до зберігання, так і до архівування електронних доказів, яке відбувається після закінчення судового провадження. Електронні докази потрібно зберігати та архівувати в оригінальній формі, у якій їх було створено, передано, отримано, та яка суттєво не змінює даних. Електронні докази мають бути доступними у зручному для читання форматі протягом усього судового провадження. Цілісність електронних доказів має бути збережена на всіх етапах судового провадження.

Архівування

47. Принципи щодо архівування охоплюють період після судового провадження та враховують Рекомендацію Rec(2003)15 Комітету міністрів Ради Європи державам-членам щодо архівування електронних документів у юридичному секторі. Національне законодавство зазвичай встановлює строки зберігання та технічні умови архівування електронних документів. Системи, які використовують для архівування, мають бути безпечними, гарантувати використання з можливістю відстеження та враховувати повагу до приватності. Необхідно вжити відповідних технічних та організаційних заходів щодо забезпечення захисту електронних доказів і запобігання несанкціонованому доступу до них. Електронний носій інформації, якщо його використовують, має бути забезпечений сертифікатом ідентифікації, який містить основні дані про нього. Такий носій повинен бути в належний спосіб захищеним, особливо від втрати, шкідливого впливу хімічних речовин, тепла, світла, радіації, магнітних або електричних полів і від механічних пошкоджень.

48. Архівні служби повинні мати можливість перевірити, наприклад за допомогою електронних підписів або інших електронних процедур, що електронні докази архівують кваліфіковані фахівці або компетентні організації і до даних не було внесено зміни. Необхідно в належний

спосіб архівувати як дані про електронні підписи, за допомогою яких підписано електронні документи, так і дані для перевірки цих підписів. Держави-члени повинні забезпечити організації в юридичному секторі, на які законом покладено обов'язок архівування, необхідними ресурсами для архівування електронних доказів.

49. Міграція означає зміну носія інформації для збереження доступу до електронних доказів. Нехтування міграцією може призвести до нечитабельності даних. Електронні документи можуть архівуватися шляхом періодичного перенесення даних з одного носія інформації на інший або з одного формату в інший. Міграція також повинна застосовуватися до метаданих архівованих електронних документів. Перехід на новий носій даних має відбуватися регулярно, беручи до уваги, наприклад, погіршення якості та зношення носія, про який йде мова, і до того, як вони застаріють через технологічний розвиток носіїв і обладнання. Перехід на новий носій або формат зберігання слід здійснювати, коли це доречно, з огляду на розвиток технологій.

Приклад довготривалого рішення

Дані можна перенести на мережеві пристрої, такі як хмарні обчислення. Ці пристрої постійно вдосконалюються завдяки технологічному розвитку середовища та апаратного забезпечення. Хмарне архівування також може забезпечити кращий контроль за витратами за рахунок оплати лише необхідного простору.

Приклад застарілого рішення

CD, DVD чи інші оптичні диски стають нечитабельними через фізичне чи хімічне зношення. Причини цього ефекту є різними: окислення відбивного шару, фізична потертість та стирання поверхонь або країв диска, зокрема видимі подряпини, а також інші типи реакцій із забрудненнями.

Підвищення рівня обізнаності, моніторинг, професійна підготовка та навчання

50. Просування цих керівних принципів передбачає їх поширення серед судів та юристів-практиків, переклад керівних принципів на місцеві мови, організацію семінарів та конференцій на тему електронних доказів.

51. Перегляд технічних стандартів щодо електронних доказів може передбачати, наприклад, нові способи їх зберігання, збереження та архівування.

52. Доступ до міждисциплінарного навчання з питань роботи з електронними доказами є необхідним для суддів, правників, зокрема юристів-практиків. Навчання може охоплювати опрацювання конкретних проблем, пов'язаних з електронними доказами, такі як важливість

метаданих, важливість позначок часу та використання хмарних обчислень або блокчейну під час збирання та вилучення доказів, необхідність надання електронних доказів в оригінальній формі, а не лише як скановані зображення чи роздруківки.

53. Обізнаність щодо ширшого цифрового контексту та використання технологій, таких як хмарні обчислення, довірчі послуги або блокчейн, є важливою для суддів, правників, зокрема юристів-практиків.

54. Вивчення матеріальних та процесуальних питань у контексті електронних доказів має бути невід'ємною частиною юридичної освіти.

Бібліографія та інші ресурси

1) Рекомендація Rec(2003)15 Комітету міністрів Ради Європи державам-членам щодо архівування електронних документів в юридичному секторі.

2) Biasiotti M., Mifsud Bonnici J., Cannataci J., Turchi F. (eds.). *Handling and Exchanging Electronic Evidence across Europe*, Springer 2018.

3) Forgó N., Hawellek C., Knoke F., Stoklas J. *The Collection of Electronic Evidence in Germany — a Spotlight on Recent Legal Developments and Court Rulings*, in: *New Technology, Big Data and the Law* (ed. Forgó, Fenwick, Corrales), Springer 2017.

4) Morabito V. *Business Innovation Through Blockchain. The B³ Perspective*, Springer International Publishing AG Cham 2017.

5) Hofmann E., Strewe U., Bosia N. *Supply Chain Finance and Blockchain Technology. The Case of Reverse Securitisation*, Springer Munich 2018.

6) Singer P., Friedman A. *Cybersecurity and cyberwar: What everyone needs to know*, Oxford, Oxford University Press 2014.

7) Mason S. *The use of electronic evidence in civil and administrative law proceedings and its effect on the rules of evidence and modes of proof. A comparative study and analysis*. Report prepared by Stephen Mason assisted by Uwe Rasmussen. Strasbourg, 27 July 2016, CDCJ(2015)14-final.

8) Albert J. *Study on possible national legal obstacles to full recognition of electronic processing of performance information on construction products (under the construction products regulation), notably within the regimes of civil liability and evidentiary value*, Final General Report, 30-CE-0517177/00–3630-CE-0517177/00–36.

9) Schünemann W., Baumann M. Editors (ed.) *Privacy, Data Protection and Cybersecurity in Europe*, Springer International 2017.

10) Voigt P., von dem Bussche A. *The EU General Data Protection Regulation (GDPR). A Practical Guide*, Springer International 2017.

11) Mason S., Seng D. (ed.) *Electronic Evidence*, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017.

12) Mason S. (ed.), *International Electronic Evidence*, British Institute of International and Comparative Law, 2008.

13) Mason S. *Electronic Signatures in Law Institute of Advanced Legal Studies for the SAS Humanities Digital Library*, School of Advanced Study, University of London 2016.

14) Mason S. *Electronic Disclosure A Casebook for Civil and Criminal Practitioners*, PP Publishing 2015.

15) Electronic Evidence: Model Policy Guidelines & Legislative Texts, Establishment of Harmonized Policies for the ICT Market in the ACP countries, HIPCAR project "Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures" 2013, https://www.itu.int.

16) Capriolli E. *Droit international de l'économie numérique*, Paris, Litec, 2007.

17) Biasiotti M. A., Turchi F., Epifani M. *The EVIDENCE Project: bridging the Gap in the Exchange of Digital Evidence Accross Europe*, SADFE 2015, http://sadfe2015.safesocietylabs.com/wp-content/uploads/2015/10/SADFE-2015-Proceedings.pdf (October 2015).

COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES

1949.2019

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

MINISTERS' DEPUTIES | CM Documents | **CM(2018)169-add1final** | 30 January 2019

Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings

(Adopted by the Committee of Ministers on 30 January 2019, at the 1335th meeting of the Ministers' Deputies)

The Committee of Ministers,

Considering that the aim of the Council of Europe is to achieve a greater unity between the member States, in particular by promoting the adoption of common rules in legal matters;

Considering the necessity of providing practical guidance for the handling of electronic evidence in civil and administrative proceedings to courts and other competent authorities with adjudicative functions; professionals, including legal practitioners; and parties to proceedings;

Considering that these guidelines seek to provide a common framework rather than a harmonisation of the national legislation of the member States;

Considering the need to respect the diversity in the legal systems of the member States;

Acknowledging the progress made in the member States towards the digitisation of their justice systems;

Noting, nonetheless, obstacles to the effective management of electronic evidence within justice systems, such as the lack of common standards and the diversity and complexity of evidence-taking procedures;

Highlighting the need to facilitate the use of electronic evidence within legal systems and in court practices;

Recognising the need for member States to examine current deficiencies in the use of electronic evidence and to identify the areas where electronic evidence principles and practices could be introduced or improved;

Noting that the aim of these guidelines is to provide practical solutions to the existing deficiencies in law and practice,

Adopts the following guidelines to serve as a practical tool for the member States, to assist them in adapting the operation of their judicial and other dispute-resolution mechanisms to address issues arising in relation to electronic evidence in civil and administrative proceedings, and invites them to disseminate these guidelines widely with a view to their implementation by those responsible for, or otherwise handling, electronic evidence.

Purpose and scope

The guidelines deal with:

- oral evidence taken by a remote link;
- use of electronic evidence;
- collection, seizure and transmission of evidence;
- relevance;
- reliability;
- storage and preservation;
- archiving;
- awareness-raising, review, training and education.

The guidelines are not to be interpreted as prescribing a specific probative value for certain types of electronic evidence and are to be applied only insofar as they are not in conflict with national legislation.

The guidelines aim to facilitate the use and management of electronic evidence within legal systems and in court practices.

Definitions

For the purposes of these guidelines:

Electronic evidence

"Electronic evidence" means any evidence derived from data contained in or produced by any device, the functioning of which depends on a software program or data stored on or transmitted over a computer system or network.

Metadata

"Metadata" refers to electronic information about other electronic data, which may reveal the identification, origin or history of the evidence, as well as relevant dates and times.

Trust service

"Trust service" means an electronic service which consists of:

d. the creation, verification and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services; or

e. the creation, verification and validation of certificates for website authentication; or

f. the preservation of electronic signatures, seals or certificates related to those services.

Court

The term "court" includes any competent authority with adjudicative functions in the performance of which it handles electronic evidence.

Fundamental principles

It is for courts to decide on the potential probative value of electronic evidence in accordance with national law.

Electronic evidence should be evaluated in the same way as other types of evidence, in particular regarding its admissibility, authenticity, accuracy and integrity.

The treatment of electronic evidence should not be disadvantageous to the parties or give unfair advantage to one of them.

Guidelines

Oral evidence taken by remote link

1. Oral evidence can be taken remotely, using technical devices, if the nature of the evidence so permits.
2. When deciding whether oral evidence can be taken remotely, the courts should consider, in particular, the following factors:
   - the significance of the evidence;
   - the status of the person giving evidence;

– the security and integrity of the video link through which the evidence is to be transmitted;

– costs and difficulties of bringing the relevant person to court.

3. When taking evidence remotely, it is necessary to ensure that:

   a. the transmission of the oral evidence can be seen and heard by those involved in the proceedings and by members of the public where the proceedings are held in public; and

   b. the person being heard from a remote location is able to see and hear the proceedings to the extent necessary to ensure that they are conducted fairly and effectively.

4. The procedure and technologies applied to the taking of evidence from a remote location should not compromise the admissibility of such evidence and the ability of the court to establish the identity of the persons concerned.

5. Irrespective of whether evidence is transmitted via a private or a public connection, the quality of the videoconference should be ensured and the video signal encrypted to protect against interception.

Use of electronic evidence

6. Courts should not refuse electronic evidence and should not deny its legal effect only because it is collected and/or submitted in an electronic form.

7. In principle, courts should not deny the legal effect of electronic evidence only because it lacks an advanced, qualified or similarly secured electronic signature.

8. Courts should be aware of the probative value of metadata and of the potential consequences of not using it.

9. Parties should be permitted to submit electronic evidence in its original electronic format, without the need to supply printouts.

Collection, seizure and transmission

10. Electronic evidence should be collected in an appropriate and secure manner, and submitted to the courts using reliable services, such as trust services.

11. Having regard to the higher risk of the potential destruction or loss of electronic evidence compared to non-electronic evidence, member States should establish procedures for the secure seizure and collection of electronic evidence.

12. Courts should be aware of the specific issues that arise when dealing with the seizure and collection of electronic evidence abroad, including in cross-border cases.

13. Courts should co-operate in the cross-border taking of evidence. The court receiving the request should inform the requesting court of all the conditions, including restrictions, under which evidence can be taken by the requested court.

14. Electronic evidence should be collected, structured and managed in a manner that facilitates its transmission to other courts, in particular to an appellate court.

15. Transmission of electronic evidence by electronic means should be encouraged and facilitated in order to improve efficiency in court proceedings.

16. Systems and devices used for transmitting electronic evidence should be capable of maintaining its integrity.

Relevance

17. Courts should engage in the active management of electronic evidence in order, in particular, to avoid excessive or speculative provision of, or demand for, electronic evidence.

18. Courts may require the analysis of electronic evidence by experts, especially when complex evidentiary issues are raised or where manipulation of electronic evidence is alleged. Courts should decide whether such persons have sufficient expertise in the matter.

Reliability

19. As regards reliability, courts should consider all relevant factors concerning the source and authenticity of the electronic evidence.

20. Courts should be aware of the value of trust services in establishing the reliability of electronic evidence.

21. As far as a national legal system permits, and subject to the court's discretion, electronic data should be accepted as evidence unless the authenticity of such data is challenged by one of the parties.

22. As far as a national legal system permits, and subject to the court's discretion, the reliability of the electronic data should be presumed, provided that the identity of the signatory can be validated and the integrity of the data secured, unless and until there are reasonable doubts to the contrary.

23. Where applicable law provides special protection for categories of vulnerable persons that law should have precedence over these guidelines.

24. As far as a national legal system so provides, where a public authority transmits electronic evidence independently of the parties, such evidence is conclusive as to its content, unless and until proved to the contrary.

Storage and preservation

25. Electronic evidence should be stored in a manner that preserves readability, accessibility, integrity, authenticity, reliability and, where applicable, confidentiality and privacy.

26. Electronic evidence should be stored with standardised metadata so that the context of its creation is clear.

27. The readability and accessibility of stored electronic evidence should be guaranteed over time, taking into account the evolution of information technology.

Archiving

28. Courts should archive electronic evidence in accordance with national law. Electronic archives should meet all safety requirements and guarantee the integrity, authenticity, confidentiality and quality of the data as well as respect for privacy.

29. The archiving of electronic evidence should be carried out by qualified specialists.

30. Data should be migrated to new storage media when necessary in order to preserve accessibility to electronic evidence.

Awareness-raising, review, training and education

31. Member States should promote awareness of the benefits and value of electronic evidence in civil and administrative proceedings.

32. Member States should keep technical standards related to electronic evidence under review.

33. All professionals dealing with electronic evidence should have access to the necessary interdisciplinary training on how to handle such evidence.

34. Judges and legal practitioners should be aware of the evolution of information technologies which may affect the availability and value of electronic evidence.

35. Legal education should include modules on electronic evidence.

COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES

1949.2019

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

MINISTERS' DEPUTIES	CM Documents	CM(2018)169-add2	17 December 2018[2]

1335th meeting, 30 January 2019

10 Legal questions

10.1 European Committee on Legal Co-operation (CDCJ)

Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings — Explanatory Memorandum

Item to be considered by the GR-J at its meeting on 17 January 2019

Contents

2 This document has been classified restricted until examination by the Committee of Ministers.

General comments

Why a new instrument?

1. Courts are being increasingly called upon to deal with electronic evidence or to authorize the production of electronic data by parties and other persons involved in civil or administrative proceedings.
2. To date, there are few standards applicable to electronic evidence at international, European or national level. Significant deficiencies remain in the law and practice applicable to electronic evidence.
3. The purpose of these guidelines on electronic evidence is not to establish binding legal standards but rather to serve as a practical tool for the Council of Europe member States in adapting the operation of their judicial and other dispute resolutions mechanisms to address issues arising in relation to electronic evidence. In this respect, the guidelines are intended to strengthen the efficiency and quality of justice.
4. Electronic evidence differs in many respects from other types of evidence and specific challenges arise when dealing with electronic evidence in the courts and other competent authorities with adjudicative functions. These challenges point towards the need to enhance knowledge about electronic evidence and improve the handling of electronic evidence in civil and administrative proceedings.

Working method and the drafting process

5. The issue of electronic evidence falls within the competence of the European Committee on Legal Co-operation (CDCJ) which is the Council of Europe intergovernmental body responsible for the standard-setting activities of the Council of Europe in the field of civil and administrative law.
6. The guidelines were drawn up by a drafting group and are based on the proposals made by CDCJ members and designated experts and were prepared at meetings held in 2018. The said meetings also involved the relevant Council of Europe bodies with expertise and responsibilities in this field.
7. The drafting group took into consideration experience arising from the operation of electronic justice mechanisms existing in member States.

Member States examples

- The electronic justice system ("Lietuvos teismų informacinė sistema ("LITEKO")) was set up in **Lithuania** in 2004. LITEKO reduces paper cases, and allows the participants of the case to submit all procedural documents on the Internet web page and monitor the progress of the case.

- **Croatia** is developing an e-Commercial Register, an e-Land Register and an integrated case-tracking system ("eSpis"). The latter will allow to electronic communication between parties to court proceedings and a court.

Structure and content

8. The guidelines are not only a declaration of principles but aspire to giving practical advice.

Preamble

9. The preamble explains that the guidelines are to be applied only in so far as they do not contradict national legislation. The guidelines are a non-binding instrument. They are not aimed at harmonisation of the national legislation of the member States. The guidelines are not to be interpreted as prescribing a specific legal value for certain electronic evidence. They are intended to be general enough to accommodate all the different legal systems. The diversity in the legal systems of the member States is fully acknowledged.

Purpose and scope

10. The guidelines aim to ensure that specific challenges related to electronic evidence are addressed, such as the potential probative value of metadata, the ease of manipulation, the distortion and erasure of electronic evidence, and the involvement of a third party (including trust services providers in the collection and seizure of electronic evidence). The guidelines apply to the resolution of disputes in both civil and administrative proceedings.

Member States example

In **Slovakia**, the administrative bodies are open to receiving electronic evidence, based on the general rule that anything that has evidentiary value for the purpose of determining the actual state of affairs may be submitted as evidence, as long as such evidence is not obtained in violation of the law.

Definitions

Electronic evidence

11. A broad definition of "electronic evidence" (also referred to as "digital evidence") is adopted. It may take the form of text, video, photographs or sounds. Data may originate from different carriers or access methods, such as mobile phones, webpages, on-board computers or GPS recorders, including data stored in a storage space outside the party's own control. Electronic messages (e-mail) are a typical example of electronic evidence, as it is evidence originating from an electronic device (computer or computer like-device) and which includes the relevant metadata (see the definition of "metadata" below).

Metadata

12. "Metadata" means data about other data. It is sometimes referred to as the "digital fingerprint" of electronic evidence. It may include important evidentiary data, such as the date and time of creation or modification of a file or document, or the author and the date and time of sending the data. Metadata is usually not directly accessible.

Trust service

13. Trust services play a critical role in the identification, authentication and security of online transactions. The definition of "trust service" is formulated in accordance with Article 3 (16) of the Regulation (EU) No 910/2014 of the European Parliament and Council of 23 July 2014 (the eIDAS Regulation). In these guidelines, reference is also made to specific trust services related to "simple", "advanced" or "qualified" electronic signatures and certificates, which implies possible application of other definitions adopted in the eIDAS Regulation.

Court

14. A broad definition of "court" is included in order to cover all authorities with competences to adjudicate legal disputes between parties to civil and administrative proceedings. They include courts, tribunals and administrative bodies.

Fundamental principles

15. The first principle explains that although the role of the experts in the evaluation of electronic evidence is important, it is ultimately for the courts to decide on the potential probative value of electronic evidence. In doing so, courts may be bound by applicable law presumptions (e.g. providing specific probative value for certain type of electronic evidence).

16. The second principle requires that electronic evidence should be neither discriminated against nor privileged over other types of evidence. In this respect courts should also adopt a technologically neutral approach. This means that any technology that enables authenticity, accuracy and integrity of data to be established should be accepted.

European Court of Human Rights' case-law

"While Article 6 of the Convention of Human Rights guarantees the right to a fair hearing, it does not lay down any rules on the admissibility of evidence or the way it should be assessed, which are therefore primarily matters for regulation by national law and the national courts" (see *García Ruiz v. Spain*, no. 30544/96, paragraph 28).

17. The third principle refers to the equality of arms and equal treatment of the parties to proceedings with regard to electronic evidence. Treatment

of electronic evidence should not be disadvantageous to parties to civil or administrative proceedings. For example, a party should not be deprived of the possibility to challenge the authenticity of evidence. If a court requests a party to submit printouts of electronic evidence, such party should not be deprived of the opportunity to submit relevant metadata.

European Court of Human Rights' case-law

"The principle of the equality of arms implies that each party must be afforded a reasonable opportunity to present his case — including his evidence — under conditions that do not place him at a substantial disadvantage vis-à-vis his opponent" (see *Letinčić v. Croatia*, no. 7183/11, paragraph 48).

Guidelines

Oral evidence taken by remote link

18. Oral evidence taken by remote link is considered as electronic evidence for the purpose of these guidelines (see the definition of "electronic evidence" above). This section of the guidelines does not, however, cover pre-recorded oral evidence. It relates to oral evidence in the form of videoconferencing (transmission of synchronized image and sound in real time). Not all oral evidence can be taken by remote link. Attention must be given to the technical devices. It may be carried out remotely using analogue or digital technical devices enabling telecommunication transmission, in particular real-time two-way communication allowing for the transmission of image and sound. If the testimony requires confidentiality, it may be necessary to apply measures or technical solutions which can limit access to the intelligible form of secure communication only to authorized persons. Devices which can ensure the integrity of telecommunications will allow the court and the parties an adequate and proper opportunity to challenge and question the "remote" witness.

Examples of EU and national regulations

- Article 10(4) of the Council Regulation (EC) No 1206/2001 of 28 May 200 1 on cooperation between the courts of the member States in the taking of evidence in civil or commercial matters provides that the requesting court may ask the requested court to use communication technology, in particular videoconferencing.
- Art. 803(3) of the **Lithuanian** Code of Civil Procedure establishes that "the courts of the Republic of Lithuania can ask a foreign court to use communication technology (such as videoconferencing) for taking evidence".

19. The decisive factors for whether oral evidence is taken by remote link are economic considerations (e.g. reduction of the costs involved), practical difficulties (e.g. illness, disability of a witness) and procedural efficiency efforts to avoid excessive length of proceedings. If a person is resident

in a different country, it may be more appropriate to question him/her remotely. The same principle relates to a group of persons that has a distant place of residence from the judicial district of the court hearing the case. If a person is a key witness it may be more appropriate to question him/her at court. Other factors to be considered by the courts include participation and costs of translators for the hearing. It is important that judges, professionals, including legal practitioners, and court staff are aware of possible differences between in-person testimony and remote testimony. For example, it is less easy to observe and interpret the demeanor of the witnesses.

20. This guideline requires attention to the process whereby the remote testimony is carried on. Particularly in case of evidence of fundamental importance for the resolution of a case, it is important to ensure that technology used makes it possible to ask questions in the course of giving testimony (if the rules of procedure so provide). This requirement is hardly met, when, transmission is distorted due to weak connectivity or if access to the technical means is limited for the parties. This may give unfair advantage to one of the parties. As far as it is technically possible, the remote evidence should be taken in a same way as it is taken inside the court.

21. The methods used should properly secure image or sound transmission against loss, distortion or unauthorized disclosure. The court may verify the identity of any person giving testimony by requiring him/her to present an appropriate document, such as a valid identity card, passport or driving license.

22. All available systems of communication, both public and private, should ensure at minimum the quality of the videoconference and encryption of the video signal in order to protect against interception. It is possible to receive evidence via a private connection, if the national law permits, provided the solutions used offer enough technical security and respect procedural safeguards. Private connection in this context means communication system that is not an official, governmental system specifically created for taking the evidence in court.

Use of electronic evidence

23. Courts should be aware of importance of electronic data submitted by the parties as evidence in its original format. If a printout of electronic evidence is filed, the court may order, at the request of a party or on its own initiative, provision of the original of the electronic evidence by the relevant person. An example of evidence that may have significant importance for resolving the point in issue, provided it is presented in original format, is geo location data. Most jurisdictions around the world have already expressly provided in their law for such use of electronic

evidence in legal proceedings. Example of such provisions can be found in the eIDAS Regulation.

Member States example

The Supreme Court of **Croatia** (case no. I Kž 696/04–7) confirmed that SMS messages may be used as evidence in the proceedings as they are equal source of information as any other written content stored on other medium.

Example of technology to be specifically used for securing the evidence (Blockchain)

Blockchain is an emerging technology which has potential to provide increased trust and security in electronic evidence. It can be defined as a distributed ledger that refers to the list of records (blocks), which are linked and secured using cryptography and are recorded in a decentralized peer-to-peer network. By design, a blockchain is inherently resistant to modification of the data. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority. This makes blockchain suitable for the evidencing purposes.

In USA, § 1913 of the Vermont Rules of Evidence reads: (1) A digital record electronically registered in a blockchain shall be self-authenticating pursuant to Vermont Rule of Evidence 902, if it is accompanied by a written declaration of a qualified person, made under oath, stating the qualification of the person to make the certification and: (a) the date and time the record entered the blockchain; (b) the date and time the record was received from the blockchain; (c) that the record was maintained in the blockchain as a regular conducted activity; and (d) that the record was made by the regularly conducted activity as a regular practice.

In China, the Hangzhou Internet Court confirmed on June 28, 2018 that the blockchain-based electronic data can be used as evidence in legal disputes. The usage of a third-party blockchain platform that is reliable without conflict of interests provided the legal ground for proving the intellectual infringement.

(http://www.xinhuanet.com/2018–06/28/c_1123051280.htm).

24. For the purposes of guideline 7, "advanced electronic signature" means an electronic signature which meets the requirements set out in Article 36 of the eIDAS regulation and "qualified electronic signature" means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.

25. In current practice most of the electronic data lack any advanced or qualified electronic signatures and are not secured in any other way. They should nevertheless still be considered by the courts as electronic evidence (while the probative value of the evidence may vary depending on the individual case) considering, for example, a variety of trust services related to electronic management of documents and identification of signatories that are available around the world. An example is biometric

signature, a method of obtaining an electronic version of a handwritten signature where a person writes his or her handwritten signature on an electronic device by using a special pen and pad. Depending on the applicable law, the court may recognize such a biometric signature as equivalent to a handwritten signature on paper.

26. Metadata provides the necessary context to evaluate the evidence (data) in the same way as a postage stamp provides context to evaluation of the ordinary (paper) letter and its content. Electronic evidence includes metadata as a matter of course and courts should be aware of its potential probative value. It can be used to trace and identify the source and destination of a communication, data on the device that generated electronic evidence, the date, time, duration and the type of evidence. The metadata may be relevant, either as indirect evidence (e.g. indicating the most relevant version of the document) or it may itself be relevant as direct evidence (e.g. in case the file data is manipulated). This guideline is also relevant in the case of lost metadata.

*Examples of case-law on metadata in **Ireland***

Metadata was considered important for authenticating the provenance of electronically created documents / materials (Koger Inc. & Koger (Dublin) Ltd v O'Donnell & Others [2010] IEHC 350).

http://www.courts.ie/Judgments.nsf/0/1F8979ED6FCCF69C-802577CB003B6360

The Irish courts have ruled that an obligation to discover electronically stored evidence includes discovery of the metadata of the native documents, where this would be relevant (Sretaw v. Craven House Capital PLC [2017] IEHC 580; Gallagher v RTE [2017] IEHC 237).

http://www.courts.ie/Judgments.nsf/0/D5847A097092C099802581C40045290E

27. Printouts of electronic evidence can be easily manipulated as they exclude metadata or other hidden data. It means that when the party submits a printout from the web browser screen such a printout can hardly be recognized as reliable electronic evidence or the basis for the expert's verification of authenticity. The printout is nothing but a copy of the screen display. It can be modified in a very simple manner because no special software or hardware requirements are required for this purpose.

Member States example

The Court of Appeal of **Lithuania** decided that instant copies of computer screen (screenshots) are not trustworthy (27 April 2018, Case No. e2A-226–516/2018).

http://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=fbf43bd0–2c01–41a5–9f69–3be0c2ef3acb

Collection, seizure and transmission

28. Electronic evidence, by its very nature, is fragile and can be altered, damagedor destroyed by improper handling or examination. For these reasons, special precautions may be taken to properly collect this type of evidence. Failure to do so may render it unusable or lead to an inaccurate conclusion. In principle, the parties are responsible for proper collection of electronic evidence in civil and administrative proceedings. Different types of data may require different methods of collection. Actions taken to secure and collect electronic evidence should not affect the integrity of that evidence. In matters of considerable importance, the parties should consider capturing the electronic evidence with the support of an IT specialist or the notary services. Judges, professionals, including legal practitioners should be aware that data are often stored with network-based services. This include both cloud computing and the online delivery of services.

29. There has been an increase in knowledge and expertise on the part of judges, professionals, including legal practitioners handling the evidence, but specific standards are still missing. Collection and seizure of electronic evidence may need adoption of special tools and procedures by member States. In the meantime, judges, professionals, including legal practitioners should seek to ensure the integrity, confidentiality and security of such data. This includes the retention of secured back-up copies should one of the means of storage fail. It is necessary to retain electronic data in their original format.

30. Although the use of data can be strictly domestic in nature, it is becoming more likely that they may have a cross-border nature, involving other countries. An example is the location in another country of the infrastructure used for the processing or storage of the data or the location of the provider that enables the storage or processing of the data. Direct cooperation between courts and trust or cloud services providers in cross-border cases is to be encouraged. When handling the electronic evidence, judges, professionals, including legal practitioners may take into consideration factors such as the place of establishment of the service provider, the place of processing the data, and the existence of local laws regulating access to the data.

Example of cross-border technology

Data sharing (clouds) is the storage of different parts of a database across various servers that might be located in different physical locations. It has become a common security technique. The global nature of the internet and the growing use of cloud services make it increasingly difficult to assume that access to data is strictly domestic in nature.

31. There are substantial differences between national procedural rules for the taking of evidence. Courts using evidence taken abroad should take those differences into consideration. It is recommended that in cross-border taking of electronic evidence, courts closely co-operate in this matter. A requesting court should be informed about the procedural rules used by the requested court in order to adapt their evaluation of the electronic evidence where appropriate. In particular, the taking of evidence abroad should not result in violation of the basic principles and rights of procedural law, such as equality of arms.

32. The efficiency of the proceedings is improved when it is possible for transmission of electronic evidence to other courts to be carried out in the original format rather than printing it and sending it out. Electronic data transmitted should be accompanied by its metadata. This includes use of additional metadata created by the courts for proper data management purposes and its smooth transmission to other courts. Having structured metadata gives the courts control over the evidence. A copy of electronic evidence should ideally be used for transmission to another court.

33. Encouragement and facilitation of the transmission of electronic evidence by electronic means can be achieved through implementation of common technical standards, files formats and digitisation of domestic judicial and administrative systems. Having regard to the higher risk of destruction of electronic evidence, local procedures should be adopted which permit secure transmission of electronic evidence.

34. Data integrity, survivability and security should be taken into consideration when it comes to transmitting evidence. Reliable services, such as trust services, may be essential, for ensuring proper transmission of electronic evidence. If the transmission requires confidentiality, it may be necessary to apply measures or technical solutions, such as encryption, which ensure access to a secure communication only to authorized persons.

Relevance

35. The amount of evidence which may be required to prove a certain fact may alter, depending on the complexity of the evidence. Unnecessary large amounts of electronic data could be easily provided by a party which would make it difficult or impossible for the court and the other participants to handle effectively. Therefore, active management of electronic evidence by the court with a view to restrict its provision to what is strictly required to decide the case is essential. The active management of data should respect the principle of proportionality. Every request to produce electronic evidence should be considered on its merits, in

particular its usefulness for probative purposes. The parties should be entitled to challenge such requests.

36. Judges, legal professionals, including legal practitioners should be aware of the possible need for technical expertise and recognize where further research or additional specialist knowledge, such as expert opinion, may be required. Experts must be competent and have sufficient training to undertake the assigned task.

Reliability

37. Separation of the digital identity from the physical may generate problems related to the reliability of the evidence. In the first place, courts should seek to establish the identity of the author of electronic data. If the applicable law does not specify the manner of establishing the identity, it may be determined in any objective way, such as electronic signature or by checking the e-mail address from which the document was sent.

38. Trust services may provide technological mechanisms that ensure the reliability of evidence. For example, certificates to electronic signatures, sometimes referred to as the "digital ID" of a person, may guarantee both authenticity and integrity of the data. Where the identity of the signatory with an electronic signature is doubtful, a court may request the service provider related to the electronic signature to make a statement in relation to the matters upon which it is competent to provide evidence. Timestamping (certification of time) may be equally important for evidencing the integrity of an electronic data.

Example of trust service

Timestamp is a mechanism that allows to prove the integrity of data. It demonstrates that data existed in a specific moment and have not been modified. The timestamp provides a value to the electronic evidence, as it includes relevant metadata about the moment of its creation.

39. As far as the applicable law allows for it, and subject to the court's discretion, the acceptance as evidence of all types of electronic evidence is encouraged and recommended for court practice. If there is a dispute, the parties generally identify the issues to be resolved, and unless a party raises the issue of the authenticity of the electronic evidence, the court does not need to raise the issue on its own initiative. Only where a party challenges the electronic evidence, the party seeking to rely on the evidence may be required to demonstrate its authenticity, for example by submitting metadata or seeking an appropriate order to obtain additional data from other persons, such as trust services providers.

40. The specific reference to court's discretion in guidelines 21 and 22 underlines the important role of court's discretion in respect of the subject matter of these guidelines.

41. As with any other evidence, a party to the proceedings may contest the evidence. In such case, the said party may request the court to exclude the evidence, for example due to the fact that the author of the data cannot be properly identified. The reliability of electronic data may be proved in any manner, for example, by qualified electronic signatures or other similar methods of identification and ensuring integrity of the data. It is, however, for applicable law, to define the legal effect of electronic signatures, for example by providing that only a qualified electronic signature should have the equivalent legal effect of a handwritten (wet ink) signature. For example, the applicable law may require the devices used to generate the signatures to be under the exclusive control of the signatory.

EU qualified electronic signature

Qualified electronic signatures ensuring integrity of data does not need specific analysis of technology used for their creation to be conducted by the court. It is enough to check the register of EU qualified trust services providers.

42. Guideline 23 concerns the burden of proof. More vulnerable persons such as consumers and children may not be technically and/or economically able to produce electronic evidence. Where they are benefited by statutory provisions that ease or reverse the burden of proof, those statutory provisions prevail over the guidelines. Courts should play an active role in cases where vulnerable persons are involved.

43. Depending on the national legal system, the evidential value of public (official) electronic systems that generate electronic evidence is to be respected. For example, data from electronic public registers can be treated as an official document, which results in presumption of its truthfulness. An electronic recording of other proceedings may be treated as reliable representation of the facts and free from the risk of human error (e.g. comparing it to the content being dictated to the protocol by the judge).

Member States examples of the public trust systems

There are specific types of trust services made available at national level such as "Trusted Profile" (**Poland**), "Electronic archiving and digitalization" (**Belgium**), "Information/documents long term preservation, LEXNET Platform for exchanging information between the Judicial Bodies and a wide range of legal operators" (**Spain**).

Storage and preservation

44. Storage within the meaning of these guidelines relates to the duration of the civil or administrative proceedings. Electronic evidence may be stored in the courts during the period of the proceedings, for example, on portable devices (memory cards), servers, back-up systems and other places of data storage (including cloud computing). The courts should store electronic evidence in its original format (e.g. not as printouts), in accordance with applicable laws. Cybersecurity issues should be also taken into consideration which means that courts should adopt proactive approaches to protecting the integrity of electronic evidence from cyberthreats, including damage or unauthorized access. By focusing on prevention, courts can prevent cyberthreats from affecting the integrity of electronic evidence and reduce overall cybersecurity risks. Regardless of the method used for storage, unauthorized individuals should not be given access to the electronic evidence.

45. Stored electronic evidence can be associated with standardised metadata describing the context of their creation as well as the existing links with other electronic records. The implementation of international standards for metadata ensures a level of consistency in storage of the electronic evidence. Because creation of standardised metadata can be difficult and time consuming, courts may use tools that can help generate the standardised metadata.

Example of solution used to standardised metadata

A number of tools are available for standardised metadata creation. For example, the metadata management tool may generate an XML (eXtensible Markup Language) file containing the metadata related to the electronic evidence. XML files require no advanced software to be professionals. It is both a standardised format and sufficiently flexible to be applied across different information systems. This may simplify both storage and retrieval of the electronic evidence.

In this regard international standards applied to metadata should be followed, such as those published by international standards communities, like ISO (International Organization for Standardization).

46. Guideline 27 concerning the preservation of electronic evidence is applicable both to the storage and the archiving of electronic evidence that takes place after completion of the proceedings. The electronic evidence should be stored and archived in the original form in which it has been created, transmitted, received and which does not materially change the data. The electronic evidence should be available in a readable format during the whole time of the proceedings. The integrity of electronic evidence should be maintained at all stages.

Archiving

47. The guidelines on archiving cover the period after the proceedings and has regard to Recommendation Rec(2003)15 of the Committee of Ministers of the Council of Europe to member States on archiving of electronic documents in the legal sector. National law typically provides retention periods and technical archiving conditions. The systems employed for archiving need to be secure and guarantee traceable use and respect for privacy. Appropriate technical and organisational measures should be implemented in order to ensure the protection of electronic evidence, and to guard against unauthorised access to it. An electronic data carrier, if used, should be provided with an identification certificate containing basic data about it. Such a carrier should be properly protected, especially against loss, harmful effects of chemicals, heat, light, radiation, magnetic or electric fields and against mechanical damage.

48. Archiving services may verify, possibly using electronic signatures or other electronic procedures, that electronic evidence is being archived by qualified specialists or competent organisations and that data have not been altered by them. Both data on electronic signatures with which the electronic documents have been signed, as well as data for verification of those signatures need to be properly archived. Member States should provide the organisations in the legal sector entrusted by law with the duty of archiving, with the necessary resources for the archiving of electronic evidence.

49. Migration means change of the storage medium in order to preserve accessibility to electronic evidence. Neglect of migration may result in unreadability of the data. Electronic documents may be archived by periodic transfer of data from one storage medium to another or from one format to another. Migration should also apply to metadata concerning the archived electronic documents. Migration to new storage medium should take place regularly, taking account for example degradation and wear in the medium in question and before they become obsolete because of the technological development of media and hardware. Migration to new storage medium or format should be carried out, when appropriate, in view of the technological development.

Example of a long-term solution

Data can be migrated to networked devices, such as cloud computing. They are being constantly improved due to technological development of media and hardware. Cloud archiving may provide also greater control over cost by paying for only the space needed.

Example of an outdated solution

CD or DVD or other optical discs become unreadable due to physical or chemical deterioration. The causes of this effect vary from oxidation of the reflective layer, to physical scuffing and abrasion of disc surfaces or edges, including visible scratches, to other kinds of reactions with contaminants.

Awareness-raising, review, training and education

50. Promotion includes wide dissemination of these guidelines to the courts and legal practitioners, its translation into the local languages, organisation of seminars and conferences on electronic evidence.

51. Review of the technical standards related to electronic evidence may include, for example, new means of its storage, preservation and archiving.

52. Access to interdisciplinary training on handling electronic evidence is necessary for judges, professionals, including legal practitioners. Training may cover specific challenges raised by electronic evidence, such as importance of metadata, importance of timestamping and use of cloud computing or blockchain in collection and seizure, need for submission of electronic evidence in the original format, rather than simply scanned images or printouts.

53. Awareness of the wider digital context and use of technologies, such as cloud computing, trust services or blockchain, is important for judges, professionals, including legal practitioners.

54. Knowledge on material and procedural matters in the context of electronic evidence should be an essential part of legal education.

Selected bibliography and other sources

1) Recommendation Rec(2003)15 of the Committee of Ministers of the Council of Europe to member States on archiving of electronic documents in the legal sector;

2) Biasiotti M., Mifsud Bonnici J., Cannataci J., Turchi F. (eds.), *Handling and Exchanging Electronic Evidence across Europe*, Springer 2018;

3) Forgó N., Hawellek C., Knoke F., Stoklas J., *The Collection of Electronic Evidence in Germany — a Spotlight on Recent Legal Developments and Court Rulings*, in: *New Technology, Big Data and the Law* (ed. Forgó, Fenwick, Corrales), Springer 2017;

4) Morabito V., *Business Innovation Through Blockchain. The B³ Perspective*, Springer International Publishing AG Cham 2017;

5) Hofmann E., Strewe U., Bosia N., *Supply Chain Finance and Blockchain Technology. The Case of Reverse Securitisation*, Springer Munich 2018;

6) Singer P., Friedman A., *Cybersecurity and cyberwar: What everyone needs to know*, Oxford, Oxford University Press 2014;

7) Mason S., *The use of electronic evidence in civil and administrative law proceedings and its effect on the rules of evidence and modes of proof. A comparative study and analysis*. Report prepared by Stephen Mason assisted by Uwe Rasmussen. Strasbourg, 27 July 2016, CDCJ(2015)14-final;

8) Albert J., *Study on possible national legal obstacles to full recognition of electronic processing of performance information on construction products (under the construction products regulation), notably within the regimes of civil liability and evidentiary value*, Final General Report, 30-CE-0517177/00–3630-CE-0517177/00–36;

9) W. Schünemann, M. Baumann Editors (ed.), *Privacy, Data Protection and Cybersecurity in Europe*, Springer International 2017;

10) Voigt P., von dem Bussche A., *The EU General Data Protection Regulation (GDPR). A Practical Guide*, Springer International 2017;

11) Mason S., Seng D. (ed.), *Electronic Evidence*, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017;

12) Mason S. (ed.), *International Electronic Evidence*, British Institute of International and Comparative Law, 2008;

13) Mason S., *Electronic Signatures in Law Institute of Advanced Legal Studies for the SAS Humanities Digital Library*, School of Advanced Study, University of London 2016;

14) Mason S., *Electronic Disclosure A Casebook for Civil and Criminal Practitioners*, PP Publishing 2015;

15) Electronic Evidence: Model Policy Guidelines & Legislative Texts, Establishment of Harmonized Policies for the ICT Market in the ACP countries, HIPCAR project "Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures 2013, https://www.itu.int;

16) Capriolli E., *Droit international de l'économie numérique*, Paris, Litec, 2007;

17) Biasiotti M. A., Turchi F., Epifani M., *The EVIDENCE Project: bridging the Gap in the Exchange of Digital Evidence Accross Europe*, SADFE 2015, http://sadfe2015.safesocietylabs.com/wp-content/uploads/2015/10/SADFE-2015-Proceedings.pdf (October 2015).

COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES

1949.2019

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

ЗАСТУПНИКИ МІНІСТРІВ	Документи Комітету міністрів	CM(2021)36add4-final	16 червня 2021 року

1407-ме засідання, 16 червня 2021 року

10. Правові питання

10.1. Європейський комітет з правового співробітництва (CDCJ)

Керівні принципи Комітету міністрів Ради Європи щодо механізмів онлайн вирішення спорів у цивільному та адміністративному судочинстві

Преамбула

Комітет міністрів,

беручи до уваги, що метою Ради Європи є досягнення більшої єдності між державами-членами, зокрема шляхом сприяння ухваленню спільних правил із правових питань;

ураховуючи необхідність надання практичних керівних принципів для осіб, які відповідають за розроблення механізмів онлайн вирішення спорів (далі — ОВС) у державах-членах, задля забезпечення відповідності цих механізмів статтям 6 та 13 Конвенції про захист прав людини і основоположних свобод (ETS № 5, «Європейська конвенція з прав людини»);

беручи до уваги, що ці керівні принципи мають бути скеровані на встановлення спільної основи, а не на гармонізацію національного законодавства держав-членів;

ураховуючи необхідність поважати різноманітність правових систем держав-членів;

визнаючи прогрес, якого досягли держави-члени у впровадженні механізмів онлайн вирішення спорів у свої правові системи;

зазначаючи, що розробники механізмів онлайн вирішення спорів (як державні, так і приватні) можуть бути недостатньо обізнані про те, що такі механізми повинні супроводжуватися надійними гарантіями дотримання прав людини;

підкреслюючи необхідність для держав-членів забезпечити сумісність таких механізмів із ключовими принципами справедливого судового розгляду та ефективного засобу правового захисту, що встановлені практикою Європейського суду з прав людини, зокрема принципами усного слухання й рівності сторін;

ухвалює ці керівні принципи як практичний інструмент для держав-членів, щоб допомогти їм адаптувати роботу своїх механізмів онлайн вирішення спорів до положень статей 6 і 13 Європейської конвенції з прав людини і принципів, розроблених на їх основі в практиці Європейського суду з прав людини, і пропонує державам-членам широко розповсюдити ці керівні принципи задля їх застосування особами, відповідальними за розроблення і впровадження механізмів онлайн вирішення спорів.

Мета та сфера застосування

Керівні принципи застосовуються до механізмів онлайн вирішення спорів (ОВС), які використовують суди. Вони містять рекомендації щодо справедливої процедури, прозорості використання ОВС та вимог до судового розгляду, особливих питань, що пов'язані з ІКТ природою механізмів ОВС, та інших питань, які не випливають із практики Європейського суду з прав людини. Керівні принципи не стосуються внутрішнього судового управління електронними матеріалами справ або альтернативних способів вирішення спорів (АВС), як-от медіація та примирення. Однак держави-члени можуть за потреби поширити їх застосування на АВС.

Визначення

Для цілей цих керівних принципів наведені нижче терміни мають такі значення:

і. Суд

«Суд» — це орган, який відповідає поняттю «суд» за змістом статті 6 Європейської конвенції з прав людини, тобто орган, який:

- установлений законом;
- керується процедурою, визначеною законом;
- вирішує питання, що належать до його компетенції шляхом ухвалення обов'язкових рішень;
- має повну юрисдикцію щодо справи;
- є незалежним і безстороннім.

ii. Онлайн вирішення спорів (ОВС)

«Онлайн вирішення спорів (ОВС)» — це будь-яка інформаційна технологія (ІТ) онлайн, яку використовує суд для вирішення спору або допомоги у його вирішенні.

iii. Штучний інтелект (ШІ)

«Штучний інтелект (ШІ)» — це сукупність наукових методів, теорій і технік, метою яких є відтворення машиною когнітивних здібностей людини.

iv. Інформаційно-комунікаційні технології (ІКТ)

«Інформаційно-комунікаційні технології (ІКТ)» — це технології, що забезпечують доступ до інформації за допомогою телекомунікацій.

Основні принципи

1. Держави-члени повинні прагнути до забезпечення довіри й упевненості в ОВС.
2. ОВС не має створювати істотних перешкод для доступу до правосуддя.
3. Процесуальні правила, застосовні до судового провадження загалом, мають також застосовуватися до судових проваджень із використанням ОВС, якщо специфіка конкретного механізму ОВС не вимагає іншого.
4. Сторони проваджень, у яких використовують ОВС, мають бути ідентифіковані за допомогою безпечних механізмів.

Керівні принципи

Справедлива процедура

Доступ до правосуддя

1. Механізм ОВС має бути зрозумілим, доступним і зручним, щоб якомога більше людей могли його легко використовувати.
2. Сторони мають бути поінформовані про те, як працює ОВС, як подати заяву, як стежити за ходом провадження і як отримати доступ до судових рішень.
3. Застосування ОВС не має бути невигідним для сторін провадження або надавати несправедливу перевагу одній зі сторін.
4. Механізм ОВС має бути розроблено та впроваджено відповідно до міжнародно визнаних технічних стандартів, щоб якомога більше людей могли самостійно його використовувати.

5. Вартість судового розгляду із застосуванням ОВС не має перевищувати вартості розгляду без його застосування.

6. Необхідно повідомляти сторони провадження про те, що їхню справу розглядатимуть із застосуванням механізму ШІ.

Рівність сторін

7. Участь у процедурах ОВС не має завдати шкоди праву особи на ефективну участь у провадженні або її праву на ефективний засіб правового захисту.

8. Процедура ОВС має забезпечувати незалежний і безсторонній судовий процес.

9. Сторони провадження, у якому застосовують ОВС, мають ознайомитися з матеріалами справи, зокрема матеріалами, що їх надали інші сторони; вони повинні мати доступ до цих матеріалів та достатньо часу й засобів для ознайомлення з їх змістом.

Докази

10. Справедливість вимагає, щоб сторонам у провадженні, у якому застосовують ОВС, було дозволено надавати докази у спосіб, який не ставить їх у невигідне становище порівняно з іншими сторонами.

11. Сторони повинні мати можливість викласти свою позицію й оскаржити докази, надані іншими сторонами.

12. ОВС має дотримуватись принципів юридичної визначеності та захисту легітимних очікувань сторін.

Ефективне провадження

13. Впровадження механізмів ОВС має бути скероване на підвищення ефективності провадження шляхом надання сторонам можливості брати участь у процесі без фізичної присутності в суді, а також настільки, наскільки це можливо, шляхом оптимізації всього процесу.

14. Технічні труднощі в роботі ОВС не мають заважати судам розглядати справи й виконувати відповідні процесуальні дії.

15. Якщо національне законодавство передбачає, що АВС є необхідною умовою для початку судового розгляду, зокрема із застосуванням ОВС, це не повинно невиправдано затягувати процес вирішення спору або істотно збільшувати витрати для сторін.

Ухвалення рішення

16. Результати провадження із застосуванням механізмів ОВС мають бути прозорими.

17. Будь-яке остаточне рішення, ухвалене із застосуванням механізмів ОВС, має бути оприлюднене відповідно до практики Європейського суду з прав людини.

Право на обґрунтоване рішення

18. Рішення, ухвалені із застосуванням механізму ОВС або за сприяння механізму ОВС, зокрема рішення, ухвалені із застосуванням механізмів ШІ, повинні мати достатнє обґрунтування.

Виконання рішення

19. Той факт, що рішення є результатом застосування механізму ОВС, не має перешкоджати його виконанню.

Право на судовий перегляд у справах, пов'язаних із суто автоматизованими рішеннями

20. Якщо національне законодавство допускає ухвалення суто автоматизованих рішень, повинна існувати можливість перегляду таких рішень суддею.

Прозорість використання механізмів ОВС та вимоги до судових засідань

Прозорість у розробленні та функціонуванні механізмів ОВС

21. Проєктування й функціонування механізмів ОВС мають бути прозорими та зрозумілими, із чіткими визначеннями та викладені доступною мовою.

Публічні та усні судові засідання

22. Застосування механізмів ОВС має гарантувати належні шляхи забезпечення громадського контролю за провадженням.

23. Застосування механізмів ОВС у судах не повинно позбавляти сторони права вимагати проведення усного судового засідання хоча б в одній судовій інстанції.

Інші питання прозорості, зокрема громадський контроль

24. Сторони провадження, у якому застосовують механізм ОВС, мають бути поінформовані про будь-які потенційні конфлікти інтересів, пов'язані з роботою механізму ОВС.

25. ОВС має бути організовано так, щоб усі створювані документи, зокрема остаточне судове рішення та інші рішення або повідомлення, були складені чіткою і зрозумілою мовою.

26. Процедурні правила, застосовні до ОВС, мають бути прозорими.

27. Сторони провадження, у якому застосовують механізми ОВС, повинні бути поінформовані про процедурні правила, застосовні до ОВС, і повинні мати доступ до інформації про них.

Спеціальні питання, пов'язані з ІКТ-характером методів ОВС

Кібербезпека

28. Необхідно забезпечити належний рівень кібербезпеки продуктів, послуг і процесів ІКТ, що сприяють ОВС, щоб задовольнити вимоги статей 6 і 13 Європейської конвенції з прав людини й забезпечити необхідну довіру до механізмів ОВС.

29. Рівень кібербезпеки продуктів, послуг і процесів ІКТ, що сприяють ОВС, необхідно вважати належним, якщо забезпечено захисні гарантії щодо:

    – несанкціонованого доступу до конфіденційних даних;

    – небажаної зміни або видалення даних;

    – технічної неможливості доступу до системи й даних, які вона містить, для осіб, які повинні мати доступ;

    – невизначеності щодо особи судді й інших фахівців, які беруть участь у процедурі ОВС;

    – шахрайства сторін з ідентичністю.

Захист прав людини, зокрема захист персональних даних

30. Державам-членам варто оцінити вплив застосування ОВС упродовж його функціонального циклу на окремих осіб і соціальні групи та визначити конкретні вимоги щодо етичного й справедливого застосування ОВС, дотримання прав людини як частини проєктування й роботи будь-якого механізму ОВС.

31. Використання механізмів ОВС не має порушувати права на захист даних, зокрема там, де це застосовно, права на інформацію, права на доступ до даних, права на заперечення щодо оброблення даних і права на видалення даних.

32. Необхідно вживати технічних та організаційних заходів для забезпечення дотримання правил щодо захисту персональних даних як під час визначення засобів оброблення, так і під час оброблення даних.

33. Механізми ОВС мають бути спроєктовані та розроблені із застосуванням принципів захисту персональних даних за замовчуванням і за проєктуванням, зокрема, через:

– впровадження технічних і організаційних заходів для забезпечення захисту персональних даних шляхом застосування, зокрема, методів анонімізації або псевдонімізації;

– запровадження обмеження на доступ і повторне використання з боку компетентних органів, які контролюють дані.

34. Аутсорсинг-технології, що використовують у механізмах ОВС, не мають призводити до оброблення персональних даних з комерційною метою.

Інші питання (що не випливають із практики Європейського суду з прав людини)

Тестування, моніторинг, модернізація, дослідження та розвиток

35. Державам-членам рекомендовано виділяти відповідне державне фінансування на розроблення механізмів ОВС, які застосовуватимуться в судових провадженнях, зокрема, на проведення відповідних досліджень.

36. Простота застосування механізмів ОВС має бути перевірена перед їхнім впровадженням.

37. Судові органи, правники та інші зацікавлені сторони повинні брати активну участь у розробленні механізмів ОВС.

38. Під час експлуатації всіх таких систем необхідно проводити постійний моніторинг і своєчасну модернізацію механізмів ОВС для забезпечення безпеки, справедливості, ефективності й інших стандартів якості.

Підвищення обізнаності, навчання та освіта

39. Держави-члени мають заохочувати фізичних і юридичних осіб до використання механізмів ОВС, зокрема інформуючи їх про існування такої можливості, про її надійність і сумісність із вимогами Європейської конвенції з прав людини.

40. Судді та юристи, а також усі учасники судового процесу мають бути обізнані з перевагами, цінностями механізмів ОВС, їх відповідністю Європейській конвенції з прав людини та іншим відповідним законам.

41. Судді та юристи, а також працівники судів повинні мати доступ до відповідного навчання з питань ОВС, яке проводять фахівці в галузі права та інформаційних технологій. Навчання має бути максимально практичним і адаптованим до потреб конкретних цільових груп.

42. Оскільки механізми ОВС не повинні обмежувати процесуальних прав сторін, судді повинні вміти визначати ризики, що можуть виникнути в результаті застосування ІКТ, й усувати їх.

43. Юридична освіта має охоплювати модулі, присвячені питанням застосування засобів ІКТ у судах.

COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES

1949.2019

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

ЗАСТУПНИКИ МІНІСТРІВ	Документи Комітету міністрів	**CM(2021)36-add5-final**	16 червня 2021 року

1407-ме засідання, 16 червня 2021 року

10. Правові питання

10.1. Європейський комітет з правового співробітництва (CDCJ)

Керівні принципи Комітету міністрів Ради Європи щодо механізмів онлайн вирішення спорів у цивільному та адміністративному судочинстві — Пояснювальна записка

ЗМІСТ

ЗАГАЛЬНІ КОМЕНТАРІ

Чому новий інструмент?

1. Методи й механізми онлайн вирішення спорів (ОВС) набувають дедалі більшого значення у вирішенні спорів у державах — членах Ради Європи. ОВС може покращити доступ до правосуддя через сприяння більш швидкому й менш витратному доступу до судів, що робить урегулювання спорів більш ефективним і результативним.

2. Проте широке використання ОВС також може обмежити доступ до правосуддя, створюючи технологічні бар'єри для всіх тих, хто не має можливості використовувати IT-технології. Крім того, необхідно приділяти увагу питанням аутентифікації й ідентифікації сторін, цифрового бар'єру, кібербезпеки й захисту персональних даних.

3. Для забезпечення справедливого вирішення спорів варто розробити відповідні й належні керівні принципи щодо захисту прав людини під час використання ОВС. У державах —членах Ради Європи ця вимога також випливає з гарантій, закріплених у Конвенції про захист прав людини і основоположних свобод (ETS № 5 «Європейська конвенція з прав людини»), особливо із гарантій справедливого судового розгляду, що містяться в статтях 6 і 13. Нині на міжнародному, європейському та національному рівнях таких стандартів дуже мало. Мета цих керівних принципів — рекомендувати стандарти для формування законодавства і практики та заповнити наявні прогалини.

4. Ці керівні принципи містять добірку мінімально необхідних заходів, яких повинні дотримуватися уряди держав-членів, законодавці, суди, а також розробники, виробники й постачальники послуг ОВС для забезпечення того, щоб ОВС не порушувало людської гідності, прав та основоположних свобод людини.

5. Мета цих керівних принципів полягає не в тому, щоб установити обов'язкові правові стандарти, а в тому, щоб слугувати практичним інструментом для держав-членів та гарантувати, що їх методи та механізми ОВС відповідають вимогам статей 6 і 13 Європейської конвенції з прав людини та принципам, установленим прецедентною практикою Європейського суду з прав людини.

Метод роботи і процес проєктування

6. Питання ОВС належить до компетенції Європейського комітету з правового співробітництва (CDCJ), який є міжурядовим органом Ради Європи, що відповідає за розроблення стандартів у галузі цивільного та адміністративного права.

7. У 2016 році було проведено дослідження про доцільність діяльності CDCJ щодо запровадження механізмів ОВС у контексті статей 6 і 13 Європейської конвенції з прав людини.

8. Наступним кроком було рішення CDCJ почати у 2017 році роботу з підготовки технічного дослідження як першого етапу цієї діяльності. Це технічне дослідження було завершено і надано CDCJ на його 93-му пленарному засіданні (14–16 листопада 2018 року).

9. Діяльність було продовжено і її результатом стала підготовка цих керівних принципів, що мають за мету забезпечення сумісності механізмів ОВС зі статтями 6 і 13 Європейської конвенції з прав людини. Керівні принципи, підготовлені на засіданнях 2019 і 2020 років, ґрунтуються на пропозиціях членів CDCJ. Група розробників урахувала досвід функціонування механізмів ОВС у державах-членах.

Національні приклади:

- У **Литві** існує можливість онлайн подання документів, онлайн оплати судових витрат і онлайн доступу до цифрових матеріалів усіх цивільних і адміністративних справ із використанням централізованої системи електронного правосуддя LITEKO; суди зазвичай видають цифрові офіційні документи (постанови, рішення, вироки, ухвали, повідомлення, повістки тощо), які завірені кваліфікованими електронними підписами та мають таку саму юридичну силу, що й аналогічні паперові документи; у 2019 році близько 74 % матеріалів судових справ із цивільних та адміністративних питань були цифровими, інші матеріали були змішаними (цифровими й паперовими); аукціони з продажу майна у виконавчому провадженні проводять тільки в електронній формі; відеоконференції можна використовувати в цивільних та адміністративних процесах, оскільки майже кожен суд оснащений принаймні одним комплектом устаткування для відеоконференцій або має змогу використовувати мобільне обладнання для відеоконференцій, а кожна судова зала оснащена обладнанням для цифрового аудіозапису. У відповідь на спалах гострої респіраторної хвороби COVID-19 усі судді литовських судів мали можливість працювати вдома з віддаленим доступом до системи правосуддя LITEKO. Було вжито заходів для більш активного використання відео- і телеконференцій із застосуванням розповсюджених приватних інструментів (як-от відеоконференції) для перетворення усних слухань на віртуальні цифрові засідання. Було також ужито додаткових заходів кібербезпеки задля забезпечення безпеки і стабільності системи електронного правосуддя.
- У **Франції** існує можливість ініціювати адміністративні та господарські провадження в режимі онлайн на спеціальних порталах і подавати судові документи в електронній формі. У цивільному судочинстві можна використовувати відеоконференції.
- У **Греції** адвокати можуть подавати всі процесуальні акти (позови, апеляційні скарги, клопотання тощо) і супровідні документи (письмові

заяви з файлами, доданими як докази) в електронній формі з використанням кваліфікованого електронного підпису. Під час основного провадження також дозволено використовувати відеоконференції.

- В **Ірландії** існує судова онлайн-платформа для розгляду певних малозначних справ. Крім того, доступні такі послуги: онлайн-система електронного ліцензування (eLicensing) для опрацювання заяв про видачу ліцензій, зокрема ліцензій на алкоголь, ігрові та лотерейні додатки тощо, система експертизи судових витрат (Legal Costs Adjudication), що дає змогу подавати позови онлайн, система судових штрафів онлайн (Court Fines Online), яка дає можливість оплачувати штрафи, накладені окружним судом, в електронній формі, а також система Верховного суду в режимі онлайн (Supreme Court online), яка дає змогу подавати заяви про дозвіл на апеляцію до Верховного суду онлайн. Також було запроваджено додаткові заходи, що забезпечують можливість проведення дистанційного судового засідання в цивільному судочинстві, електронного подання документів до суду до початку розгляду (eFiling), дистанційного подання «заяв про достовірність» відомостей як альтернативи показанням під присягою, а також для органів, які проводять слухання чи розгляд апеляційних скарг, щоб здійснювати це дистанційно.
- У **Польщі** процедура оформлення платіжних доручень є повністю електронною. Вимогу подають через індивідуальний обліковий запис, створений на спеціальній ІТ-платформі. Усі акти й документи доступні в режимі онлайн.
- У **Португалії** процедура виселення, що передбачає примусове розірвання договорів оренди, може бути ініційована через онлайн-платформу (Balcão Nacional de Arrendamento). Citius — це електронна платформа, яку використовують суди. Представники у справах можуть використовувати її для подання процесуальних документів і повідомлень. В адміністративних і податкових юрисдикціях за допомогою онлайн-системи SITAF представники у справах можуть подавати процесуальні документи, отримувати повідомлення і вести свої справи в електронній формі. Обидві системи (Citius і SITAF) також підтримують діяльність мирових суддів і прокурорів. Сторони провадження мають онлайн-доступ до документів, що стосуються їхніх справ. Довідки, що стосуються судових проваджень, також можна отримати в електронній формі. Усі національні суди мають щонайменше одну залу для проведення відеоконференцій, а всі судові зали оснащені системами аудіозапису.
- У **Бельгії** введено Центральний реєстр платоспроможності (RegSol) — цифрова платформа, що дає змогу кредиторам, уповноваженим агентам і зацікавленим сторонам ініціювати справи щодо неплатоспроможності, отримувати до них доступ або спостерігати за ходом справ, що перебувають у провадженні господарського суду.

- У **Сполученому Королівстві** введено: 1) онлайн-платформу MONEYCLAIMS і 2) платформу ОВС для вирішення справ, ініційованих пасажирами авіакомпаній.
- В **Угорщині** штучний інтелект використовують в онлайн-базі даних анонімізованих судових рішень (записи з можливістю пошуку).
- У **Туреччині** впроваджено Національну судову інформаційну систему, яка має назву UYAP, що дає судам і фізичним особам змогу здійснювати процесуальні дії в режимі онлайн.

10. Ці керівні принципи повною мірою враховують керівні принципи Комітету міністрів 2019 року щодо електронних доказів у цивільному та адміністративному провадженні (далі — керівні принципи щодо електронних доказів).

Структура і зміст

11. Ці керівні принципи значною мірою повторюють структуру принципів, розроблених у практиці Європейського суду з прав людини (далі — ЄСПЛ) за статтею 6 Європейської конвенції з прав людини (далі — Конвенція) й зібраних у «Посібнику зі статті 6 Європейської конвенції з прав людини — Право на справедливий суд (цивільна частина)».

12. Хоча в керівних принципах часто використовують більш нейтральне слово «варто», його не можна сприймати як таке, що зменшує юридичну силу Конвенції, коли йдеться про принципи з Конвенції та з практики ЄСПЛ.

ПРЕАМБУЛА

13. Ці керівні принципи поширюються на механізм ОВС (як обов'язковий або добровільний інструмент), який використовують у судових провадженнях щодо цивільних, зокрема господарських, та адміністративних справ (визначення терміна «суд» див. у пункті 18 нижче). Оскільки різноманітність правових систем держав-членів є визнаною, керівні принципи містять доволі загальні положення, що стосуються цих правових систем. Зокрема, керівні принципи не містять жодних рекомендацій для держав-членів щодо того, чи варто їм впроваджувати методи та механізми ОВС у свої судові системи. З іншого боку, керівні принципи є не лише декларацією принципів, вони покликані надати практичні поради й рекомендації.

МЕТА ТА СФЕРА ЗАСТОСУВАННЯ

14. У цих керівних принципах розглянуто, зокрема, ключові принципи справедливого судового розгляду й ефективного засобу правового захисту в тлумаченні ЄСПЛ, наприклад, принцип рівності сторін.

15. Мета керівних принципів — допомогти державам-членам забезпечити відповідність методів і механізмів ОВС статтям 6 і 13 Конвенції без шкоди для переваг, які може надати ОВС, зокрема щодо витрат на вирішення спорів. У цьому контексті варто повторити, що положення Конвенції необхідно тлумачити у світлі сучасних умов, з огляду на панівні економічні та соціальні умови [«Маркс проти Бельгії» (*Marckx v. Belgium*), 13 червня 1979 року, п. 41, Серія А № 31; «Тайрер проти Сполученого Королівства» (*Tyrer v. the United Kingdom*), 25 квітня 1978 року, п. 31, Серія А № 26].

Ключові положення Європейської конвенції з прав людини

Пункт 1 статті 6 Конвенції передбачає: «Кожен має право на справедливий і публічний розгляд його справи упродовж розумного строку незалежним і безстороннім судом, встановленим законом, який вирішить спір щодо його прав та обов'язків цивільного характеру <...>. Судове рішення проголошується публічно, але преса і публіка можуть бути не допущені в зал засідань протягом усього судового розгляду або його частини в інтересах моралі, громадського порядку чи національної безпеки в демократичному суспільстві, якщо того вимагають інтереси неповнолітніх або захист приватного життя сторін, або — тією мірою, що визнана судом суворо необхідною, — коли за особливих обставин публічність розгляду може зашкодити інтересам правосуддя».

У практиці Суду за статтею 13 Конвенції ідеться: «Кожен, чиї права та свободи, визнані в цій Конвенції, було порушено, має право на ефективний засіб правового захисту в національному органі, навіть якщо таке порушення було вчинене особами, які здійснювали свої офіційні повноваження».

Керівні принципи стосуються:

- справедливої процедури;
- прозорості використання ОВС та вимог до судових засідань;
- спеціальних питань, пов'язаних з ІКТ-характером методів ОВС;
- інших питань (що не випливають із практики ЄСПЛ).

16. Із використанням терміна «онлайн вирішення спорів» пов'язана дуже велика плутанина. Під ним часто розуміють електронний варіант альтернативного вирішення спорів (АВС), що зазвичай відбувається в позасудовому порядку. Прикладом може слугувати Платформа Європейського Союзу з онлайн вирішення спорів. Однак ці керівні принципи стосуються використання нових технологій під час судових засідань. Причиною цього є мета цих керівних принципів: вони присвячені питанню про те, як можна забезпечити гарантії щодо судових процедур, які містяться в статтях 6 і 13 Європейської конвенції з прав людини, під час використання електронних механізмів вирішення спорів. Тобто яким юридичним і технічним умовам ці

механізми мають відповідати, щоб задовольняти вимоги, які випливають зі статей 6 і 13 Європейської конвенції з прав людини. Дія статей 6 і 13 не поширюється на позасудове врегулювання спорів, тобто на механізми альтернативного вирішення спорів (АВС), тому їх навмисно виключено зі сфери застосування цих керівних принципів. Проте держави-члени можуть поширити застосування цих керівних принципів на АВС, як-от арбітраж або медіацію, якщо це доречно. Водночас державам-членам варто враховувати, що керівні принципи було розроблено для процедур, які здійснює суд. Це означає, що не всі керівні принципи можна застосувати безпосередньо і, можливо, буде потрібне додаткове коригування з боку держав-членів для використання *mutatis mutandis* у межах конкретних механізмів АВС.

17. Керівні принципи не застосовують до внутрішнього судового управління електронними матеріалами справ. Наприклад, до алгоритму розподілу справ між суддями.

ВИЗНАЧЕННЯ

Суд

18. Широке визначення поняття «суд» використовується для того, щоб охопити всі органи, які мають повноваження з розгляду правових спорів із використанням ОВС у цивільному та адміністративному провадженні. Керівні принципи містять пряме посилання на поняття «суд» у значенні статті 6 Європейської конвенції з прав людини для того, щоб узгодити сферу застосування цих керівних принципів зі сферою застосування статті 6. У своїх рішеннях Європейський суд з прав людини встановив критерії, за якими суд може бути визнаний судом за змістом статті 6 Європейської конвенції з прав людини, і ці критерії повністю відображені в керівних принципах. Керівні принципи охоплюють провадження в органах, наділених функціями ухвалення рішень, і тільки ті провадження, що мають судовий характер. Це розмежування є важливим, оскільки інші види діяльності таких органів можуть мати несудовий характер. Ці керівні принципи не поширюються на незмагальні й односторонні процедури, у яких не беруть участі протиборчі сторони і які застосовуються за відсутності спору про права [«Алавердян проти Вірменії» (*Alaverdyan v. Armenia*), заява № 4523/04, рішення про прийнятність від 24 серпня 2010 року, п. 35; «Кіпр проти Туреччини» (*Cyprus v. Turkey*) (ВП), № 25781/94, ЄСПЛ 2001-IV].

Онлайн вирішення спорів (ОВС)

19. Поняття «онлайн вирішення спорів» уперше виникло наприкінці 1990-х років і розвивалось протягом двох десятиліть разом

із розвитком інтернету, зокрема, онлайн-покупок тощо. Спочатку це поняття асоціювалося лише з механізмами альтернативного вирішення спорів (АВС) із використанням електронних комунікацій, що особливо зручно тоді, коли сторони перебувають далеко одна від одної. Поняття «онлайн вирішення спорів» широко використовувалося й використовується нині як синонім електронного альтернативного вирішення спорів (е-АВС). Наприклад, у Регламенті № 524/2013 Європейського Парламенту та Ради від 21 травня 2013 року сферу його застосування обмежено «позасудовим вирішенням спорів щодо договірних зобов'язань, які випливають із договорів про онлайн-продаж або надання послуг між споживачами, які проживають на території ЄС, і продавцями, які працюють на території ЄС». Однак із плином часу значення терміна «онлайн вирішення спорів» було розширене і наразі охоплює також методи та механізми, що доповнюють, прискорюють і полегшують багато функцій традиційних судів.

20. Іноді буває складно відрізнити поняття «онлайн вирішення спорів» від суміжних, але інших понять, як-от поняття «кіберправосуддя». Останнє стосується загального включення технологій у систему правосуддя. Згідно з Керівними принципами щодо змін у напрямі кіберправосуддя (Європейська комісія з питань ефективності правосуддя Ради Європи, грудень 2016 року) кіберправосуддя «в широкому сенсі — це об'єднання всіх ситуацій, у яких застосування ІКТ є тільки частиною процесу вирішення спорів, чи то в судовому, чи позасудовому порядку». Отже, поняття «кіберправосуддя» є ширшим ніж поняття «онлайн вирішення спорів», оскільки охоплює не лише ОВС, а й інші механізми.

21. Для цілей цих керівних принципів під ОВС варто розуміти технологію, яку використовують для вирішення спору дистанційно за допомогою комп'ютерів, зокрема мобільних пристроїв та інтернету. ОВС як таке не є формою вирішення спорів, а радше належить до інформаційних технологій (ІТ), які використовуються в межах судових проваджень. Це не новий вид розгляду й не альтернатива будь-якому такому судовому розгляду. ОВС надає нові способи доступу до наявних видів судового розгляду. Це поняття випливає з триваючої трансформації національних судових систем у більш цифрову форму з можливістю віддаленого доступу для сторін. Механізми ОВС призначені для полегшення електронних комунікацій і отримання результату без необхідності фізичного подання документів або фізичної присутності в судовому засіданні чи зустрічі. З огляду на це Комісія ООН із права міжнародної торгівлі (ЮНСІТРАЛ) у своїх Технічних коментарях щодо онлайн вирішення спорів (Нью-Йорк, 2017 року) визначає ОВС як

«механізм вирішення спорів через використання електронних комунікацій та інших інформаційно-комунікаційних технологій».

22. Керівні принципи охоплюють такі методи ОВС, як:

    i. онлайн-системи/платформи, безпосередньо доступні сторонам та/або їх представникам для подання заяв (як-от позови, зустрічні позови, відповіді тощо);

    ii. онлайн-системи для зберігання, обробки та оцінювання електронних доказів;

    iii. штучний інтелект, методи аналізу великих баз даних і автоматизація тією мірою, якою вони впливають на судочинство;

    iv. платформи для проведення судових нарад і засідань у режимі онлайн, наприклад, за допомогою аудіо- та відеоконференцій, зокрема для надання усних показань свідками та експертами.

Штучний інтелект (ШІ)

23. Штучний інтелект (ШІ) — це широка галузь інформаційно-комунікаційних технологій (ІКТ), яка швидко розвивається й уможливлює автоматичне формулювання висновків. ШІ створює потенціал для прийняття автоматизованих рішень, рекомендацій і прогнозів, а отже, може зробити цивільне та адміністративне провадження ефективнішим, доступнішим й менш затратним.

24. Проте важливо розуміти, що ОВС — це не те саме, що ШІ. Не всі механізми ОВС містять компоненти ШІ. ОВС — це ширше поняття, що охоплює всі види механізмів онлайн вирішення спорів, зокрема інструменти для автоматизації, які не обов'язково мають елемент ШІ. Відмінність між ОВС і ШІ збережено у всьому тексті керівних принципів. Хоча вимоги щодо дотримання гарантій, що випливають зі статей 6 і 13 Європейської конвенції з прав людини, стосуються всіх механізмів ОВС, незалежно від того, чи мають вони елементи ШІ чи ні, деякі питання в цьому контексті мають більше значення, коли йдеться про механізми ШІ. Це особливо стосується питань, пов'язаних з автоматизованим прийняттям рішень без втручання людини й можливості перегляду цих рішень.

25. Система ШІ — це інформаційна система, що працює як програмне забезпечення або інтегрована у фізичний апаратний пристрій і розв'язує складні проблеми та функціонує як у фізичному, так і в цифровому вимірах. Така система функціонує через сприйняття свого середовища за допомогою збору та інтерпретації зібраних, структурованих і неструктурованих даних, роблячи висновки з наявних знань, обробляючи отриману на основі цих даних інформацію задля

прийняття рішень про найбільш прийнятні дії, яких необхідно вжити для досягнення поставленої мети.

26. Для цілей цих керівних принципів визначенням ШІ є те, що запропоноване в Європейській етичній хартії з використання штучного інтелекту в судових системах та їх середовищі, ухваленій Європейською комісією з питань ефективності правосуддя (CEPEJ) 3–4 грудня 2018 року. У Хартії викладено п'ять принципів, якими варто керуватися під час розроблення інструментів ШІ в європейських судових системах. Ці п'ять принципів відображено в керівних принципах, присвячених ШІ. У цих керівних принципах також враховано визначення ШІ, запропоноване в Повідомленні Європейської комісії про ШІ й доопрацьоване незалежною експертною групою високого рівня з питань штучного інтелекту, створеною Європейською комісією. У керівних принципах також враховано визначення системи ШІ, яке міститься в Рекомендації Ради ОЕСР із питань штучного інтелекту, ухваленій у 2019 році.

Інформаційно-комунікаційні технології (ІКТ)

27. Термін «інформаційно-комунікаційні технології» (ІКТ) означає технології, що забезпечують доступ до інформації за допомогою телекомунікацій. Сюди входять інтернет, бездротові мережі, стільникові телефони та інші засоби зв'язку. Наприклад, особи, які беруть участь в ОВС, можуть спілкуватися в режимі реального часу за допомогою таких технологій, як обмін миттєвими повідомленнями, голосовий зв'язок за протоколом IP (VoIP) і відеоконференції.

ОСНОВНІ ПРИНЦИПИ

Принцип 1

28. Зміцнення довіри до ОВС та впевненості в ній має вирішальне значення для належного використання ІКТ у судах. Наразі часто трапляється, що люди, іноді навіть судді, сумніваються, чи варто використовувати механізми ОВС, особливо якщо залучені компоненти ШІ. Основний виклик полягає в тому, як держави-члени можуть створити і зміцнити довіру до ОВС та впевненість у ній. Це можна зробити тільки через застосування тих самих ключових принципів справедливого судового розгляду й ефективного засобу правового захисту, які Європейський суд з прав людини розробив у своїй практиці в контексті існуючих судових проваджень. Ці основні принципи необхідно додатково роз'яснити й перенести в контекст ІКТ. Необхідно проаналізувати та надати відповіді на конкретні виклики, що виникають під час застосування цих принципів у контексті ОВС.

29. Держави-члени можуть використати ці керівні принципи для створення міцної правової та етичної основи для використання ОВС. Підхід захисту прав людини має стати вихідною позицією для розроблення механізмів ОВС, щоб зробити правосуддя ефективним і дієвим. Держави-члени можуть також створити і зміцнити довіру до ОВС та впевненість у ньому, пояснивши громадськості, що ОВС не покликане повністю замінити наявні судові процедури, а радше доповнити їх і створити додаткові можливості для доступу до правосуддя. ОВС треба розглядати як допоміжний засіб для ухвалення судових рішень і полегшення роботи судді, а не як обмеження. ОВС має бути адаптованим до потреб суддів та інших користувачів і жодним чином не має порушувати гарантій та процесуальних прав, як-от право на справедливий розгляд справи суддею. ОВС має покращувати відправлення правосуддя, полегшувати доступ користувачів до судів і зміцнювати гарантії, викладені в статті 6 Європейської конвенції з прав людини: доступ до правосуддя, безсторонність та незалежність судді, справедливість і розумна тривалість розгляду.

Практика Суду Європейського Союзу

Судовий захист, про який ідеться в статтях 6 і 13 Європейської конвенції з прав людини, забезпечується доти, доки електронні засоби є не єдиним засобом доступу до процедури (врегулювання) (об'єднані справи C-317/08–C-320/08, «Розальба Алассіні та Філомена Каліфано проти «Вінд SpA», Лючія Анна Джорджа Яконо проти «Телеком Італія SpA» і «Мультисервіс Srl» проти «Телеком Італія SpA» (Rosalba Alassini and Filomena Califano v. Wind SpA, Lucia Anna Giorgia Iacono v. Telecom Italia SpA and Multiservice Srl v. Telecom Italia SpA), рішення Європейського Суду від 8 березня 2010 року, пп. 58 і 60).

Принцип 2

30. ОВС може сприяти ефективнішому й дієвішому доступу до правосуддя. Проте основною перешкодою для ширшого використання ОВС є доступ до технології. Деякі люди не мають необхідних навичок або можливостей для використання ОВС і вирішення спору онлайн (цифровий бар'єр). Наприклад, вони можуть бути не обізнані з використанням цифрових додатків або не мати доступу до інтернету, комп'ютера або інших інструментів чи технологій. Ця група людей повинна мати можливість отримувати відповідну допомогу. Державам-членам варто розробляти ОВС у спосіб, який би адекватно розв'язував проблему цифрового бар'єру. Наприклад, механізми ОВС можна зробити необов'язковими. Влада може створити пункти підтримки в приміщеннях судів або в бюро юридичної допомоги. Можна створити допоміжні програми для населення. Застосування пілотних проєктів і зворотного зв'язку з користувачами також

допомагає розв'язати проблему цифрового бар'єру. Як пояснено в керівних принципах, механізми ОВС повинні мати простий і зручний для користувача інтерфейс, щоб якомога більше людей могли користуватися технологією.

Принцип 3

31. Цей принцип вимагає, щоб за відсутності будь-яких особливостей, пов'язаних із використанням конкретних механізмів ОВС, на процесуальні питання поширювалися ті самі правила, що й на відповідну судову процедуру за загальними правилами. До ОВС можуть і мають застосовуватися ті самі стандарти належної правової процедури, що й до судової офлайн-процедури, зокрема стандарти незалежності, нейтральності та безсторонності. Будь-які коригування загальних процедурних правил, що вносять з огляду на особливий характер механізму ОВС, не мають підривати принципи справедливого судового розгляду й ефективного засобу правового захисту.

Принцип 4

32. Важливо, щоб сторони провадження, у якому використовують ОВС, були належно ідентифіковані й не було шахрайства з ідентичністю. Відокремлення цифрової ідентичності від фізичної може створити проблеми, пов'язані з ідентифікацією сторін. Насамперед суди мають прагнути до індентифікації сторін. До таких надійних механізмів належать, зокрема: i) сертифікати до електронних підписів, які іноді називають «цифровим посвідченням» особи; ii) підтвердження особи оператором платіжної системи, яка використовувалася для онлайн-оплати судових витрат; iii) публічні трастові служби, що надають технологічні механізми, які забезпечують належну ідентифікацію.

КЕРІВНІ ПРИНЦИПИ

Справедлива процедура

Доступ до правосуддя

Керівний принцип 1

33. Правосуддя — для всіх. У багатьох державах — членах ЄС заявники можуть подавати свої справи без участі адвоката, тому особливо важливо зробити весь процес зрозумілим. Задля підвищення доступності система ОВС має бути розроблена так, щоб інтерфейс для користувачів був максимально простим й інтуїтивно зрозумілим для користувача. За можливості, інструменти ОВС мають бути доступні цілодобово і без вихідних з різних операційних систем комп'ютерів та мобільних пристроїв. ОВС має надавати сторонам можливість використовувати стандартні форми, завантажувати відповідні документи

й отримувати своєчасні відповіді. За допомогою ОВС суди повинні також мати можливість використовувати зв'язок у режимі реального часу. Наскільки це дозволяє національна правова система, технічні засоби, наявні в ОВС, можуть забезпечувати гнучкість щодо мови, використовуваної під час розгляду, наприклад, за допомогою вбудованих програм перекладу у випадку багатомовного розгляду за участю сторін із різних держав або культур. Принцип зручності для користувачів не має поширюватися тільки на сторони провадження та їхніх представників; інструменти ОВС мають бути однаково зручні для суддів та інших працівників суду.

Керівний принцип 2

34. Сторони повинні мати доступ до всієї необхідної інформації. Тому важливо надавати користувачам відповідну допомогу, інформацію і зворотний зв'язок. Під час розроблення ОВС можна зробити допомогу (наприклад, як керівництво для користувача) легкодоступною. Така допомога може містити інформацію про те, як подати позов і отримати інформацію про хід розгляду справи. ОВС може структурувати процес для сторін провадження. Це також означає, що врегулювання спорів за допомогою ОВС може здійснюватися практично в будь-якому місці, що робить процес зручним і простим для сторін.

Практика Європейського суду з прав людини

Якщо відповідний закон надає особам можливість подавати скаргу без участі адвоката, національним судам варто консультувати заявників про те, як усунути формальні недоліки їхніх скарг [«Венде і Куковка проти Польщі» (Wende and Kukówka v. Poland), № 56026/00, п. 54, 10 травня 2007 року].

Велика хартія суддів

У Великій хартії суддів, ухваленій Консультативною радою європейських суддів (КРЄС) у 2010 році, у пункті 14 «Доступ до правосуддя та прозорість» ідеться про те, що «правосуддя має бути прозорим, а інформація про роботу судової системи має оприлюднюватися».

Національний приклад: Польща

У Польщі заявникам надано можливість знайти всю відповідну інформацію про необхідні формальні вимоги й технічні питання на сайті електронного суду (загальну інформацію про електронний суд, інформацію для заявника та відповідача, приклади правильних і неправильних заяв, типові питання, правила онлайн-платежів тощо).

Керівний принцип 3

35. Важливо, щоб кожна сторона мала справедливу та рівну можливість аргументувати свою позицію як з питань факту, так і з питань права,

а також мала право реагувати на подання іншої сторони та спростовувати їх. Обидві сторони повинні мати змогу відкривати докази й відповідні матеріали в доступний спосіб. ОВС прискорює процеси, але водночас створює ризик збільшення інформаційного перевантаження (що сповільнює оброблення інформації). З огляду на це, хоча спори необхідно розглядати впродовж розумного строку, сторони повинні мати необхідний для реагування час.

Практика Європейського суду з прав людини

Принцип рівності сторін передбачає, що кожна сторона повинна мати розумну можливість представити свою справу, зокрема докази, в умовах, які не ставлять її в суттєво невигідне становище порівняно з опонентом [«Летінчич проти Хорватії» (Letinčić v. Croatia), № 7183/11, п. 48, 3 травня 2016 року].

Керівний принцип 4

36. Під час розроблення ОВС варто керуватися міжнародно визнаними технічними стандартами, як-от принципи універсального дизайну в контексті ІКТ. Це передбачає орієнтований на користувача підхід і відсутність перешкод у використанні ОВС через бар'єри в технічному дизайні і функціональних можливостях, а також вартість використання. Дотримання цих стандартів зробить контент доступним для ширшого кола людей, як-от люди з обмеженими можливостями, і зробить ОВС доступнішим для користувачів загалом. Зокрема, ОВС може не обмежуватися виключно текстовою комунікацією, а уможливлювати візуальну й аудіокомунікацію сторін (відео- або аудіоконференції). Варто сприяти розробленню систем ОВС, що дозволяють використовувати ефективніші види комунікацій. Це не виключає розроблення систем ОВС, що забезпечують можливість багатоваріантного вибору видів комунікації (текстової, аудіо, візуальної або різних ІКТ). ОВС має функціонувати належно, забезпечуючи конфіденційність комунікації та дозволяючи встановити контакт, якому не перешкоджають жодні практичні або інші обставини [«Марсело Віола проти Італії» (*Marcello Viola v. Italy*), № 45106/04, пп. 63–77, ЄСПЛ 2006-XI (витяги); «Голубєва проти Росії» (*Golubeva v. Russia*), № 1062/03, 17 грудня 2009 року].

Керівний принцип 5

37. ОВС за своєю природою може забезпечити економію коштів і стати економічною альтернативою розгляду, що здійснюється традиційним способом. Як наслідок, можна очікувати, що вартість використання ОВС для сторін має бути принаймні такою самою, що й вартість доступу до системи правосуддя з використанням ресурсів

безпосередньо на місці. За наявності загальних правил звільнення від витрат і надання безоплатної допомоги їх варто застосовувати й до ОВС.

Керівний принцип 6

38. Необхідно повідомляти сторони про те, що їхню справу розглядатимуть за допомогою ОВС із застосуванням механізму штучного інтелекту. Зокрема, сторони мають право на інформацію про підстави застосування в їхній справі операцій з обробки даних із використанням ШІ. Така інформація має описувати й наслідки такого застосування. Цю вимогу прозорості також підтверджено всіма наявними рекомендаціями, етичними кодексами й керівними принципами, у яких визначено етичні стандарти для розроблення, впровадження та використання штучного інтелекту, як встановлено Радою Європи, органами ООН, Європейським Союзом, ОЕСР та іншими міжнародними інституціями. Розробники, інженери, постачальники, адміністратори та професійні користувачі ОВС мають дотримуватися цих стандартів.

Рівність сторін

Керівний принцип 7

39. У керівних принципах чітко вказано, що ОВС не має позбавляти сторону права бути заслуханою судом. Права на доступ до суду, змагальне провадження та ефективний засіб судового захисту є основоположними правами, які гарантовано Європейською конвенцією з прав людини. Попри свою важливість, цілі досягнення ефективності та прискорення судочинства не можуть виправдовувати порушення цих прав.

Керівний принцип 8

40. Незалежність і безсторонність процесів прийняття рішень у межах ОВС є найважливішими вимогами для забезпечення дотримання стандартів Європейської конвенції з прав людини. Довіра і впевненість в ОВС формуються завдяки недопущенню упередженості (або будь-якого суб'єктивного сприйняття наявності упередженості) щодо інтересів будь-якої зі сторін. Пункт 1 статті 6 Європейської конвенції з прав людини прямо вказує, що суд має бути незалежним і безстороннім. Це ще важливіше в контексті механізмів ОВС, оскільки вони можуть передбачати процес, у якому суддя не присутній фізично, унаслідок чого можуть виникнути питання довіри.

Керівний принцип 9

41. Знання матеріалів справи, зокрема матеріалів, наданих іншими сторонами, і доступ до них є необхідною умовою справедливого

розгляду. До того ж матеріали справи, включаючи всі відповідні метадані, мають бути достатньо точними й докладними, щоб сторони за бажанням могли оскаржити їх зміст. Якщо стороні бракує часу, варто передбачити можливість для такої сторони запросити додатковий час. Ці керівні принципи охоплюють не лише доступ до документів, поданих іншими сторонами, а й матеріали справи, які часто містять документацію, що підготував суд.

Практика Європейського суду з прав людини

Вимога «змагальності» провадження відповідно до статті 6 Європейської конвенції з прав людини передбачає можливість ознайомитися із зауваженнями або доказами, які надала інша сторона, і прокоментувати їх. «Змагальність» по суті означає, що відповідні матеріали або докази мають бути доступні обом сторонам [«Руїз-Матеос проти Іспанії» (Ruiz-Mateos v. Spain), 23 червня 1993 року, п. 63, Серія A № 2].

Докази

Керівний принцип 10

42. Важливо забезпечити, щоб сторони розгляду, у якому використовують ОВС, не опинялися в невигідному становищі через відсутність доступу до цифрових послуг або нерозуміння того, як ці послуги працюють. ОВС має бути якомога зручнішим для користувачів і працювати так, щоб не порушувати інтересів будь-якої зі сторін. Див. Керівні принципи щодо електронних доказів (зокрема, частину про основні принципи).

Керівний принцип 11

43. Використання електронних доказів може створити особливі проблеми для сторони, яка бажає оскаржити автентичність або цілісність таких доказів. ОВС має забезпечувати відповідні гарантії задля полегшення такого оскарження. Для цього можна використовувати інструкції, шаблони або інші інструменти. Наприклад, у разі оскарження електронних доказів, тій стороні, яка подає ці докази, може знадобитися продемонструвати їх автентичність, наприклад, через надання метаданих або отримання відповідного розпорядження про отримання додаткових даних від інших осіб, як-от постачальників трастових послуг. Достовірність електронних даних можна довести будь-яким способом, наприклад, за допомогою кваліфікованих електронних підписів або інших аналогічних методів ідентифікації й забезпечення цілісності даних. Варто дотримуватися положень національного законодавства, які встановлюють доказову силу державних (офіційних) електронних систем, що генерують електронні докази. Крім того, сторонам варто дозволити оскаржувати свідчення експертів, якщо такі свідчення можуть визначити результат розгляду.

У всіх цих випадках ОВС має дотримуватися міжнародних стандартів, що застосовуються до аналізованих даних, наприклад, стандартів, опублікованих міжнародними інституціями зі стандартизації, як-от Міжнародна організація зі стандартизації (ISO). Стандартизація моделей комунікації може забезпечити значне підвищення ефективності. Див. Керівні принципи щодо електронних доказів (зокрема, керівні принципи № 17–24 розділу про відповідність електронних доказів).

Керівний принцип 12

44. Особливі проблеми можуть виникнути під час розгляду доказів у судах із використанням механізмів ОВС. Ці проблеми вказують на необхідність послідовності в роботі з доказами. Важливо уникати суперечливої судової практики і сприяти юридичній визначеності. З огляду на це національна правова система може дозволити сторонам спиратися на попередні рішення, ухвалені судом у подібних або ідентичних справах. Це може допомогти сторонам структурувати свої докази на основі таких попередніх рішень або шаблонів, оприлюднених судами на вебсторінках. Держави-члени можуть видати конкретні рекомендації, наприклад, щодо формату даних, які буде подано як докази. Однак такі рішення не мають підривати незалежність суддів.

Ефективне провадження

Керівний принцип 13

45. Оскільки значна кількість рішень Європейського суду з прав людини стосується порушення статті 6 Європейської конвенції з прав людини в контексті надмірної тривалості судового розгляду, для держав-членів вкрай важливо активізувати зусилля щодо усунення цієї проблеми. Ефективне провадження вимагає уникнення невиправданих затримок. У цьому контексті ОВС надає перевагу. Крім того, завдяки використанню компонентів штучного інтелекту можна істотно покращити роботу суду. Використання компонентів ШІ може прискорити процедуру й уможливити більш повний аналіз справи. Ефективного провадження можна досягти тільки за умови максимальної раціоналізації процесу. Зокрема, суд повинен вимагати фізичної присутності сторін лише в разі потреби. ОВС може допомогти уникнути необхідності у фізичній присутності не лише сторін, а й інших учасників процесу, чия присутність в іншому випадку була б необхідною, що часто створює проблеми й уповільнює процес. Багато держав-членів у своїх судах використовують відеоконференції з особами, які перебувають у віддаленому місці, щоб забезпечити, наприклад, явку свідків і експертів. Правильно розроблене ОВС також дозволяє оплачувати судові витрати в режимі онлайн. Див. Керівні принципи щодо

електронних доказів (зокрема, керівні принципи 1–5 розділу про усні докази, одержані через віддалені канали зв'язку).

Практика Європейського суду з прав людини

Своєю вимогою розглядати справи впродовж «розумного строку» Суд підкреслює важливість відправлення правосуддя без затримок, які можуть поставити під загрозу його ефективність і довіру до нього [«X. проти Франції» (H. v. France), 24 жовтня 1989 року, п. 58, Серія A № 162-A; «Катте Клітске де ла Грандже проти Італії» (Katte Klitsche de la Grange v. Italy), 27 жовтня 1994 року, п. 61, Серія A № 293-B].

Держава може бути визнана відповідальною не лише за затримку в розгляді конкретної справи, а й за нездатність збільшити ресурси для розгляду накопичених справ або за структурні недоліки судової системи, які призводять до затримок. Отже, для розв'язання проблеми необґрунтованої затримки судового провадження державам треба вжити низку законодавчих, організаційних, бюджетних та інших заходів [«Рутковський та інші проти Польщі» (Rutkowski and Others v. Poland), № 72287/10 та 2 інші, п. 128, 7 липня 2015 року].

Керівний принцип 14

46. Особливу увагу варто приділяти тому, щоб провадження не затягувалося без необхідності через технічні труднощі. Щоб уникнути небажаного впливу на діяльність суду, завжди мають бути доступні альтернативні варіанти на той випадок, якщо система ІКТ перебуває на технічному обслуговуванні або має технічні проблеми. Такі технічні труднощі не мають шкодити сторонам, і за потреби повинна існувати можливість коригування строків, які передбачають накладення санкції.

Керівний принцип 15

47. Для забезпечення ефективного, своєчасного та адекватного вирішення спорів і їх зменшення держави-члени можуть впровадити пірамідальну модель вирішення спорів, згідно з якою винесення рішення суддею є останнім рівнем такого вирішення. Дружнє врегулювання спорів із застосуванням АВС може забезпечити економічно ефективний і більш задовільний для сторін результат, ніж судовий розгляд. Однак спроби вирішити спір за допомогою АВС до порушення судового розгляду мають бути розумними й не мають ставити під загрозу або заперечувати доступ до суду як основоположне право, захищене статтею 6 Європейської конвенції з прав людини. Використання згаданих вище методів і механізмів не повинно створювати істотних затримок або істотно збільшувати витрати сторін.

Винесення рішення

Керівний принцип 16

48. Ознайомлення сторін із результатами провадження, у якому застосовувалося ОВС, є важливим із трьох причин: 1) для забезпечення рівності сторін щодо інформації, 2) для забезпечення можливості ретельного вивчення результатів і їх оскарження за потреби та 3) для визначення напряму розвитку законодавства. У контексті ОВС найважливішими чинниками є громадський контроль і вимога про проведення розгляду в розумний строк із дотриманням належної правової процедури.

Керівний принцип 17

49. Цей керівний принцип випливає з права на публічне винесення судового рішення. У пункті 1 статті 6 Європейської конвенції з прав людини прямо вказано, що судове рішення проголошується публічно. Однак це не вимагає зачитування рішення у відкритому судовому засіданні. Можна використовувати інші способи оприлюднення рішення, наприклад, надавати рішення за запитом [«Мозер проти Австрії» (*Moser v. Austria*), № 12643/02, п. 101, 21 вересня 2006 року]. У кожному окремому випадку форму оприлюднення необхідно оцінювати з огляду на особливості кожного окремого провадження [«Претто та інші проти Італії» (*Pretto and Others v. Italy*), 8 грудня 1983 року, п. 26, Серія A № 71; «Аксен проти Німеччини» (*Axen v. Germany*), 8 грудня 1983 року, п. 31, Серія A № 72]. Наприклад, повний текст рішення можна розмістити на сайті суду. Згідно з практикою Європейського суду з прав людини вимога про публічне проголошення вважається дотриманою, якщо повний текст рішення було внесено до судового реєстру, а отже, він став доступним для всіх («Претто та інші проти Італії», згадана вище, пп. 27–28).

Право на обґрунтоване рішення

Керівний принцип 18

50. Кожне судове рішення, ухвалене з використанням ОВС або за сприяння ОВС, має бути чітким, щоб кожен учасник процесу міг зрозуміти, чому суд підтримує певну позицію [«Серявін та інші проти України» (*Seryavin and Others v. Ukraine*), № 4909/04, пп. 55–62, 10 лютого 2011 року]. ОВС не відміняє права на отримання пояснення ухваленого рішення. Суд має навести достатньо деталізовані аргументи. Обсяг обов'язку щодо обґрунтування залежить від характеру рішення й обставин справи. Варто вивчити основні аргументи сторін, які вимагають конкретної та чіткої відповіді. Належно обґрунтовані рішення необхідні, по-перше, для того, щоб запевнити сторони в тому, що їхні аргументи було враховано під час ухвалення рішення, і, по-друге,

щоб допомогти стороні вирішити, чи має вона достатньо підстав для оскарження рішення. Тільки через винесення обґрунтованого рішення можна забезпечити громадський контроль за відправленням правосуддя. Це означає, що щонайменше результат провадження має бути відомим сторонам.

Виконання рішення

Керівний принцип 19

51. Виконання остаточного й обов'язкового рішення, ухваленого в результаті роботи механізму ОВС, має бути невіддільною частиною «права на суд» для цілей статті 6 Європейської конвенції з прав людини. Кожна сторона судового розгляду із застосуванням ОВС має право на виконання судового рішення, а затримка у виконанні судового рішення не має бути такою, яка порушує право сторони на справедливий суд. Право на виконання судових рішень набуває ще більшого значення в контексті адміністративного провадження [«Шарджі та інші проти Албанії» (*Sharxhi and Others v. Albania*), № 10613/16, п. 92, 11 січня 2018 року]. ОВС може сприяти прискоренню виконавчого провадження так само, як може прискорити стадію провадження. Наприклад, національне законодавство може передбачати надсилання судовому виконавцю виконавчого листа в електронній формі безпосередньо через ІТ-систему. Електронний зв'язок із судовим виконавцем дозволяє швидше і простіше контролювати виконання судових рішень.

Практика Європейського суду з прав людини

Неможливо уявити, щоб у пункті 1 статті 6 було докладно описано процесуальні гарантії, надані сторонам провадження (справедливе, публічне і швидке провадження), але не передбачено захисту виконання судових рішень <...>. Відтак виконання рішення, ухваленого будь-яким судом, слід розглядати як невіддільну частину «судового процесу» для цілей статті 6 Європейської конвенції з прав людини [«Бурдов проти Росії» (Burdov v. Russia), № 59498/00, п. 34, ЄСПЛ 2002-III]. Тому необґрунтовано тривала затримка у виконанні обов'язкового судового рішення може порушувати Конвенцію [«Бурдов» (№ 2), № 33509/04, п. 66, ЄСПЛ 2009].

Національний приклад: Литва

Справи щодо судових наказів про стягнення коштів здебільшого розглядають із використанням онлайн-звернення й цифрового управління справами. Судові накази зазвичай видають як цифрові офіційні документи із захищеними електронними підписами, які в електронній формі можна передати судовому виконавцеві для забезпечення виконання.

Право на судовий перегляд у справах, пов'язаних із виключно автоматизованими рішеннями

Керівний принцип 20

52. Не може бути єдиної або простої відповіді на питання про те, як має здійснюватися право на перегляд рішення, ухваленого з використанням елемента ОВС, оскільки це залежить від характеру й обсягу відповідного елемента ОВС. Якщо ОВС відіграє лише другорядну роль і просто допомагає судді в провадженні, немає причин відступати від стандартних правил оскарження, які застосовуються до проваджень, що не містять елементу ОВС. Однак це питання стає вирішальним, коли інструменти ОВС є інструментами для ухвалення суто автоматизованих рішень. Сценарії, у яких механізми ОВС застосовуються для ухвалення суто автоматизованих рішень, варіюються від незначних справ, які легко автоматизувати, оскільки вони юридично прості, а механізм ОВС здебільшого застосовують для розрахунків до складних справ, у яких використовуються новітні механізми штучного інтелекту.

53. Однак саме в цьому контексті на перший план виходить стаття 13 Європейської конвенції з прав людини. Стаття 13 передбачає, що кожен, чиї права та свободи, визнані в цій Конвенції, було порушено, має право на ефективний засіб юридичного захисту в національному органі. Сторонам має бути дозволено оскаржувати суто автоматизовані рішення і вимагати, щоб такий перегляд здійснював суддя. Європейський суд з прав людини не уточнює, на якому рівні має реалізовуатись цей засіб юридичного захисту. Фактично можливі дві моделі: держава-член вирішує, чи варто здійснювати перегляд на тому ж судовому рівні або на вищому апеляційному рівні. Використання ОВС може відкрити нові шляхи захисту порушених прав у національних судових системах. З огляду на унікальний характер ОВС держава-член може прийняти рішення (незалежно від наявних механізмів перегляду) про створення додаткового процесу перегляду на тому ж рівні, на якому було ухвалено автоматизоване рішення. Або ж держава-член може залишити перегляд справи суддею на наявному рівні оскарження. У будь-якому разі в цих керівних принципах не встановлено вимоги автоматичного перегляду всіх автоматизованих рішень або зміни наявної моделі перегляду.

Практика Європейського суду з прав людини

У статті 13, у якій прямо йдеться про обов'язок держав захищати права людини передусім у межах власних правових систем, встановлено додаткову гарантію, яка забезпечує ефективне користування цими правами [«Кудла проти Польщі» (Kudła v. Poland) (ВП), № 30210/96, п. 152, ЄСПЛ 2000-XI].

Консультативна рада європейських суддів — Висновок № 14 (2011)

Впровадження ІТ у судах Європи не повинно шкодити «людському обличчю» та символічному значенню правосуддя. <...> Правосуддя має залишатися гуманним, оскільки воно стосується насамперед людей та спорів між ними.

Прозорість використання ОВС та вимоги до судових засідань

Прозорість у розробленні та функціонуванні механізмів ОВС

Керівний принцип 21

54. Прозорість ОВС має вирішальне значення. Задля сприяння доступу до правосуддя треба роз'яснювати громадськості принципи розроблення й роботи механізмів ОВС зрозумілою мовою. Громадськість має розуміти наслідки використання ОВС і знати, що ОВС працює добре та що результати вирішення спорів за його сприяння є справедливими. Ці керівні принципи виходять за межі простої вимоги щодо оприлюднення основної інформації про розроблення і використання ОВС в інтернеті. Для залучення громадськості можна використовувати різні методи. Справжні комунікаційні стратегії та політика передбачають пресрелізи, відеотрансляції, а також вебінари або публікації в соціальних мережах. Держави-члени можуть пояснити громадськості, що ОВС робить правосуддя доступнішим, зокрема через відсутність необхідності фізичної присутності в суді, економію витрат на поїздку в суд, можливість подавати документи за допомогою електронних засобів, забезпечення довіри і зменшення стресу для осіб, які представляють себе в судовому провадженні.

Публічні та усні слухання

Керівний принцип 22

55. Діяльність традиційного суду (фізичної будівлі суду) є очевидною для громадськості й може бути перевірена представниками громадськості через відвідування публічних слухань. Інша річ, коли провадження або окремі слухання проводять дистанційно в електронній формі за допомогою механізмів ОВС. Варто пам'ятати, у чому полягає мета публічних слухань: вони дозволяють громадськості здійснювати громадський нагляд за рішеннями та судовим процесом. Забезпечення прозорості провадження в такий спосіб є формою підзвітності, яка підвищує справедливість. Таку функцію громадського контролю необхідно забезпечити й під час дистанційного електронного провадження з використанням інструментів ОВС. Цих цілей можна досягти як традиційними, так і новими засобами. З технічного погляду цифрові суди можна зробити відкритими навіть більше ніж будівлі фізичних судів. Конкретне технічне рішення залежить від відповідної процедури. Наприклад, якщо віртуальні слухання в судах

замінюють судове слухання, ОВС може забезпечити контрольований доступ громадськості до віртуальних слухань та інформації без необхідності фізичної присутності спостерігачів у залі суду. ОВС не вимагає організації традиційних публічних слухань, але її можна застосовувати для забезпечення публічності слухань під час використання інструментів ОВС, які забезпечують віддалену (віртуальну) присутність на слуханнях сторін, свідків, експертів або когось із них; судді та/або спостерігачі можуть водночас бути фізично присутніми в залах суду або будь-яких інших приміщеннях, де можна транслювати судові слухання. У будь-якому разі вимога публічних слухань не вимагає від держав-членів відкривати віртуальні слухання для необмеженого числа одночасних трансляцій для громадськості, так само як кількість місць у фізичному залі суду також обмежена. Будь-який такий варіант має передбачати належні гарантії щодо захисту персональних та інших конфіденційних даних, достатньої кібербезпеки й інших принципів, про які йдеться в цих керівних принципах.

Керівний принцип 23

56. ОВС не спрямоване на закриття судів і залів засідань. Його мета полягає в підвищенні ефективності та результативності. Право на усне слухання не обов'язково вимагає фізичної присутності, а відеоконференції можуть у належний спосіб гарантувати сторонам їхнє право, наприклад, якщо сторони добровільно відмовляються від права на фізичну присутність [«Володимир Васильєв проти Росії» (*Vladimir Vasilyev v. Russia*), № 28370/05, пп. 81–90, 10 січня 2012 року]. Залежно від справи, відеоконференції, у яких учасники можуть чути й бачити один одного в режимі реального часу (і в яких передбачено, що на свідків не тиснуть поза екраном та що особу свідків належно встановлено), можуть функціонувати як «усні» слухання (за умови, що технологія працює на обох кінцях трансляції та її можна архівувати). Усне слухання не завжди необхідне для забезпечення участі сторін у провадженні. Можна проводити письмове провадження з використанням механізмів ОВС за умови, що сторони мають право на усне слухання у формі перегляду на тому самому рівні або слухання на апеляційному етапі провадження. Наприклад, в адміністративному провадженні усне слухання в певному органі є обов'язковим тільки в деяких випадках, а увагу більше зосереджено на праві на активну участь у провадженні в широкому розумінні на будь-якому його етапі. Така участь не вимагає усних слухань, а передбачає можливість сторони висловити свою думку про матеріали справи, зокрема зібрані докази та клопотання, подані іншою стороною [«Вільхо Ескелайнен та інші проти Фінляндії» (*Vilho Eskelinen and Others v. Finland*) (ВП), № 63235, п. 74, ЄСПЛ 2007-II]. Використання ОВС може підвищити ефективність письмового провадження.

Інші питання прозорості, зокрема громадський контроль

Керівний принцип 24

57. Гарантії незалежності та безсторонності судової влади необхідно ефективно інтегрувати в судові провадження, у яких застосовується ОВС [«Агрокомплекс проти України» (*Agrokompleks v. Ukraine*), № 23465/03, п. 136, 6 жовтня 2011 року]. ОВС має бути прозорим із погляду встановлення особи і належності постачальників ОВС, а також осіб, що вступають у судовий процес, й адміністраторів механізмів ОВС. Державам-членам варто ухвалити політику, спрямовану на виявлення та врегулювання конфлікту інтересів у ОВС.

Керівний принцип 25

58. Гарантії, закріплені в пункті 1 статті 6 Європейської конвенції з прав людини, містять зобов'язання складати всі документи, підготовлені в межах ОВС, зокрема остаточне судове рішення та інші рішення або повідомлення, чітко зрозумілою мовою. Мова складання документів має уможливлювати ефективне використання сторонами будь-якого наявного права на оскарження.

Керівний принцип 26

59. Процедурні правила, застосовні до ОВС, мають надавати розуміння процесів вирішення спору. Ці правила мають відповідати вимогам суспільства, установи та правової бази, у межах яких їх застосовують. Зокрема, механізми ОВС мають передбачати процедури усунення чинників, які можуть зашкодити справедливому використанню ОВС. Наприклад, у межах ОВС може знадобитися розкрити або приховати різні частини інформації залежно від стадії процесу й типу користувача. З огляду на це в ОВС можна інтегрувати низку заходів зі зниження ризиків і підвищення безпеки, що широко застосовують в інших секторах, зокрема в банківському секторі, системі онлайн-платежів і секторі охорони здоров'я. Ці процедури необхідно врахувати в архітектурі ОВС.

Керівний принцип 27

60. Відповідну інформацію можна розмістити на вебсайті суду в зручній і доступній для користувача формі. Наприклад, на вебсайті суду можна застосовувати послуги з перетворення тексту на аудіозапис. Ефективне управління інформацією ОВС гарантує, що інформація є достовірною й надійною, її можна швидко й легко знайти, її зберігають упродовж належного періоду, використовують із засобами захисту та належно захищають. Прозорість процедурних правил, застосовних до ОВС, сприяє підвищенню довіри, підзвітності, відкритості та ефективності.

Спеціальні питання, пов'язані з ІКТ-характером методів ОВС

Кібербезпека

Керівний принцип 28

61. Система правосуддя є вразливою через чимраз складніші й численніші кібератаки на суди. Використання ОВС викликає побоювання щодо збільшення кількості порушень безпеки, які можуть загрожувати цілісності судової системи й оброблюваних нею даних. Кіберзагрози є цілком реальною небезпекою для систем правосуддя. Існує ризик, що судові документи та докази можуть стати об'єктом маніпуляцій і атак. Порушення безпеки може призвести до підроблення або розкриття конфіденційної інформації. З огляду на це суди можуть розглянути можливість запровадження механізмів підвищення безпеки даних. Є способи запобігти таким порушенням в ІКТ (наприклад, через зниження ризику виникнення атаки) та/або пом'якшити їх наслідки (наприклад, через завчасне планування правильних дій у разі атаки). Дуже важливо, щоб держави-члени забезпечили належний рівень кібербезпеки систем ОВС та їх цілісність. Механізми ОВС потребують захисту від несанкціонованого використання системи зовнішніми сторонами й отримання закритої інформації. Мають існувати внутрішні обмеження щодо повноважень на доступ до інформаціїдля забезпечення того, щоб сторони спору не мали доступу до інформації, яку вони не мають права отримувати. Це вимагає надійної аутентифікації та контролю доступу.

62. У Додатку до цієї пояснювальної записки міститься контрольний перелік питань із кібербезпеки для держав-членів.

Керівний принцип 29

63. Важливо, щоб під час проєктування ОВС у систему було імплементовано систему безпеки. Безпеку необхідно гарантувати протягом усього строку роботи механізму ОВС за допомогою процесів проєктування й розроблення, які постійно удосконалюються для зниження ризику заподіяння шкоди через зловмисну експлуатацію. Існує два основних принципи, яких необхідно дотримуватися, — «безпека за проєктуванням» і «безпека за замовчуванням». Перший принцип означає, що всім, хто бере участь у проєктуванні й розробленні продуктів, послуг і процесів ІКТ, що сприяють ОВС, рекомендовано на початкових етапах проєктування та розроблення вживати заходів щодо максимально можливого захисту безпеки цих продуктів, послуг і процесів — так, щоб можна було передбачити кібератаки та мінімізувати їх наслідки. Принципу «безпека за проєктуванням» необхідно дотримуватися на найраніших етапах проєктування й розроблення для захисту безпеки ОВС. Принцип «безпека за замовчуванням» означає, що продукти, послуги та процеси ІКТ, що сприяють

ОВС, спроєктовано так, щоб забезпечити вищий рівень безпеки, який має дозволити першому користувачу отримати конфігурацію із максимально безпечними налаштуваннями за замовчуванням, а отже, зменшує навантаження на користувачів, яке пов'язане з необхідністю налаштовувати продукт, послугу або процес ІКТ.

64. Сертифікація відіграє важливу роль у підвищенні довіри й безпеки продуктів, послуг і процесів ІКТ, що сприяють ОВС. Вона передбачає комплексний набір правил, технічних вимог, стандартів і процедур. Щоб продемонструвати ризик кібербезпеки, сертифікати можуть бути трьох гарантованих рівнів (базовий, істотний, високий), які є співмірними з рівнем ризику, пов'язаного з передбачуваним використанням продукту, послуги або процесу з погляду ймовірності й наслідків інциденту. Для отримання певних рівнів сертифікації може знадобитися наявність національної правової системи, що дозволяє й регулює випробування та тестування на проникнення в (державні) системи ІКТ.

Захист прав людини, зокрема захист персональних даних

Керівний принцип 30

65. Уряди держав-членів, законодавці, суди, а також розробники, виробники й постачальники послуг ОВС мають постійно оцінювати можливі негативні наслідки застосування методів і механізмів ОВС для прав і основоположних свобод людини і з огляду на ці наслідки застосовувати попереджувальний підхід, що ґрунтується на відповідних заходах із запобігання та пом'якшення ризиків. На всіх етапах обробки, включно зі збиранням даних, їм варто застосовувати підхід «права людини за проєктуванням» і уникати потенційних упереджень, зокрема тих, які можуть бути ненавмисними або прихованими, і ризиків дискримінації або інших негативних наслідків для прав і основоположних свобод людини.

Керівний принцип 31

66. Необхідно забезпечити відповідність усієї обробки персональних даних із використанням механізмів ОВС із законодавством про захист даних. Ключовими елементами цього підходу є законність, чесність, визначення мети і пропорційність обробки даних. Важливими вимогами також є відповідальність за відповідність та дотримання вимог (підзвітність), прозорість, безпека даних і управління ризиками.

Керівний принцип 32

67. Захист персональних даних має бути пріоритетом і забезпечуватися належними ресурсами. Недостатній захист може ускладнити доступ до судів. Цей ризик варто збалансовувати навчанням працівників судів захисту персональних даних, чіткою політикою та керівними

принципами захисту даних, проведенням аудитів захисту даних і ефективним впровадженням їх результатів. Сучасні режими захисту даних [як-от оновлена Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (ETS № 108)] відіграють важливу роль у захисті прав і інтересів суб'єктів персональних даних. Державам-членам варто приділити особливу увагу Керівним принципам із питань штучного інтелекту й захисту даних, ухваленим у 2019 році Консультативним комітетом Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних (T-PD) Ради Європи.

68. «Технічні та організаційні заходи» у значенні цих керівних принципів — це функції, процеси, засоби контролю, системи, процедури та заходи, вжиті для захисту й забезпечення безпеки персональних даних, оброблюваних у межах системи ОВС. Ці заходи є вимогою для безпечної обробки, запобігання порушенням безпеки, забезпечення відповідних операторів, записів про діяльність з обробки, проєктування й міцної основи задля забезпечення захисту прав і свобод користувачів ОВС. Конкретні заходи передбачають, зокрема: i) захист від несанкціонованого доступу до конфіденційних даних, як-от персональні дані, конфіденційні ноу-хау й комерційна інформація або інші види потенційно чутливої інформації, зібраної в процесі ОВС; ii) забезпечення цілісності даних задля виключення можливості небажаної зміни або видалення даних, що стосуються електронних процесуальних документів, зокрема самого рішення чи доказів; iii) виявлення шахрайства з боку сторін, оскільки через онлайн-контекст судді може бути складніше встановити особу сторони.

Керівний принцип 33

69. Впровадження ОВС може становити загрозу для приватного життя осіб, тому під час такого впровадження варто враховувати аспекти етики та прав людини. Має існувати належний баланс між практичною цінністю відкритих даних і недоторканністю приватного життя суб'єктів персональних даних. Механізми ОВС варто проєктувати й розробляти відповідально, керуючись принципами «недоторканність приватного життя за замовчуванням» і «недоторканність приватного життя за проєктуванням». «Недоторканність приватного життя за замовчуванням» означає, що суд має забезпечити обробку персональних даних із максимальним захистом недоторканності приватного життя, а «недоторканність приватного життя за проєктуванням» означає, що на найраніших етапах проєктування ОВС необхідно впроваджувати технічні та організаційні заходи так, щоб із самого початку забезпечити захист принципів недоторканності приватного життя та захисту персональних даних.

Керівний принцип 34

70. Існує ризик того, що задля зниження вартості впровадження ОВС держави-члени вирішать передати платформи ОВС зовнішнім провайдерам в обмін на доступ до особистих даних користувачів. Також можливо, що ОВС експлуатуватимуть компанії, бізнес-модель яких ґрунтується на відстеженні даних. Дотримання вимоги недоторканності приватності вимагає, щоб комерційне відстеження, профілювання або таргетинг не були вбудовані в системи ОВС, оскільки така діяльність потенційно серйозно впливає на особисту свободу та автономію людей і може призвести до упередженості й дискримінації. Якщо всі або будь-яка частина механізмів ОВС передається зовнішнім провайдерам, із ними варто укладати ґрунтовний договір на обробку персональних даних, який гарантуватиме дотримання законодавства про захист персональних даних і реалізацію прав осіб на захист персональних даних.

Інші питання (що не випливають із практики Європейського суду з прав людини)

Тестування, моніторинг, модернізація, дослідження та розроблення

Керівний принцип 35

71. Для забезпечення вдосконалення технології державам-членам рекомендовано стимулювати прогрес у сфері ОВС шляхом розроблення й підтримання таких механізмів самостійно або через стимулювання неурядових та/або приватних проєктів і програм. Розроблення механізмів ОВС мають фінансувати (якщо це доцільно й можливо) державні органи задля зміцнення суспільної довіри до ОВС. Метою такого фінансування може бути створення середовища, сприятливого для розвитку ОВС відповідно до статей 6 і 13 Європейської конвенції з прав людини. Зміни у сфері кіберправосуддя мають відбуватися під впливом суду, а не технологій. Відповідні дослідження можуть заповнити прогалини в правових і технічних знаннях і поліпшити функціонування ОВС.

Керівний принцип 36

72. Метою тестування ОВС є оцінка його відповідності встановленим правовим, процесуальним і технічним вимогам. Наприклад, завдяки тестуванню ОВС можна перевірити, чи приводить кожен тип введення даних користувачем до бажаного результату. Тестування має ґрунтуватися на таких чинниках якості, як надійність, зручність використання, цілісність, безпека, функціональність, ефективність, мобільність, експлуатаційні якості та сумісність. Достатнє тестування та доопрацювання перед введенням у дію забезпечують ефективність

і прийнятну додану вартість. Тісна, постійна участь майбутніх користувачів допомагає звести до мінімуму будь-які розбіжності між потребами, викладеними на папері, і тим, як ІТ-фахівці вирішують їх на практиці, і дозволяє переорієнтувати запропоновані технічні рішення, якщо це можливо й не впливає на графік проєкту або його вартість. Випробування на пілотних об'єктах надає можливість отримати інформацію від перших користувачів, перш ніж затвердити наступний етап проєкту або розгорнути його в ширшому масштабі.

Керівний принцип 37

73. Для належного проєктування механізму ОВС необхідно налагодити конструктивний діалог між тими, хто розробляє технологію, і тими, хто відповідає за ухвалення судових рішень. Держави-члени мають самі вирішувати, яких зацікавлених сторін і якою мірою варто залучати, оскільки це залежить від типу конкретного ОВС. Деякі з них вимагають більших ресурсів від зацікавлених сторін, наприклад залучення компонентів ШІ, а деякі — менших. Судові органи повинні брати активну участь в етапах тестування та пілотування. У цьому контексті також важливо забезпечити, щоб проєктування ОВС не позбавляло суддів їхньої здатності ухвалювати рішення. Однак судді не єдині фахівці, яких можна залучити до проєктування. У діалозі можуть брати участь і інші зацікавлені сторони, як-от адвокати, працівники судів і користувачі суду. Розробники технології повинні прагнути краще зрозуміти систему правосуддя і співпрацювати із суддями і працівниками судів, щоб архітектура ІКТ відповідала потребам як судів, так і громадськості. Архітектура ОВС також має бути гнучкою й готовою до адаптації до судового прецедентного права або практики. Більше інформації див. у Керівних принципах щодо змін у напрямі кіберправосуддя (Аналіз використовуваних інструментів і короткий виклад кращої практики), ухвалених Європейською комісією з питань ефективності правосуддя 7 грудня 2016 року.

Керівний принцип 38

74. ОВС повинна залишатися на сучасному рівні надання послуг і технологічних інновацій. Кожен механізм ОВС проходить період експлуатації від початкового планування до припинення експлуатації. Механізм ОВС має циклічний характер, тобто він постійно вдосконалюється через зміни й модернізацію. Необхідно регулярно замінювати застаріле обладнання або програмне забезпечення, модернізувати системи безпеки й постійно вдосконалювати механізми. Кожна держава-член має визначити власну оптимальну практику для різних етапів розроблення ОВС.

Підвищення обізнаності, навчання та освіта

Керівний принцип 39

75. Підвищення обізнаності, навчання та освіта фізичних і юридичних осіб є ключовим чинником для успішного застосування методів і механізмів ОВС і забезпечення його розроблення та використання. Необхідно вживати заходів щодо вдосконалення низки цифрових навичок (від базових до розвинених) різних соціально-економічних груп. До них належать цифрові навички для літніх людей та інших цільових груп, як-от особи з інвалідністю. Державні органи як основні постачальники судових послуг та механізмів ОВС також потребують відповідних знань і навичок. Зокрема, вони мають бути компетентними в питаннях розроблення механізмів ОВС з огляду на потреби громад та бізнесу та вимоги Європейської конвенції з прав людини задля створення і зміцнення суспільної довіри до ОВС.

Рекомендація Rec(2004)4 **Комітету міністрів державам-членам про роль Європейської конвенції з прав людини в університетській освіті та професійній підготовці**

Комітет міністрів рекомендує державам-членам, зокрема, пересвідчитися в тому, що «в рамках університетської освіти і професійної підготовки на національному рівні проводиться вивчення Конвенції з прав людини та прецедентної практики Суду і що така освіта й підготовка включені, зокрема <...> як елемент підготовчих програм при складанні іспитів на місцевому або загальнодержавному рівнях для отримання різноманітних правничих спеціальностей, а також первісної підготовки і підвищення кваліфікації суддів, прокурорів та адвокатів».

У межах дослідження щодо Рекомендації Rec(2004)4 Редакційна група III Комітету експертів із Європейської конвенції з прав людини (DH-SYSC) заявила, зокрема, що держави-члени мають суттєво підвищити ефективність такої університетської освіти і професійної підготовки через надання кожній категорії населення необхідних інструментів для виконання зобов'язань, що випливають із Європейської конвенції з прав людини. З цією метою держави-члени мають забезпечити якісну адресну й доступну професійну підготовку. До того ж, наскільки це можливо, професійну підготовку мають проводити особи, які добре знають систему Європейської конвенції з прав людини та мають практичний досвід у відповідній професійній галузі [див. документ DH-SYSC-III(2019)01 Rev, пп. 2 і 5].

Керівний принцип 40

76. Державам-членам необхідно забезпечити, щоб механізми ОВС були орієнтовані на користувача, були доступними, чесними, прозорими, підзвітними та економічно доцільними. Судді, адвокати та всі учасники судових розглядів мають знати, що використання ОВС потенційно може привести до більшої автоматизації, більшої швидкості

обробки інформації, підвищення ефективності та зменшення витрат на вирішення спорів. Тобто ОВС надає можливість вирішити більшу кількість спорів, що, зрештою, приведе до розширення доступу до вирішення спорів та економії коштів. ОВС також здатне докорінно змінити доступ до правосуддя, наприклад, для осіб, яким важко потрапити в суди. Для поширення таких подробиць про можливості ОВС серед усіх зацікавлених фахівців можна використовувати методи онлайн-навчання.

Керівний принцип 41

77. Судді та юристи, а також працівники судів повинні мати доступ до міждисциплінарної підготовки з питань функціонування ОВС. Фахівці з вирішення спорів повинні мати достатньо навичок і підготовки для виконання своїх обов'язків. Фахівець, що знається на цифрових технологіях, має бути обізнаний із технологічними досягненнями і, зокрема, розробками у галузі інформаційної безпеки. Експерти зазвичай підкреслюють необхідність належних засобів захисту й контролю, а також важливість проведення для всіх працівників судів тренінгів із питань IT-безпеки під час онлайн-комунікацій. Держави-члени мають вжити заходів для забезпечення того, щоб судді, юристи та працівники судів мали можливість звертатися до експертів у галузі права та IT за консультаціями, коли під час надання послуг з ОВС необхідні спеціальні знання щодо тлумачення та застосування законів і нормативних актів. Підготовка з питань ОВС може охоплювати конкретні проблеми, що виникають під час його застосування, як-от кібербезпека. Важливо знати про ширший цифровий контекст і використовувати новітні технології, як-от хмарні обчислення, трастові послуги або блокчейн.

Керівний принцип 42

78. Судді повинні вміти використовувати механізми ОВС і дотримуватися належної практики в роботі з ОВС. Така практика враховує, наприклад, ризик того, що деяким особам (з інвалідністю або психічними розладами, соціально незахищеним або літнім людям) буде складно отримати доступ до правосуддя. Задля уникнення цього суддів закликають консультуватися з адвокатами, які зазвичай працюють із незахищеними або маргіналізованими верствами населення. Ще один ризик полягає в тому, що відмова від свободи розсуду і людського міркування може призвести до упередження і стереотипів. Судді також можуть запобігти цьому ризику під час перегляду справи (див. пункти 52–53 вище). Судді мають бути обізнані про ризики, пов'язані з даними, питаннями безпеки й недоторканності приватного життя, та усвідомлювати їх.

Керівний принцип 43

79. У навчальних закладах юридичного напряму рекомендовано у разі потреби змінити методи навчання і створити основу для формування навичок юриста, який розуміється на цифрових технологіях, щоб навчити студентів використовувати технології для надання юридичних послуг. Належна практика передбачає нові моделі навчання, як-от підвищення рівня онлайн-навчання, впровадженого під час пандемії. Юридична освіта і професія можуть дотримуватися такої практики, щоб іти в ногу з технологічним прогресом, зокрема впровадженням механізмів ОВС у системи правосуддя. Важливо, щоб студенти не забували про законодавство, яке регулює права людини. Студенти також мають знати, що наразі суди використовують штучний інтелект для поліпшення своєї практики. У цьому контексті рекомендовано надавати студентам можливість вивчити не лише чинне становище юридичної практики, а й напрям її розвитку. Для того щоб вважати людину обізнаною у галузі цифрових технологій, вона повинна мати широке коло компетенцій. Викладачі можуть використовувати реальні приклади.

ДОДАТОК

КОНТРОЛЬНИЙ СПИСОК ПИТАНЬ ІЗ КІБЕРБЕЗПЕКИ ДЛЯ ДЕРЖАВ-ЧЛЕНІВ

Під час проєктування ОВС держави-члени мають ураховувати таке:

1. **Захист даних, що зберігаються, передаються або обробляються іншим способом**:
   a. від випадкового або несанкціонованого зберігання, обробки, доступу або розкриття впродовж усього періоду експлуатації продукту, послуги або процесу ІКТ, що сприяє ОВС.
   b. від випадкового або несанкціонованого знищення, втрати, зміни або браку доступу впродовж усього періоду експлуатації продукту, послуги або процесу ІКТ, що сприяє ОВС.
2. **Управління доступом користувачів за допомогою безпечної ідентифікації й аутентифікації:** уповноважені особи, програми або машини повинні мати можливість доступу тільки до тих даних, послуг або функцій, право доступу до яких вони мають.
3. **Виявлення та документування відомих залежностей і вразливостей:**
   ⇨ Сучасні продукти й системи ІКТ часто використовуються і ґрунтуються на одній або кількох технологіях і компонентах третіх сторін, як-от програмні модулі, бібліотеки або інтерфейси прикладного програмування. Таке використання, яке називають «залежність», може створювати додаткові ризики кібербезпеки, оскільки

вразливості, виявлені в компонентах третіх сторін, можуть також вплинути на безпеку продуктів, послуг і процесів ІКТ, що сприяють ОВС. У багатьох випадках виявлення й документування таких залежностей дозволяє кінцевим користувачам продуктів, послуг і процесів ІКТ поліпшити свою діяльність з управління ризиками кібербезпеки, наприклад, через удосконалення процедур управління та усунення вразливостей кібербезпеки користувачів.

⇨ До того ж таких залежностей і вразливостей певною мірою можна уникнути, надавши, наскільки це можливо, необхідні ресурси для власного проєктування й розроблення.

4. **Протоколювання доступу до даних, їх використання та обробки:** задля документування того, до яких даних, послуг або функцій було отримано доступ, використано або оброблено в інший спосіб, коли і ким.

5. **Дозвіл на ознайомлення з файлами журналу:** задля перевірки, до яких даних, послуг або функцій було отримано доступ, використано або оброблено в інший спосіб, коли і ким.

6. **Тестування вразливості:** перевірка того, що продукти, послуги та процеси ІКТ, що сприяють ОВС, не містять відомих вразливостей.

   ⇨ Задля перевірки вразливості може знадобитися національна правова система, що дозволяє й регулює тестування та тестування на проникнення до (державних) систем ІКТ.

7. **Забезпечення резервного обладнання та технічної підтримки:** задля своєчасного відновлення доступу до даних, послуг і функцій у разі фізичного або технічного інциденту.

8. **Безпека за проєктуванням і за замовчуванням:** задля безпеки продуктів, послуг та процесів ІКТ, що сприяють ОВС, за проєктуванням і за замовчуванням.

9. **Оновлення апаратного і програмного забезпечення:** задля оснащення продуктів, послуг та процесів ІКТ, що сприяють ОВС, сучасним програмним і апаратним забезпеченням, що не містить загальновідомих вразливостей, а також механізмами безпечного оновлення.

Для максимального зменшення ризиків кібербезпеки й підвищення довіри можна запросити сертифікацію кібербезпеки продуктів, послуг і процесів ІКТ, що сприяють ОВС. Наприклад, для країн ЄС сертифікацію можна запросити в межах Регламенту Європейського парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій, а також про скасування Регламенту (ЄС) № 526/2013 (Акт про кібербезпеку).

ПОКАЖЧИК

1. Керівні принципи Комітету міністрів Ради Європи щодо електронних доказів у цивільному та адміністративному судочинстві (ухвалені Комітетом міністрів 30 січня 2019 року на 1335-му засіданні заступників міністрів), CM(2018)169-add1final.

2. Онлайн вирішення спорів і дотримання права на справедливий судовий розгляд і права на ефективний засіб правового захисту (статті 6 і 13 Європейської конвенції з прав людини). Спеціальне дослідження механізмів онлайн вирішення спорів. Підготовлено професором Джулією Хьорнле, Центр вивчення комерційного права, Лондонський університет королеви Марії, Метью Хьюітсоном (Південна Африка) та Іллею Черногоренко (Україна), Страсбург, 1 серпня 2018 року, CDCJ(2018)5.

3. Посібник зі статті 6 Європейської конвенції з прав людини, Право на справедливий суд (цивільна частина), оновлено 31 серпня 2019 року, Рада Європи/ Європейський суд з прав людини, 2019 рік.

4. Дослідження наслідків передових цифрових технологій (зокрема систем ШІ) для поняття відповідальності в межах прав людини. Підготовлено Експертним комітетом із правозахисних аспектів автоматизованої обробки даних і різних форм штучного інтелекту (MSI-AUT). Доповідач: Карен Юнг, DGI(2019)05.

5. Керівні принципи з питань штучного інтелекту та захисту даних, T-PD(2019)01.

6. Європейська етична хартія щодо використання штучного інтелекту в судових системах та їх оточенні, Рада Європи, Комісія з питань ефективності правосуддя (CEPEJ), 3–4 грудня 2018 року.

7. «Європейські судові системи, ефективність і якість правосуддя: використання інформаційних технологій у європейських судах», Дослідження CEPEJ № XX, видання 2016 року (дані за 2014 рік).

8. Консультативна рада європейських суддів (КРЄС), Висновок № 14 (2011), «Правосуддя та інформаційні технології (ІТ)».

9. Редакційна група Комітету експертів із Європейської конвенції з прав людини (DH-SYSC), Редакційна група III щодо пропозицій до Рекомендації Rec(2004)4, Передова національна практика, що ілюструє принципи, викладені в Додатку I до переглянутої Рекомендації Rec(2004)4 [документ DH-SYSC-III(2019)01 Rev], 2019.

10. Велика хартія суддів, Рада Європи, Консультативна рада європейських суддів (КРЄС), 2010 р.

11. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (ETS № 108); див. http://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 [станом на 20 листопада 2020 року].

12. Парламентська асамблея Ради Європи, Резолюція 2054 (2015), «Доступ до правосуддя та Інтернет: потенціал і виклики», Доповідь: док. 13918 від 10 листопада 2015 року.

13. Регламент Європейського парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій, а також про скасування Регламенту (ЄС) № 526/2013 (Акт про кібербезпеку) (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&from=EN) [станом на 20 листопада 2020 року].

14. Рекомендація Ради ОЕСР щодо штучного інтелекту, OECD/LEGAL/0449, ухвалена 22 травня 2019 року, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 [станом на 20 листопада 2020 року].

15. Група експертів високого рівня Європейської комісії з питань штучного інтелекту, «Визначення ШІ: основні можливості та наукові дисципліни». Визначення, розроблене для цілей звіту за результатами роботи Групи експертів високого рівня з питань ШІ, Брюссель, 18 грудня 2018 року; https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai [станом на 20 листопада 2020 року].

16. Байром Н. Цифрове правосуддя: стратегія даних Служби судів і трибуналів Її Величності та забезпечення доступу до правосуддя. Звіт і рекомендації, Фонд юридичної освіти, жовтень 2019 року.

17. Хьорнл Дж. Транскордонне онлайн вирішення спорів, «Кембрідж Юніверсіті Прес», 2009 р.

18. Хьорнл Дж. Заохочення альтернативного онлайн вирішення спорів (ABC) в ЄС і за його межами, журнал «European Law Review», 2013 р., том 38 (2), стор. 187–208.

19. Технічні коментарі ЮНСІТРАЛ щодо онлайн вирішення спорів, Нью-Йорк, 2017 р.

20. Стандарти практики онлайн вирішення спорів, розроблені Інтернет-корпорацією з присвоєння імен та номерів, режим доступу: https://www.icann.org/en/system/files/files/odr-standards-of-practice-en.pdf [станом на 20 листопада 2020 року].

21. Робоча група III ЮНСІТРАЛ (Онлайн вирішення спорів); Тридцять третя сесія, Нью-Йорк, 2016 р., Онлайн вирішення спорів під час транскордонних електронних комерційних операцій, A/CN.9/WG.III/WP.140, https://undocs.org/en/A/CN.9/WG.III/WP.140 [станом на 20 листопада 2020 року].

22. Рейні Б. et al., Якобс Вайт та Ові. Європейська конвенція з прав людини, «Оксфорд Юніверсіті Прес», 2014 р.

23. Карнейро Д. et al. ОВС: перспектива штучного інтелекту, журнал «Artificial Intelligence Review», 2014 р., том 41, стор. 211–240.

24. Альтреас Н. et al. Прогнозування судових рішень Європейського суду з прав людини: перспектива обробки з використанням природної мови, журнал «Peer J Computer Science» (опубліковано 24 жовтня 2016 року) https://peerj.com/articles/cs-93.pdf [станом на 20 листопада 2020 року].

25. Лоутоцький П. Онлайн вирішення спорів і новітні розробки типового закону ЮНСІТРАЛ, Кофола Інтернешнл 2015: актуальні проблеми врегулювання міжнародних (транскордонних) спорів: матеріали конференції (ред. К. Дрлічкова), Брно, 2015 р., стор. 243–256.

26. Шерер М. Штучний інтелект і прийняття правових рішень: широкий простір, Журнал міжнародного арбітражу, 2019 р., том 36, № 5, стор. 539–574.

27. Ханріот М. Онлайн вирішення спорів (ОВС) як рішення транскордонних споживчих спорів: забезпечення виконання рішень, журнал вирішення спорів «McGill», 2015 р., том 2, стор. 1–22.

28. Узелац А., ван Рі К. Х. Трансформація цивільного правосуддя, Ius Gentium: порівняльні перспективи права і правосуддя, «Спрінгер Інтернешнл Паблішінг» 2018 р.

29. Віткаускас Д. та Діков Г. Захист права на справедливий суд відповідно до Європейської конвенції з прав людини: посібник для практикуючих юристів, Рада Європи, 2017 р. Режим доступу: https://rm.coe.int/protecting-the-right-to-a-fair-trial-under-the-european-convention-on-/168075a4dd [станом на 20 листопада 2020 року].

COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES

1949.2019

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

MINISTERS' DEPUTIES CM Documents **CM(2021)36add4-final** 16 June 2021

1407th meeting, 16 June 2021

10 Legal questions

10.1 European Committee on Legal Co-operation (CDCJ)

Guidelines of the Committee of Ministers of the Council of Europe on online dispute resolution mechanisms in civil and administrative court proceedings

Preamble

The Committee of Ministers,

Considering that the aim of the Council of Europe is to achieve a greater unity between the member States, in particular by promoting the adoption of common rules in legal matters;

Considering the necessity to provide practical guidance for policy makers responsible for designing online dispute resolution (ODR) mechanisms in the member States, with a view to ensuring that such mechanisms are compatible with Articles 6 and 13 of the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5, the "European Convention on Human Rights");

Considering that these guidelines should aim at establishing a common framework and not at harmonising the national legislations of the member States;

Considering the need to respect the diversity of the legal systems of the member States;

Acknowledging the progress made by the member States in introducing online dispute resolution mechanisms in their legal systems;

Noting that developers of online dispute resolution mechanisms (whether public or private) may not be sufficiently aware that such mechanisms should be accompanied by robust human rights safeguards;

Highlighting the need for member States to ensure that such mechanisms are compatible with the key principles of a fair trial and effective remedy set out in the case law of the European Court of Human Rights, including the principles of oral hearing and equality of arms,

Adopts the following guidelines to serve as a practical tool for the member States, to assist them in adapting the operation of their online dispute resolution mechanisms to the provisions of Articles 6 and 13 of the European Convention on Human Rights and the principles developed thereto in the case law of the European Court of Human Rights, and invites the member States to disseminate these guidelines widely with a view to their implementation by those responsible for designing and implementing online dispute resolution mechanisms.

Purpose and scope

The guidelines apply to online dispute resolution (ODR) mechanisms used by courts. They provide guidance in relation to fair procedure, transparency in the use of ODR and requirements for hearings, special issues related to the ICT nature of ODR techniques and other issues not stemming from the jurisprudence of the European Court of Human Rights. They do not cover internal management of electronic case files by the courts or alternative dispute resolution (ADR) mechanisms, such as mediation and conciliation. However, member States may wish to extend their application to ADR if and where appropriate.

Definitions

For the purpose of these guidelines, the terms below have the meanings indicated:

i. Court

"Court" refers to a body within the concept of a "tribunal" under Article 6 of the European Convention on Human Rights, that is a body which:

- is established by law;
- is governed by a procedure prescribed by law;
- determines matters within its competence by issuing binding decisions;
- has full jurisdiction over the case;
- is independent and impartial.

ii. Online dispute resolution (ODR)

"Online dispute resolution (ODR)" refers to any online information technology (IT) used by a court to resolve or assist in resolving a dispute.

iii. Artificial intelligence (AI)

"Artificial intelligence (AI)" refers to a set of scientific methods, theories and techniques the aim of which is to reproduce, by a machine, the cognitive abilities of a human being.

iv. Information and communication technology (ICT)

"Information and communication technology (ICT)" refers to technology that provides access to information through telecommunications.

Fundamental principles

1. Member States should seek to ensure trust and confidence in ODR.
2. ODR should not create substantial barriers for access to justice.
3. Procedural rules which apply to court proceedings in general should also apply to court proceedings involving ODR, unless the specific nature of a particular ODR mechanism requires otherwise.
4. Parties to proceedings involving the use of ODR should be identified using secure mechanisms.

The guidelines

Fair procedure

Access to justice

1. ODR should be easily understood, affordable and user friendly so that it can be used comfortably by as many people as possible.
2. Parties should be informed about how ODR operates, how to file an application, how to monitor progress of the proceedings and how to access decisions.
3. Use of ODR should not be disadvantageous to the parties or give unfair advantage to one of the parties.
4. ODR should be designed and implemented in accordance with internationally recognised technical standards, in order to allow its use by as many people as possible with as much autonomy as possible.
5. The cost of court proceedings involving ODR should not be higher than those not involving an ODR element.

6. Parties should be notified when it is intended that their case will be processed with the involvement of an AI mechanism.

Equality of arms

7. Participation in ODR proceedings should not prejudice an individual's right to participate effectively in the proceedings or their right to an effective remedy.
8. ODR proceedings should ensure an independent and impartial adjudicative process.
9. Parties to proceedings involving ODR should have knowledge of the materials in the case file, including those submitted by the other parties; they should have access to these materials and sufficient time and means to acquaint themselves with their contents.

Evidence

10. Fairness requires that parties to proceedings involving ODR should be permitted to present evidence in a manner that does not place them at a disadvantage vis-à-vis other parties.
11. Parties should have the opportunity to present their case and to contest evidence submitted by other parties.
12. ODR should respect the principles of legal certainty and protection of the legitimate expectations of the parties.

Effective proceedings

13. Implementation of ODR should aim to improve the effectiveness of the proceedings by allowing parties to participate without being physically present in court and by streamlining the whole process as far as possible.
14. Technical difficulties in the functioning of ODR should not prevent the courts, even for short periods, from examining cases and performing appropriate procedural steps.
15. Where national law provides that ADR constitutes a prerequisite for instituting court proceedings, including those involving ODR, this should not protract the dispute resolution process unnecessarily or result in a substantial increase in costs for the parties.

Delivery of the decision

16. The outcomes of the proceedings involving ODR should be transparent.
17. Any final decision reached using ODR should be made public in accordance with the jurisprudence of the European Court of Human Rights.

Right to a reasoned decision

18. Sufficient reasons should be given for decisions reached using ODR or with the assistance of ODR, in particular the decisions reached with the involvement of AI mechanisms.

Enforcement of the decision

19. The mere fact that the decision is a result of an ODR mechanism should not prevent it from being enforceable.

Right to judicial review in cases involving purely automated decisions

20. Where national law allows for purely automated decisions, such decisions should be open to review before a judge.

Transparency in the use of ODR and requirements for hearings

Transparency in the design and operation of ODR mechanisms

21. The design and operation of ODR mechanisms should be made transparent and explained in an intelligible manner using clear and plain language.

Public and oral hearings

22. The use of ODR mechanisms should guarantee appropriate ways to ensure public scrutiny of proceedings.

23. The use of ODR in courts should not in itself deprive parties of a right to request an oral hearing before at least one level of jurisdiction.

Other issues of transparency, including public scrutiny

24. Parties to proceedings involving ODR should be informed about any potential conflicts of interest related to the operation of an ODR mechanism.

25. ODR should be designed in such a way that all documents generated, including the final judgment and other decisions or notifications, are written in clear and plain language.

26. Procedural rules applicable to ODR should be transparent.

27. Parties to proceedings involving ODR should be aware of and have the ability to access information concerning the procedural rules applicable to ODR.

Special issues related to the ICT nature of ODR techniques

Cybersecurity

28. An appropriate level of cybersecurity of ICT products, services and processes facilitating ODR should be ensured in order to meet the requirements in Articles 6 and 13 of the European Convention on Human Rights and to ensure the necessary trust and confidence in ODR mechanisms.

29. The level of cybersecurity of ICT products, services and processes facilitating ODR should be considered appropriate when safeguards are provided against:

    – unauthorised access to confidential data;

    – the unwanted alteration or deletion of data;

    – the technical impossibility to access the system and the data contained therein for those who should have access;

    – uncertainty over the identity of the judge and other professionals involved in ODR proceedings;

    – identity fraud by parties.

Human rights protection, including personal data protection

30. Member States should assess the impact of ODR use, throughout its entire life cycle, on individuals and social groups, and identify the specific requirements for ethical and fair use of ODR and respect for human rights as part of the development and operation of any ODR mechanism.

31. The use of ODR mechanisms should not infringe data protection rights, including, where applicable, the right to information, the right to access data, the right to object to processing data and the right to erasure.

32. Technical and organisational measures should be implemented to ensure that rules on personal data protection are respected, both when determining the means of processing and during data processing.

33. ODR mechanisms should be designed and developed by applying the principles of personal data protection by default and by design, in particular by:

    – implementing technical and organisational measures to ensure that personal data are protected by the application of, in particular, anonymisation or pseudonymisation techniques;

    – introducing access and reuse restrictions by the competent authorities who maintain control of the data.

34. Outsourcing the technology used in ODR should not lead to processing of personal data for commercial purposes.

Other issues (not stemming from the jurisprudence of the European Court of Human Rights)

Testing, monitoring, upgrading, research and development

35. Member States are encouraged to allocate appropriate public funding for the development of ODR mechanisms to be used in court proceedings, including relevant research.
36. The ease of use of ODR mechanisms should be sufficiently tested before implementing the latter.
37. The judiciary, lawyers and other relevant stakeholders should be actively involved in designing ODR mechanisms.
38. Continuous monitoring and timely upgrading of ODR mechanisms, ensuring safety, fairness, efficiency and other quality standards, should be included into the life cycle of all such systems.

Awareness raising, training and education

39. Member States should encourage individuals and legal entities to use ODR mechanisms, in particular by informing them about the existence of such an option, its reliability and its compatibility with the requirements of the European Convention on Human Rights.
40. Judges, legal practitioners and all those involved in court proceedings should be made aware of the benefits and value of ODR mechanisms and their compliance with the European Convention on Human Rights as well as with other relevant laws.
41. Judges and legal practitioners as well as court staff should have access to appropriate training on ODR, delivered by legal and IT professionals. The training should be as practical as possible and tailored to the needs of specific target groups.
42. As ODR mechanisms should not compromise parties' procedural rights, judges should be able to identify risks that might result from using ICT and to eliminate such risks.
43. Legal education should include modules on the use of ICT tools in courts.

COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

MINISTERS' DEPUTIES	CM Documents	CM(2021)36-add5-final	16 June 2021

1407th meeting, 16 June 2021

10 Legal questions

10.1 European Committee on Legal Co-operation (CDCJ)

Guidelines of the Committee of Ministers of the Council of Europe on online dispute resolution mechanisms in civil and administrative court proceedings — Explanatory Memorandum

CONTENTS

GENERAL COMMENTS

Why a new instrument?

1. Online dispute resolution (ODR) techniques and mechanisms play an increasingly important role in dispute resolution in the Council of Europe member States. ODR has the ability to improve access to justice by facilitating faster and less costly access to courts, thereby making dispute resolution more effective and efficient.

2. However, wide use of ODR also has the potential to restrict access to justice by setting up technological barriers to all those who do not have the capacity to use technology. Moreover, attention needs to be given to issues of authentication and identification of the parties, digital divide, cybersecurity and personal data protection.

3. To ensure that disputes are resolved fairly, there is a need to develop appropriate and adequate guidelines on human rights protection in the use of ODR. Within the member States of the Council of Europe, this requirement also follows from the guarantees enshrined in the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5 the "European Convention on Human Rights"), especially the judicial guarantees contained in Articles 6 and 13. To date, there are few such standards at international, European, and at national levels. These guidelines aim to recommend standards to shape law and practice and fill existing gaps.

4. These guidelines suggest a set of baseline measures that member States' governments, legislators, courts as well as ODR developers, manufacturers and service providers should follow in order to ensure that ODR do not undermine human dignity, human rights and fundamental freedoms.

5. The purpose of these guidelines is not to establish binding legal standards but rather to serve as a practical tool for member States to ensure that their ODR techniques and mechanisms comply with the requirements of Articles 6 and 13 of the European Convention on Human Rights and the principles developed in the jurisprudence of the European Court of Human Rights in respect of those articles. The guidelines do not impose any obligation on member States to introduce ODR into their national law or to enlarge the use of ODR.

Working method and the drafting process

6. The issue of ODR falls within the competence of the European Committee on Legal Co-operation (CDCJ) which is the Council of Europe's intergovernmental body responsible for standard-setting activities in the field of civil and administrative law.

7. In 2016 a study was undertaken on the feasibility for the CDCJ to undertake an activity on ODR mechanisms with reference to Articles 6 and 13 of the European Convention on Human Rights.

8. As a follow-up to this, the CDCJ decided to start, in 2017, work on the preparation of a technical study as a first step of the activity. This technical study has been completed and presented to the CDCJ at its 93rd plenary meeting (14–16 November 2018).

9. The activity was continued with the preparation of these guidelines aiming at ensuring the compatibility of ODR mechanisms with Articles 6 and 13 of the European Convention on Human Rights. The guidelines are based on the proposals made by CDCJ members and were prepared at the meetings held in 2019 and 2020. The drafting group took into consideration experience arising from the operation of ODR mechanisms in place in member States.

National examples:

- In **Lithuania** online filing, online payment of court fees and digital cases materials with online access are available in all civil and administrative cases using the centralised e-justice system LITEKO; courts normally issue digital official documents (orders, decisions, judgments, rulings, notifications, summons, etc.) authenticated by qualified electronic signatures and having the same legal value as analogous paper documents; in 2019 about 74 percent of court case files in civil and administrative matters were digital, other files were mixed (digital and physical/paper); property sale auctions in enforcement proceedings are held only electronically; videoconferencing can be used in civil and administrative procedures as almost each court is equipped with at least one set of video-conference equipment or may use mobile video conferencing equipment and every court room is equipped with equipment for digital audio recording. As a response to Covid-19 outbreak all judges of the Lithuanian courts were provided with the possibility to work from their homes with remote access to justice system LITEKO. Steps were taken to start more active use of video and teleconferencing with widespread private tools (such as videoconferencing) for conversion of oral hearings into virtual digital meetings. Additional cybersecurity measures were implemented to ensure safety and stability of the e-justice system.
- In **France**, it is possible to initiate administrative and commercial proceedings online on dedicated portals and to submit court documents in an electronic way. It is possible to use videoconferencing in civil proceedings.
- In **Greece,** all procedural acts (i.e. claim, appeal, remedy etc.) and the documents that support them (written statements with attached files as evidence) can be filed electronically by the lawyers with the use of a qualified electronic signature. Videoconference during the main proceedings is also permitted.

- **Ireland** has an online court platform for certain small claims. As well as this, the following services are also available: an online eLicensing system to process licensing applications including alcohol related licences and gaming and lottery applications etc., the Legal Costs Adjudication system which allows claims to be made online, the Court Fines Online system which allows for electronic payment of fines imposed by the District Court, and the Supreme Court online system which allows for application for leave to appeal to the Supreme Court to be made online. Additional measures have also been introduced to provide for remote hearings in civil proceedings, the electronic submission of documents to courts in advance of proceedings known as «eFiling», the remote submission of «Statements of Truth» as an alternative to sworn affidavits, and for bodies conducting hearings or appeals to do so via remote means.
- In **Poland** the procedure for payment orders is fully electronic. The claim is submitted through an individual account created on a dedicated IT platform. All acts and documents are available online.
- In **Portugal** eviction proceedings, meant to enforce the termination of lease contracts, can be initiated over an online platform ("Balcão Nacional de Arrendamento"). Citius is an e-platform used by courts. Legal representatives can use it to submit their procedural documents and notifications. Also in administrative and tax jurisdictions, via SITAF online system, legal representatives can submit their procedural documents, be notified and consult their cases electronically. Both systems (Citius and SITAF) also support the activities of magistrates and public prosecutors. Parties to the proceedings have online access to documents relating to their cases. Certificates concerning court proceedings can also be obtained electronically. All national courts are equipped with at least one video conference room and all courtrooms have audio recording systems.
- **Belgium** introduced the Central Solvency Register ("RegSol"), a digital platform enabling creditors, authorised agents and interested parties to commence, access or follow up pending insolvency files administered by the Business court.
- **The United Kingdom** introduced: 1) a MONEYCLAIMS platform online and 2) an ODR platform to resolve cases resulting from airline passengers.
- In **Hungary** artificial intelligence is used in the online anonymous judgment database (searchable records).
- **Turkey** has implemented the National Judiciary Informatics System called "UYAP", enabling courts and individuals to carry out procedural acts online.

10. The present guidelines take full account of the Committee of Ministers 2019 Guidelines on electronic evidence in civil and administrative proceedings (hereinafter the "guidelines on electronic evidence").

Structure and content

11. The present guidelines largely follow the structure of principles developed in the jurisprudence of the European Court of Human Rights under Article 6 of the European Convention on Human Rights as helpfully compiled in the Court's "Guide on Article 6 of the European Convention on Human Rights — Right to a fair trial (civil limb)".

12. While in these guidelines the conditional "should" is frequently used, where the relevant principles are taken from the European Convention on Human Rights and case-law of the European Court of Human Rights the use of the conditional "should" must not be understood as reducing the legal effect of the European Convention on Human Rights.

PREAMBLE

13. The present guidelines apply to ODR used in court proceedings concerning civil (including commercial) and administrative disputes, be it a compulsory or voluntary instrument (for the definition of "court", see paragraph 18 below). The diversity of legal systems of member States is fully acknowledged and the guidelines are intended to be general enough to accommodate all the different legal systems. In particular, the guidelines do not provide any recommendations to member States as to whether they should introduce ODR techniques and mechanisms in their judicial systems. On the other hand, the guidelines are not only a declaration of principles but aspire to give practical advice and guidance.

PURPOSE AND SCOPE

14. The present guidelines address, in particular, the key principles of a fair trial and effective remedy as interpreted by the European Court of Human Rights in its case-law, for example, the principle of equality of arms.

15. The guidelines aim to assist member States in ensuring that ODR techniques and mechanisms are compatible with Articles 6 and 13 of the European Convention on Human Rights without compromising the benefits which ODR can bring, in particular, in so far as the costs of dispute resolution are concerned. In this context, it should be reiterated that the provisions of the European Convention on Human Rights must be interpreted in the light of present-day conditions, while taking into account the prevalent economic and social conditions (*Marckx v. Belgium*, 13 June 1 979, §41, Series A no. 31; *Tyrer v. the United Kingdom*, 25 April 1978, §31, Series A no. 26).

Key provisions of the European Convention on Human Rights

Case-law of the Court on Article 6(1) provides: "In the determination of his civil rights and obligations (…) everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice."

Case-law of the Court on Article 13 provides: "Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."

The guidelines deal with:

- fair procedure;
- transparency in the use of ODR and requirements for hearings;
- special issues related to the ICT nature of ODR techniques;
- other issues (not stemming from the jurisprudence of the European Court of Human Rights).

16. There is a widespread confusion regarding the use of the term "ODR". It is frequently understood as the electronic variant of the alternative dispute resolution (ADR), typically organised outside the court. An example is the European Union Online Dispute Resolution Platform. However, these guidelines concern use of new technologies in existing in-court proceedings. The reason for this is the focus of these guidelines: they deal with the question of how the guarantees referring to court procedures contained in Articles 6 and 13 of the European Convention on Human Rights can be secured when electronic mechanisms for resolving disputes are being used, in other words what legal and technical conditions these mechanisms must fulfil in order to meet the requirements stemming from Articles 6 and 13 of the European Convention on Human rights. Out-of-court and non-court-related dispute resolution, i.e. "alternative dispute resolution (ADR) mechanisms, do not fall under Articles 6 and 13 and therefore are intentionally excluded from the scope of these guidelines. However, member States may decide to extend the implementation of these guidelines to ADR, such as arbitration or mediation, accordingly if and where appropriate. While doing so, member States should be aware that the guidelines were drafted and aligned to existing in-court proceedings. This means that not all of the particular guidelines can be

directly applied and may need to be further adjusted by member States to be used *mutatis mutandis* within specific ADR mechanisms.

17. The guidelines do not apply to internal management of electronic case files by the courts. This includes, for example, the algorithm for allocation of cases among the judges.

DEFINITIONS

Court

18. A broad definition of "court" is included in order to cover all authorities with competences to adjudicate legal disputes using ODR in civil and administrative proceedings. Direct reference is made to the concept of a "tribunal" in the meaning of Article 6 of the European Convention on Human Rights in order to align the scope of these guidelines with the scope of Article 6. In its judgments the European Court of Human Rights set out the criteria for the court to be recognised as tribunal in the meaning of Article 6 of the European Convention on Human Rights and those criteria are fully reflected in the guidelines. The guidelines cover proceedings before bodies entrusted with decision making functions and only those proceedings which are of a judicial nature. This delimitation is important because other activities carried out by such bodies may be of non-judicial nature. These guidelines do not apply to non-contentious and unilateral procedures which do not involve opposing parties and which are available where there is no dispute over rights (*Alaverdyan v. Armenia*, application no. 4523/04, decision on admissibility of 24 August 2010, § 35; *Cyprus v. Turkey* [GC], no. 25781/94, ECHR 2001-IV).

Online dispute resolution (ODR)

19. The term "online dispute resolution (ODR)" first appeared in the late 1990s and has developed over two decades in line with the expansion of the Internet and, particularly, online shopping and other transactions. Initially, the concept was associated only with alternative dispute resolution (ADR) mechanisms that used electronic communications, which is especially convenient in cases where the parties are located far away from each other. ODR was and is still widely used as a synonym of electronic alternative dispute resolution (eADR). For example, Regulation No 524/2013 of the European Parliament And of the Council, of 21 May 2013, limits its scope to the "out-of-court resolution of disputes concerning contractual obligations stemming from online sales or service contracts between a consumer resident in the Union and a trader established in the Union". However, it should be noted that over the years the meaning of the term "ODR" has been extended to comprise also techniques and mechanisms that complete, speed up and facilitate many functions of the traditional courts.

20. It may sometimes be difficult to differentiate the concept of ODR from other related but different concepts, such as, the concept of "cyberjustice". The latter refers to the general incorporation of technology into the justice system. According to the "Guidelines on how to drive change towards Cyberjustice" (CEPEJ, December 2016), Cyberjustice is "broadly understood as grouping together all the situations in which the application of ICTs, at least, forms part of a dispute resolution process, whether in or out of court". Consequently, the concept of Cyberjustice is broader than that of ODR, encompassing ODR mechanisms, but also others.

21. For the purposes of these guidelines, ODR refers to technology used for dispute resolution that is carried out remotely through the use of computers, including mobile devices, and the internet. ODR is not in itself a form of dispute resolution but rather refers to information technology (IT) that is used in the existing in-court proceedings. This is not a new type of proceedings and not an alternative to any such in-court proceedings. ODR provides new ways of access to the existing types of in-court proceedings. The concept follows from the ongoing transformation of national judicial systems into more digitalised form with remote access for the parties. ODR mechanisms are designed to facilitate electronic communications and in order to obtain an outcome without the need for the physical presentation of documents or for physical presence at a court meeting or hearing. In this line, United Nations Commission on International Trade Law (UNCITRAL) Technical Notes on Online dispute resolution, New York 2017, define ODR as a "mechanism for resolving disputes through the use of electronic communications and other information and communication technology".

22. The guidelines cover such ODR techniques as:

    i. online filing systems/platforms directly accessible for the parties and/or their representatives for the filing of statements (such as claims, counterclaims, responses, etc.);

    ii. online systems for storing, processing and assessing electronic evidence;

    iii. artificial intelligence, big data analysis techniques and automation, to the extent that they affect court proceedings;

    iv. platforms for online court meetings and online hearings, for example by audio- and videoconferencing, including giving of oral testimony by witnesses and experts.

Artificial intelligence (AI)

23. Artificial intelligence (AI) is a broad and rapidly evolving area of information and communication technology (ICT) that enables automated reasoning. It creates the potential for making automated decisions, recommendations and forecasts and thus can make civil and administrative proceedings more effective, accessible and affordable.

24. However, it is important to understand that ODR is not the same as AI. Not all ODR mechanisms involve AI components. ODR is a wider concept covering all kinds of online mechanisms for dispute resolution, including tools for automation that do not necessarily include an element of AI. The distinction between ODR and AI is kept throughout the guidelines. While the requirements to meet the guarantees stemming from Articles 6 and 13 of the European Convention on Human Rights apply to all ODR mechanisms, regardless of whether they involve AI elements or not, certain questions in this context bear increased significance with regard to AI mechanisms. This is particularly true for questions referring to automated decision-making without human intervention and the possibility for reviewing those decisions.

25. An AI system is an information system operating in the form of software or integrated in a physical hardware device that solves complex problems and functions in both physical and digital dimensions. Such a system functions by perceiving its environment through the collection and interpretation of collected, structured and unstructured data, drawing conclusions from available knowledge, processing information obtained on the basis of this data in order to make decisions on the most appropriate action to be taken in order to achieve the desired goal.

26. For the purposes of these guidelines, the definition of AI is that proposed by the European Ethical Charter on the use of artificial intelligence in judicial systems and their environment adopted by the European Commission for the Efficiency of Justice (CEPEJ) on 3–4 December 2018. The Charter sets out five principles which guide the development of AI tools in the European judicial systems. Those five principles are reflected in the guidelines dedicated to AI. The present guidelines also take into consideration the definition of AI proposed in the European Commission Communication on AI, as further elaborated by the Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission. The guidelines also follow the definition of AI system included in the Recommendation of the OECD Council on Artificial Intelligence adopted in 2019.

Information and communication Technology (ICT)

27. "ICT" means "Information and communication Technology" and refers to technology that provides access to information through

telecommunications. This includes the Internet, wireless networks, cell phones, and other communication media. For example, ODR users can communicate in real-time using technologies such as instant messaging, voice over IP (VoIP), and videoconferencing.

FUNDAMENTAL PRINCIPLES

Principle 1

28. Building trust and confidence in ODR is crucial for the proper use of ICT in the courts. It is now frequently the case that people, sometimes even judges, have doubts regarding use of ODR mechanisms, in particular where AI components are involved. The main challenge is how member States can build and enhance trust and confidence in ODR. This can be done only by applying the same key principles of a fair trial and effective remedy as interpreted by the European Court of Human Rights in its case-law in the context of existing in-court proceedings. These basic principles need to be further explained and transposed into the ICT context. The particular challenges arising from the application of these principles in the ODR context need to be analysed and addressed.

29. These guidelines can be used by member States to create a sound legal and ethical framework for using ODR. A human rights approach should constitute the starting point in designing the ODR mechanisms to make justice effective and efficient. Member States may also build and enhance trust and confidence in ODR by explaining to the public that use of ODR is not meant to fully replace the existing in-court proceedings but rather to supplement them and create additional options for access to justice. ODR needs to be seen as an ancillary aid to judicial decision-making, and to facilitate the judge's work, not as a constraint. ODR has to be adapted to the needs of judges and other users, and it should never infringe guarantees and procedural rights such as that of a fair hearing before a judge. ODR should improve the administration of justice, facilitate the user's access to the courts and reinforce the safeguards laid down in Article 6 of the European Convention on Human Rights: access to justice, impartiality, independence of the judge, fairness and reasonable length of proceedings.

Case-law of the Court of Justice of the European Union

The judicial protection mentioned resulting from Articles 6 and 13 of the European Convention on Human Rights is assured as long as electronic means are not the sole means for accessing the (settlement) procedure (Joined Cases C-317/08 to C-320/08, Rosalba Alassini and Filomena Califano v. Wind SpA, L ucia Anna Giorgia Iacono v. Telecom Italia SpA and Multiservice Srl v. Telecom Italia SpA, ECJ judgment of 8 March 2010, paras. 58 and 60).

Principle 2

30. ODR can contribute to more effective and efficient access to justice. However, the main obstacle to much wider use of ODR is access to technology. Some people do not have the necessary skills or facilities to use ODR and have a dispute resolved online (the "digital divide"). For example, they may be unfamiliar with using digital applications or may not have access to Internet, a computer or other tools or technologies. This group of people should be able to benefit from an appropriate assistance. Member States should develop ODR in such a way that the digital divide is adequately addressed. For example, ODR mechanisms can be kept optional. Authorities can set up support kiosks in court buildings or in legal aid bureaus. Supportive programs for the public can be created. The use of pilot schemes and user-feedback also help to address the digital divide problem. As it is explained in the guidelines, ODR mechanisms should have a simple and user-friendly interface to enable as many people as possible to use the technology.

Principle 3

31. The principle requires that where no particularities stem from the specific use of ODR mechanisms, procedural issues should be subject to the same rules that apply to the respective court procedure generally. ODR can and should be subject to the same due process standards that apply to the court procedure in an offline context, in particular independence, neutrality and impartiality. Any adjustments to the general procedural rules introduced due to the specific nature of an ODR mechanism must not undermine the principles of fair trial and effective remedy.

Principle 4

32. It is important that the parties to proceedings involving ODR are properly identified and there is no identity fraud. Separation of the digital identity from the physical one may generate problems related to the identification of the parties. In the first place, courts should seek to establish the identity of the parties. Such secure mechanisms include, in particular: i) certificates to electronic signatures, sometimes referred to as the "digital ID" of a person; ii) confirmation of identity by a payment system operator that has been used for paying court fees online; iii) public trust services providing technological mechanisms that ensure proper identification.

THE GUIDELINES

Fair procedure

Access to justice

Guideline 1

33. Justice is for everyone. In many member States applicants can lodge their cases without being represented by a lawyer, therefore it is particularly important to make the whole process easily understandable for its users. In order to enhance accessibility, the design of ODR should keep user interfaces as simple and intuitive as possible. If possible, the ODR instruments should be made accessible 24/24, 7/7 and from different computer and mobile devices operating systems. ODR should allow parties to use standard forms, upload related documents and receive timely responses. By means of ODR courts may also use real time communication. As far as a national legal system permits, technical tools available in ODR can offer flexibility regarding the language used in the proceeding, for example, by built-in translation programs, in case of multilingual proceedings involving parties from different countries or cultures. The principle of user-friendliness is not to be understood as being limited to litigants and their representatives but ODR tools should be equally user-friendly to judges and other court staff.

Guideline 2

34. Parties need access to all the necessary information. It is important then that appropriate assistance, information and feedback is provided to users. The design of ODR can make assistance (for example, tutorials) easily available to users. This includes information on how to submit a claim and receive information about the progress of the case. ODR may structure the process itself for litigants. It also means that dispute resolution through ODR can be done almost anywhere, making the process convenient and easy for litigants.

European Court of Human Rights' case-law

When the relevant law provides individuals with a possibility of lodging a compliant without being represented by a lawyer, domestic courts should advise applicants on how to remedy the formal deficiencies of their complaints (*Wende and Kukówka v. Poland*, no. 56026/00, § 54, 10 May 2007).

Magna Carta of Judges

The "Magna Carta of Judges" adopted by the Consultative Council of European Judges (CCJE) in 2010 emphasised in paragraph 14 on "access to justice and transparency" that "justice shall be transparent and information shall be published on the operation of the judicial system".

National example: Poland

In Poland applicants are provided with the possibility to find all relevant information on necessary formal requirements and technical issues on the e-court's website (general information on the e-court, information for applicant, for defendant, examples of correct and incorrect applications, FAQs, regulations on online payments, etc.).

Guideline 3

35. Essentially, each party must be given a fair and equal opportunity to argue his or her case as to both matters of fact and law and each party should have a right to react to and rebut the submissions of the other party. Evidence and relevant material must be disclosed to both parties in an accessible and adequate way. ODR speeds up processes, but also risks increasing information overload (which slows down information processing). Because of that, while disputes should be dealt within a reasonable time, parties should be granted reasonable time periods for reaction.

European Court of Human Rights' case-law

The principle of the equality of arms implies that each party must be afforded a reasonable opportunity to present his case — including his evidence — under conditions that do not place him at a substantial disadvantage vis-à-vis his opponent (*Letinčić v. Croatia*, no. 7183/11, § 48, 3 May 2016).

Guideline 4

36. ODR design needs to be guided by the internationally recognised technical standards, such as Design for All principles in the ICT context. This implies user-centred approach and that the use of ODR should not be hindered by the existence of barriers in their technical design and functionalities, nor by the inherent cost of their use. Following these standards will make content accessible to a wider range of people, such as persons with disabilities and make ODR more accessible to users in general. In particular ODR implementation may not be limited exclusively to text communication but allow and enable parties' visual and audio communication (video or audio conferences). Development of ODR systems allowing for more efficient types of communication should be promoted. This does not preclude designing of ODR systems which provide multiple choice communication types (text, audio, visual or various ICT). ODR should function properly to ensure confidentiality of communication, enabling the contact which is unfettered by any practical or other obstacle (*Marcello Viola v. Italy*, no. 45106/04, § 63–77, CEDH 2006-XI (extracts); *Golubeva v. Russia*, no. 1062/03, 17 December 2009).

Guideline 5

37. ODR has the potential to create cost savings by its very nature and to provide an economical alternative to proceedings handled in the traditional way. As a consequence, it is reasonable to expect that the cost of ODR use for the parties should be at least neutral in relation to the costs of access to the justice system using on-site resources. When general principles of exemption from costs and free assistance exist, they should be applicable to ODR.

Guideline 6

38. Parties should be notified when it is intended that their case will be processed with an ODR tool that involves an AI mechanism. In particular litigants have a right to obtain information on the reasoning underlying AI data processing operations applied to them. This should include the consequences of such reasoning. This transparency requirement is also confirmed by all existing recommendations, ethical codes and guidelines establishing ethical standards for designing, deployment and use of artificial intelligence, as established by the Council of Europe, the United Nations bodies, European Union, OECD and other international institutions. These standards need to be respected by designers, engineers, providers, administrators and professional users of ODR.

Equality of arms

Guideline 7

39. The guideline makes it clear that ODR should not deprive a party of the right to be heard by the court. The rights of access to a court, to adversarial proceedings and to an effective judicial remedy are fundamental rights of individuals that are safeguarded under the European Convention on Human Rights. While important, the objectives of achieving efficiency and expediting proceedings cannot justify infringing these rights.

Guideline 8

40. Independence and impartiality in ODR decision-making processes are essential requirements in order to ensure compliance with standards of the European Convention on Human Rights. Trust and confidence in ODR are built by avoiding the existence of - or any perception of - bias towards the interests of any of the parties. Article 6(1) of the European Convention on Human Rights explicitly states that the court must be independent and impartial. It is even more important for ODR as they may entail a process where the adjudicator is not physically present and trust issues may arise as a consequence.

Guideline 9

41. Knowledge of, and access to, the materials in the case-file, including those submitted by other parties is an essential requirement for fair proceedings. Moreover, the materials in the case-file, including all relevant metadata, should be sufficiently precise and detailed to enable the parties to challenge or contest their contents if they wish to do so. Where the time is insufficient for a party, a possibility to request an additional time should be available. The guideline covers not only access to documents submitted by the other parties, but also to the materials in the case-file, which often includes documentation produced by the court itself.

European Court of Human Rights' case-law

The requirement of "adversarial" proceedings under Article 6 of the European Convention on Human Rights entails having an opportunity to know and comment on the observations filed or evidence adduced by the other party. "Adversarial" essentially means that the relevant material or evidence is made available to both parties (*Ruiz-Mateos v. Spain*, 23 June 1993, § 63, Series A no. 2).

Evidence

Guideline 10

42. It is important to ensure that parties to proceedings involving ODR are not placed in a disadvantageous position because of their lack of access to digital services or their lack of understanding of how the services operate. ODR should be as user-friendly as possible and not operate in a manner that would be likely to prejudice the interests of any of the parties. See the guidelines on electronic evidence for further reference (in particular, in the part concerning fundamental principles).

Guideline 11

43. The use of electronic evidence may create specific challenges for a party wishing to challenge the authenticity or integrity of such evidence. ODR should provide appropriate safeguards in order to facilitate such a challenge. Instructions, templates or other tools can be used for this purpose. For example, where a party challenges the electronic evidence, the party seeking to rely on the evidence may be required to demonstrate its authenticity, for example by submitting metadata or seeking an appropriate order to obtain additional data from other persons, such as trust services providers. The reliability of electronic data may be proved in any manner, for example, by qualified electronic signatures or other similar methods of identification and ensuring integrity of the data. Provisions of national legislation establishing the evidential value of public (official) electronic systems that generate

electronic evidence should be respected. Moreover, parties should be permitted to challenge expert evidence where such evidence is likely to determine the outcome of the proceedings. In all these cases ODR should promote international standards applied to analysed data, such as those published by international standards communities, like ISO (International Organization for Standardization). The standardisation of communication patterns can produce considerable efficiency gains. See the guidelines on electronic evidence for further reference (in particular, guidelines no. 17–24 of the section on relevance of the electronic evidence).

Guideline 12

44. Specific challenges may arise when dealing with evidence in the courts using ODR mechanisms. These challenges point towards the need for consistency in the handling of the evidence. It is important to avoid discordant jurisprudence and to promote legal certainty. In this respect, parties may be allowed by their national legal system to rely on the previous decisions made by a court in similar or identical cases. This may help parties to have structured their evidence based on such previous decisions or on templates provided by the courts on the webpages. Specific recommendations may be issued by member States, for example on the format of the data to be submitted as evidence. Such solutions, however, should not undermine the independence of judges.

Effective proceedings

Guideline 13

45. As a large number of the judgments of the European Court of Human Rights relates to the violation of Article 6 of the European Convention on Human Rights in the context of referrals the excessive length of court proceedings, it is crucial for member States to increase their efforts in order to eliminate this problem. Effective proceedings require avoidance of undue delays. In this regard ODR provides advantage. Additionally, due to use of AI components the work of a court may be further significantly improved. The use of AI components may speed up the procedure and may allow for a more complete analysis of the case. Effective proceedings may be achieved only under condition that the process is streamlined as much as possible. In particular, physical presence of the parties should be required by the court only when it is necessary. ODR may assist in avoiding the necessity of physical presence not only of the parties themselves but also of other attendees, whose presence would otherwise be required, which often causes problems and slows down the proceedings. Many member States use videoconferencing in their courts with persons situated at a remote location to ensure, for example, an appearance of witnesses and experts. Proper design of the ODR also means that ODR allows payments of court fees on-line. See

the guidelines on electronic evidence for further reference (in particular guidelines 1–5 of the section on oral evidence taken by remote link).

European Court of Human Rights' case-law

In requiring cases to be heard within a "reasonable time", the Court underlines the importance of administering justice without delays which might jeopardise its effectiveness and credibility (*H. v. France,* 24 October 1989, § 58, Series A no. 162-A; *Katte Klitsche de la Grange v. Italy*, 27 October 1994, § 61, Series A no. 293-B).

A state may be found liable not only for delay in the handling of a particular case, but also for failure to increase resources in response to a backlog of cases or for structural deficiencies in its judicial systems that cause delays. Tackling the problem of unreasonable delay in court proceedings may thus require the state to take a range of legislative, organisational, budgetary and other measures (*Rutkowski and Others v. Poland*, nos. 72287/10 and 2 others, § 128, 7 July 2015).

Guideline 14

46. Special attention needs to be paid to ensuring that proceedings are not unnecessarily protracted by technical difficulties. Alternatives have to always be available whenever the ICT system is under maintenance or is facing technical problems, in order to avoid any adverse impact on court activity. Such technical difficulties must not be detrimental to the parties and there should be a possibility to adjust time periods providing for a sanction, as necessary.

Guideline 15

47. To ensure efficient, timely and adequate resolution of disputes and their de-escalation member States may integrate a pyramid model of dispute resolution where adjudication by a judge comes as a last tier. Amicable settlement of disputes with the involvement of ADR may further provide cost-efficient and more satisfactory result to parties than adjudication. However, attempts to settle a dispute with the involvement of ADR before instituting adjudicative proceedings before a judge shall be reasonable and should not compromise or deny access to court as a fundamental right protected by the Article 6 of the European Convention on Human Rights. Use of above-mentioned methods and techniques should not create substantial delay or increase substantively the costs for the parties.

Delivery of the decision

Guideline 16

48. The outcomes of the proceedings involving ODR being known to the parties is important for three reasons: (1) to ensure equality of information between the parties, (2) to ensure that the outcomes can be scrutinised and appealed if necessary and (3) to guide the development of the law.

In case of ODR the most important factors are the public scrutiny and the requirement that the proceedings are conducted in a reasonable time, with due process.

Guideline 17

49. This guideline stems from the right to public delivery of judgment. Article 6 (1) of the European Convention on Human Rights explicitly states that judgment shall be pronounced publicly. However, this does not require reading out of the judgment in open court. Other means of rendering a judgment public are allowed, such as making judgments available on request (*Moser v. Austria*, no. 12643/02, § 101, 21 September 2006). In each case the form of publicity must be assessed in the light of the special features of the proceedings in question (*Pretto and Others v. Italy*, 8 December 1983, § 26, Series A no. 71; *Axen v. Germany*, 8 December 1983, § 31, Series A no. 72). For example, the full text of the judgment can be made available on the court website. According to the jurisprudence of the European Court of Human Rights the requirement for public pronouncement has been complied with where, by being deposited in the court registry, the full text of the judgment has been made available to everyone (*Pretto and Others v. Italy*, cited above, §§ 27–28).

Right to a reasoned decision

Guideline 18

50. Every judicial decision reached using ODR or with the assistance of ODR needs to be clear in order to allow everyone involved to understand why the court is supporting a certain position (*Seryavin and Others v. Ukraine*, no. 4909/04, §§ 55–62, 10 February 2011). ODR does not suspend the right to obtain an explanation for the decision taken. Sufficiently detailed reasons should be given. The extent of the duty to give reasons depends on the nature of the decision and the circumstances of the case. The main arguments of the parties should be examined and require a specific and explicit response. Sufficiently reasoned decisions are required, firstly, in order to reassure the parties that their respective arguments have been taken into account in arriving at the decision and, secondly, to assist a party in deciding whether there are sufficient grounds to appeal against the decision. It is only by giving a reasoned decision that there can be public scrutiny of the administration of justice. This means that, at the very least, the outcomes must be known to the parties.

Enforcement of the decision

Guideline 19

51. Execution of a final and binding decision which results from an ODR mechanism must be regarded as an integral part of the "right to a

court" for the purposes of Article 6 of the European Convention on Human Rights. Every litigant to the ODR has a right to enforcement of a judgment, and the delay in the execution of a judgment must never be such that it impairs the litigant's right to a fair trial. The right to the execution of judicial decisions is of even greater importance in the context of administrative proceedings (*Sharxhi and Others v. Albania*, no. 10613/16, § 92, 11 January 2018). ODR can contribute to expediting enforcement proceedings in the same way as it can expedite the adjudicative stage of proceedings. For example, national law may provide for the electronic enforcement clause sent directly through the IT system to the bailiff. Electronic communication with the bailiff makes it quicker and easier to monitor the execution of judicial decisions.

European Court of Human Rights' case-law

It would be inconceivable that Article 6 (1) should describe in detail procedural guarantees afforded to litigants — proceedings that are fair, public and expeditious — without protecting the implementation of judicial decisions (...) Execution of a judgment given by any court must therefore be regarded as an integral part of the "trial" for the purposes of Article 6 of the European Convention on Human Rights (*Burdov v. Russia*, no. 59498/00, § 34, CEDH 2002-III). An unreasonably long delay in enforcement of a binding judgment may therefore breach the Convention (*Burdov (n° 2)*, no. 33509/04, § 66, CEDH 2009).

National example: Lithuania

The majority of court order proceedings regarding monetary claims are handled using online filling and digital case management. Court orders are generally issued as digital official documents with secure electronic signatures that can be submitted electronically to the bailiff for enforcement.

Right to judicial review in cases involving purely automated decisions

Guideline 20

52. There can be no single, or simple, answer to the question concerning how the right to review a decision involving an ODR element should be exercised because it depends on the character and the scope of the ODR element concerned. Where the ODR only plays a subordinate role helping a judge in the proceedings, there is no reason to deviate from the standard rules on appeal applicable to proceedings not involving an ODR element. However, the question becomes crucial when ODR instruments take the shape of tools for purely automated decisions. The scenarios in which ODR mechanisms leading to purely automated decisions could be used extend from minor cases which can be easily automated because they are legally simple and the ODR mechanism is primarily used for calculation purposes, to complex cases involving advanced AI mechanisms.

53. However, it is in this context that Article 13 of the European Convention on Human Rights comes into play. Article 13 provides that everyone whose rights and freedoms as set forth in the European Convention on Human Rights are violated shall have an effective remedy before a national authority. Parties should be allowed to contest purely automated decisions and to request that such review is to be made by a judge. The European Court of Human Rights does not specify at what level this remedy is to take place. Basically, two models are conceivable: it is for the member State to decide if the review should be made at the same judicial level or at a higher appeal level. The use of ODR can open up new avenues of redress for infringements in the national judicial systems. In view of the unique character of the ODR the member State may decide, irrespective of existing review mechanisms, to establish an additional review process on the same level as the one, on which the automated decision was made. Alternatively, the member State can leave the review before a judge to its existing appeal level. In any case, this guideline does not require all automated decisions to be automatically subject to review or to change the existing review model.

European Court of Human Rights' case-law

Article 13, giving direct expression to the States' obligation to protect human rights first and foremost within their own legal system, establishes an additional guarantee for an individual in order to ensure that he or she effectively enjoys those rights (*Kudła v. Poland* [GC], no. 30210/96, § 152, CEDH 2000-XI).

Consultative Council of European Judges — Opinion No. (2011) 14

The introduction of IT in courts in Europe should not compromise the human and symbolic faces of justice. (…) Justice is and should remain humane as it deals primarily with people and their disputes.

Transparency in the use of ODR and requirements for hearings

Transparency in the design and operation of ODR mechanisms

Guideline 21

54. Transparency in ODR is crucial. Both the design and operation of ODR mechanisms need to be explained to the public, in an easy-understandable language, in order to promote access to justice. The public should understand the implications of the use of ODR, believe that the ODR works well and that its outcomes are fair. This guideline goes beyond a simple requirement to disclose basic information on the design and use of ODR on the Internet. Different methods can be used to engage the public. Genuine communication strategies and policies includes press releases, video broadcasts, and webinars or social media

publications. Member States can explain to the public that ODR makes justice more accessible, e.g. by not requiring the physical presence at the court, saving the costs of the travel to the court and allowing the parties to file documents by electronic means or ensuring confidence and reducing stress for individuals representing themselves in the proceedings.

Public and oral hearings

Guideline 22

55. In case of a traditional court (physical court buildings) its activity is self-explanatory to the public and can be inspected by members of the public by attending public hearings. It might be different when proceedings or separate hearings are performed remotely and electronically with the help of ODR mechanisms. One should remember what the aim of public hearings is: they allow for public scrutiny of judicial decisions and proceedings. Making proceedings transparent in this way is a form of accountability that enhances fairness. This function of public scrutiny must also be ensured in remotely conducted electronic proceedings using ODR tools. Here, these aims can be achieved by traditional and new means. Technically, digital courts can be designed as open courts, if not more so than physical court buildings. The particular technical solution depends on the design of the procedure in question. For example, where virtual hearings in the courts replace a court hearing, ODR may allow public access to virtual hearings and information in a controlled manner without the observers having to physically go to a courtroom. Organising traditional public hearing is not required in ODR but it might be used to ensure publicity of hearings while using ODR tools for remote (virtual) attendance of hearings by parties, witnesses, experts or some of them; judges and/or observers at the same time might be physically present in courtrooms or any other physical rooms where court hearings might be broadcasted. In any case, however, the requirement of public hearing does not require member States to open up their virtual hearings to an unlimited number of simultaneous streams to the public, just as much as seats in a physical courtroom are also limited. Any such option must consider the due safeguards in respect of protection of personal and other sensitive data, sufficient cybersecurity and other principled discussed in these guidelines.

Guideline 23

56. The purpose of ODR is not to close the courts and hearing rooms. The aim is to improve effectiveness and efficiency. The right to an oral hearing does not necessarily require physical presence, and videoconferencing may be an appropriate way to guarantee litigants their right for example where parties voluntarily renounce their right to a physical presence (*Vladimir Vasilyev v. Russia*, no. 28370/05, § 81–90, 10 January 2012).

Videoconferencing where the communicators can hear and see each other in real time (and where provision is made that, for example witnesses are not coached from behind the screen and that witnesses' identity is properly authenticated) may, depending on the case, function as well as an "oral" hearing (provided the technology works on both ends of the transmission and this can be archived). An oral hearing is not always necessary to secure the parties participation in the proceedings. Written proceedings using ODR mechanisms can be permissible provided that the litigants have the right to have an oral hearing in the form of a review on the same level or re-hearing at an appeal stage of the proceedings. For instance, in administrative proceedings, an oral hearing before the authority is obligatory only in certain cases, and more emphasis is placed on the broadly understood right to active participation in proceedings at any stage of the proceedings. Such participation does not require oral hearings, but the possibility of expressing the party's opinion on the materials in the case-file, including evidence collected and motions lodged by the other party (*Vilho Eskelinen and Others v. Finland [GC]*, no. 63235, § 74, ECHR 2007-II). Using ODR can enhance the efficiency of written proceedings.

Other issues of transparency, including public scrutiny

Guideline 24

57. Safeguards for independence and impartiality of the judiciary must be effectively incorporated into proceedings involving ODR (*Agrokompleks v. Ukraine*, no. 23465/03, § 136, 6 October 2011). ODR must be transparent in terms of the identities and affiliations of the ODR providers and those of the interveners and managers of the ODR mechanisms. Member States should adopt policies dealing with identifying and handling conflicts of interest in the ODR.

Guideline 25

58. The guarantees enshrined in Article 6 (1) of the European Convention on Human Rights include the obligation that all documents generated by ODR, including the final judgment and other decisions or notifications, are written in clear and plain language. The language used must be such as to enable the parties to make effective use of any existing right of appeal.

Guideline 26

59. Procedural rules applicable to ODR should make clear the process used to resolve a dispute. These rules should meet the requirements of the society, institution, and legal frameworks they serve. In particular ODR should incorporate procedures for addressing factors which may harm the fair use of ODR. For example, an ODR may need to display

or conceal different parts of information depending on the stage of process and the type of user. In this respect ODR can learn from a range of measures to mitigate risks and improve security, commonly used in other sectors including banking, online payment systems and healthcare sectors. These procedures need to be factored into the ODR's architecture.

Guideline 27

60. Relevant information can be made available on the court website in a user-friendly and accessible manner. For example, a court website may use text-to-audio transcription services. Good ODR information management ensures that information is authentic and reliable, can be retrieved quickly and easily, is retained for an appropriate length of time, is disposed of securely and appropriately, and is suitably protected. Transparency of procedural rules applicable to ODR contribute to increased trust, accountability, openness and efficiency.

Special issues related to the ICT nature of ODR techniques

Cybersecurity

Guideline 28

61. The justice system is vulnerable because of the increasingly sophisticated and numerous cyber-attacks to which courts are exposed. With the use of ODR comes the fear of an increase in the number of security breaches that would jeopardise the integrity of the judicial system and the data it handles. Cyber threats are a very real danger for justice systems. Risk exists that court documents and evidence can be subject to manipulation and attack. A breach in security could result in forgery, or the disclosure of confidential information. Against this background, courts may consider mechanisms for enhancing data security. There are ways of preventing such breaches in ICT (e.g. by reducing the risk of an attack occurring) and/or mitigating their effects (e.g. by planning in advance the right course of action in the event of an attack). It is crucial that an appropriate level of cybersecurity in the ODR systems and their integrity are ensured by member States. ODR mechanisms require protection to prevent external parties from hacking the system and obtaining non-public information. Regarding the authority to access information, there should be internal limitations to ensure that parties to disputes cannot access information that they are not allowed to obtain. This requires secure authentication and access control.

62. The Appendix to this explanatory memorandum contains a cybersecurity checklist for member States.

Guideline 29

63. It is important that security is built into the design of the ODR. Security is to be ensured throughout the lifetime of the ODR mechanism by design and development processes that constantly evolve to reduce the risk of harm from malicious exploitation. There are two basic principles that needs to be followed: the "security-by-design" and "security-by-default". The first means that all those involved in the design and development of ICT products, services and processes facilitating ODR are encouraged to implement measures at the earliest stages of design and development to protect the security of those products, services and processes to the highest possible degree, in such a way that the occurrence of cyber-attacks is presumed and their impact is anticipated and minimised. The principle of "security-by-design" is to be followed at the earliest stages of design and development to protect the security of ODR. The principle of "security-by-default" means that ICT products, services and processes facilitating ODR are configured in a way that ensures a higher level of security which should enable the first user to receive a default configuration with the most secure settings possible, thereby reducing the burden on users of having to configure an ICT product, service or process appropriately.

64. Certification plays a critical role in increasing trust and security in ICT products, services and processes facilitating ODR. This includes a comprehensive set of rules, technical requirements, standards and procedures. To express the cybersecurity risk, a certificate may refer to three assurance levels (basic, substantial, high) that are commensurate with the level of the risk associated with the intended use of the product, service or process, in terms of the probability and impact of an incident. The obtaining of certain certification levels may necessitate the existence of a national legal framework allowing and regulating testing and ethical hacking of (state-run) ICT systems.

Human rights protection, including personal data protection

Guideline 30

65. Member States' governments, legislators, courts as well as ODR developers, manufacturers and service providers should continuously assess the possible adverse consequences of ODR techniques and mechanisms on human rights and fundamental freedoms, and, considering these consequences, adopt a precautionary approach based on appropriate risk prevention and mitigation measures. In all phases of the processing, including data collection, they should adopt a "human rights by-design" approach and avoid potential biases, including those that may be unintentional or hidden, and risks of discrimination or other adverse impacts on the human rights and fundamental freedoms of individuals.

Guideline 31

66. It is necessary to ensure compliance of all processing of personal data using ODR mechanisms with data protection laws. The key underlying elements of this approach are the lawfulness, fairness, purpose specification, and proportionality of data processing. Responsibility for, and demonstration of, compliance (accountability), transparency, data security and risk management are also essential requirements.

Guideline 32

67. Personal data protection has to be a priority and needs to be properly resourced. Inadequate protection may hamper access to the courts. This risk should be counter-balanced by personal data protection training for court staff, clear data protection policies and guidelines, data protection audits and effective implementation of their results. Contemporary data protection regimes (such as the updated Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) play an important role in safeguarding the rights and interests of data subjects. Special consideration should be given by member States to the Guidelines on Artificial Intelligence and Data Protection adopted in 2019 by the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) of the Council of Europe.

68. "Technical and organisational measures", in the sense of these guidelines, are the functions, processes, controls, systems, procedures and measures taken to protect and secure the personal data that is processed within ODR system. These measures are a requirement for security of processing, preventing breaches, ensuring suitable processors, records of processing activities, design and a strong foundation for ensuring that rights and freedoms of the ODR users are protected. Specific measures include among others: i) protection against unauthorised access to confidential data, such as personal data, undisclosed know-how and business information, or other types of potentially sensitive information collected during ODR proceedings; ii) ensuring integrity of the data in order to exclude possibility of the unwanted alteration or deletion of data concerning electronic procedural documents, including the decision itself or pieces of evidence; iii) identification of fraud by parties, since the online context could make it harder for a judge to ascertain the identity of a party.

Guideline 33

69. ODR implementation can pose a threat to the privacy of individuals and should, therefore, be complemented by ethical and human rights considerations. There should be an appropriate balance between the utility of open data and the privacy of the data subjects. ODR mechanisms

should be designed and developed responsibly, by applying the principles of "privacy-by-default" and "privacy-by-design". "Privacy-by-default" means that the court must ensure that personal data is processed with the highest privacy protection and "privacy-by-design" means that ODR need to implement technical and organisational measures, at the earliest stages of its design, in such a way that safeguards privacy and data protection principles right from the start.

Guideline 34

70. There is a risk that, in order to reduce the cost of ODR implementation, member States decide to outsource ODR platforms to external providers in exchange for access to personal data of users. It is also possible that that ODR is exploited by the companies that base their business model on tracking the data. Privacy concerns require that commercial tracking, profiling or targeting is not built into the design of ODR systems, because such activities have potentially serious impact on the personal freedom and autonomy of individuals and may lead to prejudice and discrimination. Where all or any part of ODR mechanisms are outsourced, providers should be bound by a comprehensive processing contract which will guarantee compliance with data protection law and exercise of individuals' data protection rights.

Other issues (not stemming from the jurisprudence of the European Court of Human Rights)

Testing, monitoring, upgrading, research and development

Guideline 35

71. To ensure technological advancements, member States are encouraged to stimulate progress in the ODR field by developing and maintaining such mechanisms themselves or stimulating non-governmental and/or private projects and programs. The development of ODR mechanisms should be funded, whenever this is appropriate and possible, by public bodies with the aim of enhancing public trust and confidence in ODR. The purpose of these funds may be the creation of an environment conducive to ODR development in accordance with Articles 6 and 13 of the European Convention on Human Rights. Changes in the field of cyber justice should be court-driven, not technology-driven. Relevant research can fill in gaps in legal and technical knowledge and improve functioning of ODR.

Guideline 36

72. The purpose of testing ODR is to evaluate its compliance with the specified legal, procedural and technical requirements. ODR testing, for example, might verify whether every type of user input produces the

intended output across the ODR application. Testing should be based on quality factors like reliability, usability, integrity, security, capability, efficiency, portability, maintainability and compatibility. Sufficient piloting and adjustments before the deployment ensure efficiency and adequate added value. Close, on-going involvement of future users helps to minimise any discrepancies between the needs stated on paper and how the IT specialists address them in practice, and enables the proposed technical solutions to be reoriented, where feasible and without affecting the project schedule or cost. Trials at pilot sites provide an opportunity to learn from a series of initial users before approving the next stage of the project or rolling it out on a bigger scale.

Guideline 37

73. The proper design of an ODR mechanism needs a constructive dialog to be established between those developing technology and those responsible for adjudication. It is for member States to decide which stakeholders should be involved and to what extent, as it depends on the type of the particular ODR concerned. Some require more input from the stakeholders, such as involvement of AI components and some less. The judiciary should be actively involved in the testing and piloting phases. In this context it is also important to ensure that the design of ODR do not deprive judges of their decision-making capacity. However, judges are not the only professionals that could be involved in the design. The dialogue may include other stakeholders such as lawyers, court staff and court users. Technology developers should strive to better understand the justice system and collaborate with judges and court staff to ensure that ICT architecture meets the needs of both the courts and the public. The ODR's architecture also needs to be flexible, and ready to adjust to judicial case-law or practices. For further references see Guidelines on how to drive change towards Cyber justice [Stock-taking of tools deployed and summary of good practices] of 7 December 2016, European Commission for the Efficiency of Justice.

Guideline 38

74. ODR must remain at the current level of service delivery and technological innovation. Each ODR mechanism goes through a development life cycle from initial planning through to disposition. The ODR mechanism has a cyclical nature which means that it constantly improves through change and upgrading. Replacing the outdated hardware or software, security upgrades, and continuous improvement on a regular basis is needed. Each member State should define its own best practices for various stages of ODR development.

Awareness raising, training and education

Guideline 39

75. Awareness raising, training and education of individuals and legal entities is key to enable successful exploitation of ODR techniques and mechanisms and to ensure its development and use. Measures need to be in place to improve a range of basic to advanced digital skills of different socio-economic groups. These include digital skills for the elderly, and other target groups, such as persons with disabilities. As the main providers of court services and ODR mechanisms, public authorities also require adequate knowledge and skills. This includes competences to develop ODR mechanisms in a responsive design manner for communities and businesses in compatibility with the requirements of the European Convention on Human Rights in order to build and enhance public trust and confidence in ODR.

Committee of Ministers Recommendation Rec(2004)4 **to member States on the European Convention on Human Rights in university education and professional training**

The Committee of Ministers recommends, inter alia, that member States ascertain "the adequate university education and professional training concerning European Convention on Human Rights and the case-law of the Court exist at national level and that such education and training are included, in particular (…) as a component of the preparation programmes of national or local examinations for access to the various legal professions and of the initial and continuous training provided for judges, prosecutors and lawyers".

In the framework of its follow-up to Recommendation Rec(2004)4, the Drafting Group III of the Committee of experts on the system of the European Convention on Human Rights (DH-SYSC), stated inter alia that member States should notably enhance the effectiveness of such university education and professional training by providing each category of public with necessary tools to comply with the obligations stemming from the European Convention on Human Rights . To this end, member States should provide quality targeted and accessible professional training. Also, professional training should be provided, as far as possible, by persons having good knowledge of the system of the European Convention on Human Rights and practical experience from the relevant professional field (see document DH-SYSC-III(2019)01 Rev, §§ 2 and 5).

Guideline 40

76. Member States need to ensure that ODR mechanisms are user-focused, accessible, fair, transparent, accountable and financially viable. Judges, legal practitioners and all those involved in court proceedings should be aware that the use of ODR has a potential to lead to greater automation, greater speed of information processing, better efficiency and lower costs of dispute resolution. This means that more disputes can be resolved,

leading ultimately to a greater access to dispute resolution and to cost savings. ODR also has the ability to revolutionise access to justice, for example to persons who would find it hard to access courts. The development of online learning methods could be used to disseminate such details of ODR experience among all professionals concerned.

Guideline 41

77. Access to interdisciplinary training on ODR operation is necessary for judges and legal practitioners as well as court staff. Dispute resolution professionals should have sufficient skills and training to carry out their duties. The digitally competent professional should be aware of advancements in technology and, in particular, keep abreast of developments within IT security. Experts generally underline the need for proper means of protection and control, and emphasise the importance of providing all court staff with IT security training for online communications. Member States should take measures to ensure legal and IT experts are available to judges, legal practitioners and court staff for consultation when specialised knowledge on the interpretation and application of laws and regulations is required in the process of providing ODR services. Training on ODR may cover specific challenges raised by ODR, such as cybersecurity. Awareness of the wider digital context and use of emerging technologies, such as cloud computing, trust services or blockchain, is important.

Guideline 42

78. Judges are encouraged to be able to use ODR mechanisms and follow good practices in the handling of ODR. Such good practices address, e.g. the risk that certain individuals (with physical or mental disabilities, socially disadvantaged or the elderly) will find it difficult to obtain access to justice. In order to prevent this, judges are encouraged to consult extensively with lawyers who tend to serve traditionally disadvantaged or marginalised groups. Another risk is that the removal of discretion and human judgment could lead to prejudice and stereotyping. This risk can be also prevented by judges in the review process (see paragraphs 52–53 above). Judges are encouraged to be aware of and understand the data risks, security, and privacy issues.

Guideline 43

79. Law schools are encouraged to change, if necessary, the way they provide education and provide a digital lawyering skills framework to teach students how to use technology to assist in the delivery of legal services. Good practices include new models of learning, such as increased level of online learning developed during pandemic crisis. Legal education and the legal profession may follow such good practices in order to keep pace with technological advancements, in particular introduction

of ODR mechanisms in the justice systems. It is important that students stay mindful of the legislation that governs human rights. Students need also be aware that courts are now utilising artificial intelligence to enhance their practices. In this respect a good practice is that students are given an opportunity to explore not only where the practice of law is now but also where it is heading. A broad range of competencies are required for an individual to be considered digitally competent. Teachers can use real-world examples.

APPENDIX

CYBERSECURITY CHECKLIST FOR MEMBER STATES

Member States should implement the following in designing ODR:

1. **Protection of stored, transmitted or otherwise processed data**:
   a. against accidental or unauthorised storage, processing, access or disclosure during the entire life cycle of the ICT product, service or process facilitating ODR.
   b. against accidental or unauthorised destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, service or process facilitating ODR.
2. **User access management through secure identification and authentication:** Authorised persons, programs or machines should only be able to access the data, services or functions to which their access rights refer.
3. **Identification and documentation of known dependencies and vulnerabilities:**
   ⇨ Modern ICT products and systems often integrate and rely on one or more third-party technologies and components such as software modules, libraries or application programming interfaces. This reliance, which is referred to as a "dependency", could "pose additional cybersecurity risks as vulnerabilities found in third-party components could also affect the security of the ICT products, services and processes facilitating ODR. In many cases, identifying and documenting such dependencies enables end users of ICT products, services and processes to improve their cybersecurity risk management activities by improving, for example, users' cybersecurity vulnerability management and remediation procedures.
   ⇨ Additionally, such dependencies and vulnerabilities could to a certain degree be avoided by providing, to the extent possible, the necessary means for in-house design and development.

4. **Logging of data accession, use and processing:** to record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom.
5. **Allowing consultation of the log files:** to make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom.
6. **Vulnerability testing:** verifying that ICT products, services and processes facilitating ODR do not contain known vulnerabilities.
   ⇨ Vulnerability testing may necessitate the existence of a national legal framework allowing and regulating testing and ethical hacking of (government) ICT systems.
7. **Providing back-up facilities and technical support:** to restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident.
8. **Security-by-design and by-default:** that ICT products, services and processes facilitating ODR are secure by-design and by-default.
9. **Up-to-date hard- and software:** to ensure that ICT products, services and processes facilitating ODR are provided both with up-to-date software and hardware that do not contain publicly known vulnerabilities, and with mechanisms for secure updates.

Cybersecurity certification of ICT products, services and processes facilitating ODR could be sought in order to minimise cybersecurity risks and to maximise trust and confidence. E.g. for EU-countries: certification could be sought in the framework of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (European Union Cybersecurity Act).

BIBLIOGRAPHY

1. Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings (Adopted by the Committee of Ministers on 30 January 2019, at the 1335th meeting of the Ministers' Deputies), CM(2018)169-add1final.
2. Online Dispute Resolution and Compliance with the Right to a Fair Trial and the Right to an Effective Remedy (Article 6 and 13 of the European Convention on Human Rights). Technical Study on Online Dispute Resolution Mechanisms. Prepared by Prof. Julia Hörnle, CCLS, Queen Mary University of London, Matthew Hewitson (South Africa) and Illia Chernohorenko (Ukraine), Strasbourg, 1 August 2018, CDCJ(2018)5.

3. Guide on Article 6 of the European Convention on Human Rights, Right to a fair trial (civil limb), updated on 31 August 2019, Council of Europe/European Court of Human Rights, 2019.

4. A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework. Prepared by the Expert Committee on human rights dimensions of automated data processing and different forms of artificial intelligence (MSI-AUT). Rapporteur: Karen Yeung, DGI(2019)05.

5. Guidelines on Artificial Intelligence and Data Protection, T-PD(2019)01.

6. European Ethical Charter on the use of artificial intelligence in judicial systems and their environment, Council of Europe, Commission for the Efficiency of Justice (CEPEJ), 3–4 December 2018.

7. "European judicial systems, efficiency and quality of justice: Use of information technology in courts in Europe", CEPEJ Studies No. XX, 2016 edition (2014 data).

8. Consultative Council of European Judges (CCJE), Opinion No. (2011)14, "Justice and information technologies (IT)".

9. Drafting Group of the Committee of experts on the system of the European Convention on Human Rights (DH-SYSC), Drafting Group III on the follow-up to Recommendation Rec(2004)4, Good national practices illustrating the principles set in Appendix I to the revised Recommendation Rec(2004)4 (document DH-SYSC-III(2019)01 Rev), 2019.

10. Magna Carta of Judges, Council of Europe, Consultative Council of European Judges (CCJE), 2010.

11. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108); see http://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 [Accessed 20 November 2020].

12. Parliamentary Assembly of the Council of Europe, Resolution 2054 (2015), "Access to justice and the Internet: potential and challenges", Report: Doc. 13918 of 10 November 2015.

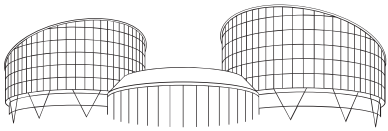
13. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&from=EN) [Accessed 20 November 2020].

14. Recommendation of the OECD Council on Artificial Intelligence, OECD/LEGAL/0449, Adopted on: 22 May 2019, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 [Accessed 20 November 2020].

15. The European Commission's high-level expert group on artificial intelligence, A Definition of AI: Main Capabilities and Scientific Disciplines. Definition developed for the purpose of the deliverables of the High-Level Expert Group on

AI Brussels, 18 December 2018; https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai [Accessed 20 November 2020].

16. Byrom N., Digital Justice: HMCTS data strategy and delivering access to justice. Report and recommendations, The Legal Education Foundation, October 2019.
17. Hörnle J., Cross-border Internet Dispute Resolution, Cambridge University Press 2009.
18. Hörnle J., Encouraging Online Alternative Dispute Resolution (ADR) in the EU and Beyond, European Law Review 2013, Volume 38 (2), pp. 187–208.
19. UNCITRAL Technical Notes on Online Dispute Resolution, New York, 2017.
20. Online Dispute Resolution Standards of Practice as developed by the ICANN available at https://www.icann.org/en/system/files/files/odr-standards-of-practice-en.pdf [Accessed 20 November 2020].
21. UNCITRAL Working Group III (Online dispute resolution) Thirty-third session, New York, 2016, Online dispute resolution for cross-border electronic commerce transactions, A/CN.9/WG.III/WP.140, https://undocs.org/en/A/CN.9/WG.III/WP.140 [Accessed 20 November 2020].
22. Rainey B. et al, Jacobs White & Ovey, The European Convention on Human Rights, Oxford University Press, 2014.
23. Carneiro D. et al., ODR: an Artificial Intelligence Perspective, Artificial Intelligence Review 2014, Volume 41, pp. 211–240.
24. Altreas N. et al, Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective, Peer J Computer Science Open Access (Published 24 October 2016) https://peerj.com/articles/cs-93.pdf [Accessed 20 November 2020].
25. Loutocký P., Online dispute resolution and the latest development of UNCITRAL model law, in: Cofola International 2015: current challenges to resolution of international (cross-border) disputes: conference proceedings (ed. K. Drličková), Brno 2015, pp. 243–256.
26. Scherer M., Artificial Intelligence and Legal Decision-Making: The Wide Open?, Journal of International Arbitration 2019, vol. 36, no. 5, pp. 539–574.
27. Hanriot M., Online dispute resolution (ODR) as a solution to cross border consumer disputes: the enforcement of outcomes, McGill journal of dispute resolution 2015, Volume 2, pp. 1–22.
28. Uzelac A., van Rhee C. H. (eds.), Transformation of Civil Justice, Ius Gentium: Comparative Perspectives on Law and Justice, Springer International Publishing 2018.
29. Vitkauskas D. and Dikov G., Protecting the right to a fair trial under the European Convention on Human Rights: A handbook for legal practitioners, Council of Europe 2017, available from: https://rm.coe.int/protecting-the-right-to-a-fair-trial-under-the-european-convention-on-/168075a4dd [Accessed 20 November 2020].



EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

П'ЯТА СЕКЦІЯ

Справа «Джаллоу проти Норвегії»

(Заява № 36516/19)

РІШЕННЯ

Стаття 6 (цивільна частина) • Справедливий судовий розгляд • Відсутність суттєво невигідного становища або нерівності сторін через участь у розгляді справи про виконання батьківських обов'язків з використанням засобів відеозв'язку в зв'язку з неможливістю в'їхати до країни, щоб бути фізично присутнім

СТРАСБУРГ

02 грудня 2021 р.

ОСТАТОЧНЕ

02.03.2022 р.

Це рішення набуло статусу остаточного відповідно до пункту 2 статті 44 Конвенції. До нього може бути внесено редакційні виправлення.

У справі «Джаллоу проти Норвегії»

Європейський суд з прав людини (П'ята секція), що засідає Палатою у такому складі:

Сіофра О'Ліpі (Síofra O'Leary), головуючий суддя,

Мартінс Мітс (Mārtiņš Mits),

Стефані Муру-Вікстрьом (Stéphanie Mourou-Vikström),

Латіф Гусейнов (Lətif Hüseynov),

Йован Ілієвскі (Jovan Ilievski),

Ладо Чантурія (Lado Chanturia),

Арнфінн Бардсен (Arnfinn Bårdsen), судді,

та Віктор Соловейчик, Секретар секції Суду,

З урахуванням:

заяви (№ 36516/19) проти Королівства Норвегії, поданої до Суду відповідно до статті 34 Європейської конвенції з прав людини (далі Конвенція) громадянином Гамбії паном Ебрімою Па Джаллоу (далі заявник) 01 липня 2019 року;

рішення надіслати повідомлення про заяву Уряду Норвегії (далі — Уряд);

зауважень сторін;

провівши нараду за зачиненими дверима 02 листопада 2021 року,

ухвалює рішення станом на цю дату:

ВСТУП

1. У справі розглядаються скарги, подані до Суду за статтями 6 і 8 Конвенції щодо провадження, у якому заявник вимагав надання йому права виконувати батьківські обов'язки щодо своєї дитини, над якою він ніколи не мав опіки, після смерті матері дитини.

ОБСТАВИНИ СПРАВИ

2. Заявник народився у 1972 році та проживає в Гамбії. У Суді його представляла пані Ш'ятвет, адвокат, яка практикує в м. Осло.

3. Пан М. Емберленд з Генеральної прокуратури (управління цивільних справ) представив Уряд Норвегії як його агент, якому допомагали пан Дж. Ванґснеса і пан Т. Мідттуна Тобіассена, адвокати того ж управління.

4. Надані сторонами фактичні обставини справи можна стисло викласти в такий спосіб.

I. КОНТЕКСТ СПРАВИ

5. У заявника двоє дітей, які проживають у Норвегії, Т. і Ґ., 1999 та 2011 років народження відповідно. Заявник живе у Гамбії, одружений і має там п'ятьох дітей.

6. Заявник був одружений з К.Дж., коли їхній старший син Т. народився в Гамбії у 1999 році.

7. Заявник і К.Дж. розлучилися приблизно у 2003 році. К.Дж. вийшла заміж у Норвегії за іншого чоловіка, який успішно подав там заяву про возз'єднання сім'ї з нею у 2003 році. К.Дж. отримала незалежну посвідку на проживання у 2004 році. Старший син, Т., отримав посвідку на проживання у Норвегії у 2007 році. До цього він жив зі своєю бабусею у Гамбії.

8. Ґ. був зачатий, коли К.Дж. у 2010 році на три тижні приїздила до Гамбії. К.Дж. повернулася до Норвегії, і у 2011 році там народився Ґ.

9. У 2011 або 2012 роках Управління праці та соціального забезпечення Норвегії (Arbeids- og velferdsdirektoratet) (далі — Управління) зверталося до К.Дж., щоб уточнити, хто є батьком Ґ. Вона повідомила їм, що це заявник, і тому Управління подало запит до посольства Норвегії у Гані, яке спробувало розшукати заявника через консульство у Гамбії. Їм вдалося зв'язатися з братом заявника, який повідомив, що заявник переїхав до Гвінеї-Бісау. Оскільки вони не змогли зв'язатися з самим заявником, у 2012 році розгляд справи було тимчасово зупинено. К.Дж. повідомили, що вона має зв'язатися з Управлінням, якщо отримає нову інформацію про батька дитини. Оскільки сам заявник не визнавав батьківство щодо Ґ., інформацію про дитину було внесено до Державного демографічного реєстру Норвегії з позначкою про те, що батько невідомий.

10. Заявник ніколи не був в Норвегії і також ніколи не виконував батьківських обов'язків щодо Ґ. З моменту свого народження у 2011 році Ґ. жив зі своєю матір'ю та братом у Норвегії.

11. Ґ. зустрівся із заявником у Гамбії у 2015 році, коли К.Дж. привезла туди обох дітей під час двотижневої відпустки. Позиції сторін про ступінь контакту між заявником і Ґ. різняться. Заявник стверджував, що К.Дж. і діти зупинилися неподалік того місця, де він жив, і що заявник і Ґ. бачилися кожні два-три дні упродовж цього періоду. Ґ., ймовірно, також бував у Гамбії і до цього один раз зустрічався із заявником. До того ж заявник стверджував, що він також підтримував контакт із дітьми по телефону до моменту смерті К.Дж. 25 червня 2017 року; проте Уряд стверджував, що Ґ., безперечно, не міг на той час розмовляти англійською, а отже, він не зміг би спілкуватися із заявником однією мовою.

12. Після смерті матері Ґ. жив з другом сім'ї, Ґ.Н., якого він називав «дядьком», і його сім'єю. Одного разу до Норвегії приїхав з Англії дядько Ґ. по матері, М.Дж., щоб доглядати за Ґ., і вони разом переїхали до квартири К.Дж. Потім Ґ. поїхав.

II. РОЗГЛЯД СПРАВИ ПРО ВИКОНАННЯ БАТЬКІВСЬКИХ ОБОВ'ЯЗКІВ ЩОДО Ґ.

13. Ґ.Н. 20 серпня 2017 року (див. пункт 12 вище) подав заяву до міського суду (tingrett) про надання йому права виконувати батьківські обов'язки щодо Ґ. Ця заява була відкликана 29 серпня 2017 року. Міський суд повідомив про ситуацію служби соціального захисту дітей; вони вже були проінформовані про смерть К.Дж.

14. Сестра покійної матері Ґ., А.Дж., яка жила в Англії, 19 вересня 2017 року звернулася до міського суду із заявою про надання їй права виконувати батьківські обов'язки щодо Ґ.

15. Міський суд 10 жовтня 2017 року отримав електронний лист від заявника, у якому він також подав заяву про надання права виконувати батьківські обов'язки щодо Ґ.

16. Міський суд призначив адвоката для надання допомоги Ґ., який подав відповідь на заяви 13 жовтня 2017 року.

17. Потім заявник пояснив свою заяву про надання йому права виконувати батьківські обов'язки щодо Ґ. у листі від 23 жовтня 2017 року.

18. Міський суд 25 жовтня 2017 року провів планове засідання, у якому взяли участь призначений судом експерт, дядько Ґ. М.Дж. (див. пункт 12 вище), опікун Ґ., адвокат А.Дж. (див. пункт 14 вище) і адвокат, призначений міським судом для надання допомоги Ґ. (див. пункт 16 вище). Було вирішено, що експерт має продовжувати вивчати ситуацію в Англії. Суд уповноважив експерта підготувати письмовий звіт.

19. У той же час 22 листопада 2017 року заявник подав заяву на отримання шенгенської візи до посольства Норвегії в Аккрі. 29 листопада 2017 року посольство відхилило заяву, надавши таке пояснення:

«Оскільки наш досвід і досвід місцевого управління з питань видачі шенгенських віз з конкретними групами та національностями показує, що багато хто не залишає Норвегію або Шенгенську зону після закінчення строку дії їхніх віз, ми практикуємо видачу віз лише у виняткових випадках. Ймовірність повернення оцінюється індивідуально, і велике значення надається як потенціалу еміграції в країні походження заявника, так і індивідуальним факторам, що стосуються заявника».

20. Заявник подав апеляційну скаргу на рішення про відмову у видачі візи до Управління імміграції (Utlendingsdirektoratet — UDI), яке відхилило її 06 квітня 2018 року.

21. У той же час 17 грудня 2017 року міський суд отримав ще одне письмове повідомлення від заявника, у якому він пояснив, що на той момент йому не було надано візи.

22. Призначена судом експерт (див. пункт 18 вище) подала свій письмовий звіт 02 січня 2018 року. Міський суд провів засідання 04 січня 2018 року. А.Дж. була присутня і дала свідчення, був заслуханий один свідок. Експерт також дала свідчення про свою роботу у цій справі. Опікун Ґ. виступив проти заяв як А.Дж., так і заявника.

23. Міський суд ухвалив рішення 08 січня 2018 року. У ньому повторювалося, що мати Ґ., К.Дж., на момент своєї смерті була єдиною, хто виконував батьківські обов'язки щодо Ґ. Батько Ґ., заявник, ніколи не жив із родиною в Норвегії. Як наслідок, за змістом статті 38 Закону про дітей, більше не було нікого, хто виконував би батьківські обов'язки щодо Ґ. І, як передбачено статтею 63 Закону про дітей, міський суд повинен був ухвалити рішення за заявами тих, хто подав заяву про надання права виконувати батьківські обов'язки (див. пункт 49 нижче).

24. Міський суд вирішив, що можлива небезпека того, що Ґ. не буде забезпечено належного догляду й утримання, або що він постраждає в інший спосіб, якщо А.Дж. буде надано право виконувати батьківські обов'язки щодо нього. Тож її заяву було відхилено. Потім суд перейшов до розгляду заяви заявника й зазначив у цьому контексті, що заявник ніколи не жив у Норвегії та висловив побажання, щоб Ґ. переїхав до Гамбії. Ба більше, Ґ. погано знав заявника: ймовірно, він зустрічався з ним лише один раз і кілька разів розмовляв із ним по телефону. До того ж заявник не дуже прагнув надати допомогу Ґ. після смерті його матері. На думку міського суду, існувала значна небезпека того, що Ґ. не буде забезпечено належного догляду й утримання, якщо заявнику будуть надані права на виконання батьківських обов'язків щодо Ґ.

25. Після оцінки всієї наданої йому інформації міський суд дійшов висновку, що мінімальні стандарти, вказані у третьому та четвертому пунктах статті 63 Закону про дітей, однозначно не були дотримані (див. пункт 49 нижче), і тому заяву заявника про надання права виконувати батьківські обов'язки щодо Ґ. було відхилено.

26. Оскільки міський суд відхилив обидві заяви про надання права виконувати батьківські обов'язки щодо Ґ., він повідомив служби соціального захисту дітей відповідно до положень статті 63 Закону про дітей (див. пункт 49 нижче). На той час Ґ. уже проживав у прийомній родині.

27. Тітка Ґ., А.Дж., подала до Вищого суду (lagmannsrett) апеляційну скаргу на рішення міського суду. Заявник написав листа до міського суду

після ухвалення ним рішення. Проте Вищий суд не врахував, що, написавши лист, заявник мав намір оскаржити рішення міського суду, і тому він не був залучений до справи як її сторона. Підготовче засідання у Вищому суді відбулось у червні 2018 року, на якому заявник, відповідно, не був присутній і не був представлений. Вищий суд призначив розгляд апеляційної скарги на 11 та 12 вересня 2018 року. Вищий суд повторно призначив призначеного міським судом експерта (див. пункт 18 вище), який подав перший звіт до Вищого суду 31 серпня 2018 року.

28. У той же час 27 червня 2018 року заявник знову подав заяву на отримання шенгенської візи. Управління імміграції відхилило його заяву 25 липня 2018 року. Заявник подав апеляційну скаргу на це рішення 17 жовтня 2018 року.

29. Стало зрозумілим те, що заявник мав намір оскаржити рішення міського суду і доручив це адвокату, який з'явився у Вищому суді 30 жовтня 2018 року. Нове підготовче засідання було проведено 15 листопада 2018 року, а слухання було перенесено на 10 та 11 січня 2019 року.

30. Вищий суд 22 листопада 2018 року надіслав лист до Управління імміграції. Він підтвердив, що у справі, яку він розглядав, заявник був стороною про право на виконання батьківських обов'язків щодо його сина після смерті матері дитини, і заявив, що розгляд апеляційної скарги було призначено на 10 та 11 січня 2019 року, і що бажано, щоб заявник був присутній протягом усього слухання. Передбачалося, що він дасть свідчення, а призначений судом експерт, члени колегії та адвокати сторін хотіли би поставити йому запитання. Враховуючи важливість справи, Вищий суд визнав, що свідчення, дані через Skype, не будуть оптимальним рішенням.

31. У листі Вищий суд також зазначив, що, на його думку, для з'ясування обставин справи та забезпечення процесуальної рівності сторін важливо, щоб заявник був присутній упродовж усього слухання. Заявник заперечував стосовно заяви А.Дж. і довелося дати йому можливість поставити запитання їй та будь-яким свідкам, яких вона може захотіти представити. Було б складно забезпечити заявнику ці права як стороні справи, якби він не був присутній.

32. До того ж Вищий суд заявив, що з суто технічної точки зору судовий розгляд може транслюватись у Гамбію за допомогою засобів відеозв'язку, щоб заявник міг стежити за ним, за умови наявності сумісного обладнання. Але заявник повинен був мати можливість обговорювати зі своїм адвокатом поставлені запитання, та оскільки вони не могли обговорюватися відкрито перед усім судом, було

складно уявити, як можна було провести слухання без численних перерв.

33. Призначений Вищим судом експерт 03 січня 2019 року подав другий звіт (див. пункт 27 вище).

34. Імміграційна апеляційна комісія (Utlendingsnemnda — UNE) 07 січня 2019 року відхилила апеляційну скаргу заявника на рішення про відхилення його заяви на отримання шенгенської візи (див. пункт 28 вище). Апеляційна комісія дійшла висновку, що ймовірність повернення заявника на батьківщину була недостатньо високою для того, щоб можна було видати йому візу. У рішенні були викладені, зокрема, такі міркування:

> «UNE бере до уваги заяву [Вищого суду] від 22 листопада 2018 року. Також UNE вважає, що участь у судовому розгляді у справі про опіку над дитиною в багатьох випадках вважається вагомою соціальною причиною для видачі візи. Проте, ураховуючи поточний стан справ, UNE вважає, що існує велика ймовірність еміграції. Тож UNE погоджується з UDI у тому, що в цьому разі недостатньо вагомих соціальних причин, які переважали б відсутність у заявника необхідних зв'язків з країною його походження. У своїй оцінці UNE підкреслює той факт, що заявник технічно може стежити за ходом судового розгляду за допомогою Skype. Також його адвокат може бути присутнім на розгляді і захищати законні інтереси заявника. UNE не вважає, що відмова у видачі візи порушує положення статті 3 Конвенції про права дитини або розділу 104 Конституції».

З тих пір заявник кілька разів подавав запит на перегляд цього рішення, і одне з рішень у відповідь на запит було ухвалене 29 травня 2019 року.

35. У листі, який Вищий суд отримав 08 січня 2019 року, заявник просив перенести судовий розгляд апеляційної скарги у зв'язку з негативним рішенням Імміграційної апеляційної комісії. Він стверджував, що відмова у видачі йому візи була недійсною, і Вищий суд має перенести розгляд, поки віза не буде йому видана, щоб він міг бути присутнім.

36. Вищий суд відхилив запит у рішенні від 09 січня 2019 року, у якому зазначив, що малоймовірно, що рішення про видачу візи було помилковим. Суд також взяв до уваги той факт, що заявник розумів, що він може не отримати візи, і можливість стежити за ходом судового розгляду за допомогою Skype була окреслена вже на зустрічі з планування у листопаді 2018 року (див. пункт 29 вище). Для Вищого суду спостереження заявника за розглядом за допомогою Skype було не ідеальним рішенням, але прийнятним за таких обставин. До того ж Вищий суд відрізнив справу заявника від справи «Чіліз проти Нідерландів» (Cılız v. the Netherlands) (№ 29192/95, ЄСПЛ 2000-VIII), зокрема, на тій підставі, що у справі заявника не було подібного питання про втручання в сімейне життя, оскільки він ніколи не жив

із Ґ. і зустрічався з ним лише двічі. До того ж Вищий суд заявив, що той факт, що висновки експертів (див. пункти 27 і 33 вище) не було перекладено, не дає підстав для перенесення термінів, і зазначив, що перший звіт датований ще 31 серпня 2018 року. Зрештою, Вищий суд підкреслив, що для Ґ. було важливо, аби питання, що стосується його батьківських обов'язків, було вирішене, оскільки з моменту ухвалення рішення міським судом минуло вже більше року, і що у заявника був адвокат, який захищав би його інтереси під час розгляду апеляційної скарги.

37. Розгляд апеляційної скарги відбувався у Вищому суді 10 та 11 січня 2019 року. До суду з'явилися А.Дж. з адвокатом, а також опікун і адвокат Ґ., призначений судом експерт та адвокат заявника. Крім сторін і призначеного судом експерта, свідчення давали п'ять свідків. До початку судового розгляду (in limine litis) 10 січня 2019 року заявник звернувся з проханням відокремити його апеляційну скаргу та апеляційну скаргу А.Дж., щоб його апеляційну скаргу розглянули пізніше. Вищий суд відхилив це прохання. У судових протоколах викладено такий порядок:

«08 січня 2019 року адвокат Ш'ятвет [(адвокат заявника)] клопотала про перенесення розгляду апеляційної скарги. 09 січня 2019 року Апеляційний суд відхилив клопотання. Серед іншого було наголошено на тому, що [Ґ.] потрібен мир і стабільність, що для нього життєво важливо, щоб питання про батьківські обов'язки було вирішене невідкладно, і що подальше перенесення цього питання було б для нього тягарем. Ті самі аргументи застосовуються і зараз.

В Апеляційному суді було роз'яснено, що Ебріма Па Джаллоу не претендує на повсякденний догляд за дитиною, а лише на виконання батьківських обов'язків. Проте це ніяк не впливає на той тягар, який у такий спосіб покладається на хлопчика.

Стверджувалося, що свідок-експерт не оцінював Ебріми Па Джаллоу. Апеляційний суд посилається у цьому контексті на той факт, що апеляційне провадження було перенесено, оскільки батько не зробив заяви, і йому була надана можливість визначити референтних осіб/інформаторів для експертної оцінки.

Апеляційний суд одноголосно постановив, що справу не слід відокремлювати, і що розгляд клопотання Ебріми Па Джаллоу про надання права виконувати батьківські обов'язки не переноситиметься».

38. Ба більше, із судових протоколів випливає, що питання про участь заявника за допомогою Skype було порушене кілька разів, зокрема, у таких примітках:

«Головуючий суддя порушив питання про те, як Ебріма Па Джаллоу стежитиме за процесом у технічному сенсі. Було роз'яснено, що технічно

йому буде складно отримати переклад англійською мовою за допомогою Skype. Необхідно було б викликати фахівців технічної підтримки, що можна було б організувати під час пізнішої перерви. Після цього адвокат Ш'ятвет погодилася, що вступні заяви можна зробити без забезпечення її клієнта Ебріми Па Джаллоу можливістю стежити за процесом за допомогою Skype.

<...>

Суд оголосив перерву з 11:05 до 11:25. Досі не було умов до того, щоб Ебріма Па Джаллоу міг стежити за ходом розгляду за допомогою Skype, але адвокат Ш'ятвет усе ж дозволила продовжити розгляд без трансляції за допомогою Skype.

<...>

Засоби для Skype-трансляції не були готові, тому перекладач здійснював переклад, сидячи поруч з особою, яка дає свідчення, використовуючи ноутбук, що належить адвокату Ш'ятвет, на якому був встановлений Skype.

<...>

У п'ятницю, 11 січня 2019 року, апеляційний розгляд продовжився в тому ж місці за участю тих самих осіб. Ебріма Па Джаллоу не брав участі за допомогою Skype з початку денних слухань, але було вирішено, що спробу встановити зв'язок буде зроблено пізніше.

Адвокат Ш'ятвет дала свою згоду на те, що розгляд може бути продовжено без присутності Ебріми Па Джаллоу за допомогою Skype.

<...>

Після обідньої перерви Ебріма Па Джаллоу долучився за допомогою Skype і зміг стежити за ходом засідання...».

39. У рішенні від 11 лютого 2019 року Вищий суд відхилив апеляційні скарги. Вищий суд дійшов висновку, що надання тітці, А.Дж., або заявнику права виконувати батьківські обов'язки не відповідатиме найкращим інтересам Ґ. Після опису правової основи Вищий суд спочатку виклав ситуацію Ґ., перш ніж перейти до заяв А.Дж. і заявника відповідно.

40. Стосовно ситуації Ґ. він, серед іншого, зазначив, що Ґ. був добре обізнаний про спір, який тривав щодо нього і це було додатковим тягарем для нього. На думку експерта (див. пункт 27 вище), Ґ. потрібен був спокій, стабільність і передбачуваність у майбутньому. Це дитина з особливими потребами як з точки зору емоційного, так і соціального розвитку, і експерт рекомендував йому жити з людьми, які володіють особливими навичками взаємодії з дітьми і знаннями про їхній розвиток, дбайливими людьми, які були б особливо чутливими до його сигналів і здатні розпізнавати й інтерпретувати його основні потреби та емоційні стани. До того ж експерт повідомив, що Ґ., якому на той момент було дев'ять років, знайшов своє місце

у своїй прийомній сім'ї і називав їх «мама, тато і старший брат». Він чітко заявив, що хоче жити з ними у Норвегії, і експерт вважав, що його від'їзд становитиме ризик для його розвитку.

41. Також Вищий суд дійшов висновку, що надання А.Дж. права виконувати батьківські обов'язки не відповідатиме найкращим інтересам Ґ. У цьому контексті він урахував, що заява А.Дж. про надання їй права виконувати батьківські обов'язки була подана виходячи з припущення, що вона також щодня піклуватиметься про хлопчика. Тож, повертаючись до заяви заявника, Вищий суд зазначив, що стало зрозумілим те, що він не хотів відповідати за повсякденний догляд за Ґ. і за те, щоб Ґ. переїхав до його дому в Гамбії. Вищому суду було незрозуміло, чи заявник мав намір приїхати до Норвегії та взяти на себе відповідальність за щоденний догляд за Ґ. пізніше.

42. Також Вищий суд підкреслив, що, оскільки розглянуте питання полягало в тому, чи відповідатиме це найкращим інтересам Ґ., якщо заявник отримає право виконувати батьківські обов'язки щодо нього без щоденного догляду за ним, батьківські навички заявника не мали значення. На думку експерта, було б добре, якби заявник отримав право виконувати батьківські обов'язки щодо Ґ. за умови, що він не хотів, щоб Ґ. переїжджав, але в іншому разі, на її думку, було б неприродно для заявника брати участь у вирішенні питання про батьківську відповідальність. Потенційна майбутня справа, що стосується щоденного догляду, була б важким тягарем для Ґ., але експерт заявила, що якби заявнику було надано право виконувати батьківські обов'язки, вона очікувала б, що він триматиметься осторонь і обережно представлятиме себе та свою сім'ю. Експерт також стверджувала, що для Ґ. тоді було важливим те, де і з ким він жив. Те, хто виконував щодо нього батьківські обов'язки, було менш важливим.

43. Вищий суд заявив, що погодився з експертом у тому, що це не матиме безпосередніх практичних наслідків для Ґ. незалежно від того, чи були надані заявнику права на виконання батьківських обов'язків, і що, мабуть, важливо, аби заявник став частиною життя Ґ. згодом, так, щоб це було корисно для Ґ. Це могло відбуватися через надсилання фотографій, прояв інтересу до повсякденного життя Ґ. і присутності там, якби Ґ. був зацікавлений у контакті. Поступово вони могли б познайомитися ближче. Такий контакт не залежав би від наявності у заявника права виконувати батьківські обов'язки.

44. Стосовно вирішення питання про виховання Вищий суд зазначив, що заявник мало знав про Ґ., а отже, не відповідав критеріям для участі у вирішенні цих питань так, щоб це відповідало найкращим інтересам Ґ. До того ж географічна та культурна прірва між заявником

і опікуном Ґ. у Норвегії ускладнила б розподіл батьківських обов'язків між заявником і опікуном Ґ.

45. Вищий суд також заявив, що він має враховувати той факт, що заявнику, якби йому було надано право виконувати батьківські обов'язки щодо Ґ., було б легше ініціювати майбутні провадження щодо Ґ. Він посилався на те, що заявник робив різні заяви про те, чого він хотів для Ґ. щодо того, де і з ким він повинен був жити. Зрештою, Вищий суд заявив, що вважає, що рішення суду у справі «Ґюль проти Швейцарії» (Gül v. Switzerland) (19 лютого 1996 р., Звіти про рішення та ухвали 1996-I) не давало вказівок щодо цього, оскільки справа заявника стосувалася лише питань батьківських обов'язків, а не повсякденного догляду, а справа Ґюля стосувалася возз'єднання сім'ї.

46. Заявник оскаржив рішення Вищого суду до Верховного суду (Høyesterett). Апеляційна комісія Верховного Суду (Høyesteretts ankeutvalg) 10 квітня 2019 року відмовила йому в дозволі на оскарження рішення Вищого суду.

III. СУДОВИЙ ПЕРЕГЛЯД РІШЕНЬ ЗАЯВНИКА ПРО ВИДАЧУ ВІЗИ ПІСЛЯ ПОДАННЯ ЗАЯВИ ДО СУДУ

47. Заявник 04 жовтня 2019 року звернувся до міського суду з клопотанням про судовий перегляд рішення Імміграційної апеляційної комісії про видачу візи від 07 січня 2019 року, у перегляді якої не було відмовлено, зокрема, у рішенні від 29 травня 2019 року (див. пункт 34 вище) у порядку цивільного позову проти держави Норвегії. Він також клопотав про ухвалення декларативного рішення, у якому зазначалося б, що цим рішенням порушувалися положення статті 8 Конвенції.

48. Судове засідання відбулося 05 травня 2020 року, а міський суд ухвалив рішення 10 червня 2020 року. Суд дійшов висновку, що відносини між Ґ. і заявником не прирівнювалися до «сімейного життя» за змістом статті 8 Конвенції. Тож відмова у видачі візи не призвела до порушення положень статті 8. Проте суд установив, що в рішенні Імміграційної апеляційної комісії була допущена процедурна помилка. Спочатку комісія виходила з припущення, що заявник не задокументував своїх сімейних стосунків у Гамбії. Цей пункт було виправлено в одному з кількох клопотань про скасування, але міський суд постановив, що Імміграційна апеляційна комісія не оцінила справу на правильних фактичних підставах. Тож рішення було визнано нечинним.

ВІДПОВІДНЕ ЗАКОНОДАВСТВО

49. Статтею 38 Закону про дітей від 08 квітня 1981 року (barneloven) у редакції, що діяла на момент розгляду справи у Суді, встановлено, що право виконувати батьківські обов'язки щодо дитини, яка втратила одного з батьків, передають іншому з батьків, якщо останній уже

виконував батьківські обов'язки, або дитина жила з ним або з нею. У статті 63 цього Закону на той час зазначалося, що якщо більше немає нікого, хто виконує батьківські обов'язки щодо дитини, особи, які хотіли б отримати таке право, повинні звернутися до суду за місцем проживання дитини. Якщо отримано лише одну заяву про надання права виконувати батьківські обов'язки, суд має задовольнити заяву, якщо немає небезпеки того, що дитині не буде забезпечено належного догляду й утримання, або що він або вона може постраждати в інший спосіб. Якщо ніхто не звертався із заявою про надання права виконувати батьківські обов'язки або суд відхилив усі заяви, суд має повідомити про це служби соціального захисту дітей для вирішення питання про влаштування дитини в сім'ю.

ЗАКОНОДАВСТВО

I. СТВЕРДЖУВАНЕ ПОРУШЕННЯ ПОЛОЖЕНЬ СТАТТІ 6 КОНВЕНЦІЇ

50. Заявник подав скаргу на те, що провадження щодо його батьківських прав і обов'язків стосовно його дитини було проведено несправедливо з порушенням положень статті 6 Конвенції, у якій зазначено таке:

«Кожен має право на справедливий... розгляд... судом... щодо його прав та обов'язків цивільного характеру...».

A. Прийнятність

51. Суд зазначає, що заявник та інший родич Ґ., А. Дж., обоє звернулися до суду із заявою про надання їм права виконувати батьківські обов'язки щодо Ґ. Суд також зазначає, що Ґ. через свого опікуна виступив проти заяв як А. Дж., так і заявника. З огляду на ці обставини Суд виходить із того, що положення статті 6 Конвенції були застосовними до розгляду, який є предметом поданої до Суду скарги.

52. До того ж Суд зазначає, що ця скарга не є ні явно необґрунтованою, ні неприйнятною з будь-яких інших підстав, перелічених у статті 35 Конвенції. Тому вона має бути визнана прийнятною.

B. Суть справи

1. Твердження сторін

53. Заявник стверджував, що йому не лише не дозволили бути фізично присутнім під час слухання в державному суді, а й відмовили у в'їзді до Норвегії для підготовки до слухання, а отже, для особистої зустрічі з Ґ., свідком-експертом, службою захисту дітей і його адвокатом. Так заявник був поставлений у значно менш вигідне становище порівняно з тіткою Ґ., А.Дж., якій було дозволено зустрітися з Ґ., експертом, службою соціального захисту дітей та її адвокатом у контексті розгляду на обох рівнях юрисдикції.

54. Також заявник стверджував, що те, що йому не було надано права виконувати батьківські обов'язки щодо Ґ., призвело до розриву біологічних зв'язків між ними, оскільки окружна рада з питань соціального захисту набула компетенції дати дозвіл на усиновлення Ґ. відповідно до Закону «Про опіку та піклування щодо дітей». Присутність заявника в суді була необхідною, оскільки розглядалися його особисті якості й спосіб життя.

55. Заявник також стверджував, що причини, наведені державним судом для обґрунтування свого рішення, були недостатніми, щоб продемонструвати, що фізична присутність заявника була непотрібною, і він зазначив, серед іншого, що суд не навів жодних причин, чому він змінив свою думку щодо позиції, висловленої у його листі від 22 листопада 2018 року до Імміграційного управління, у якому стверджувалося, що присутність заявника мала велике значення як для роз'яснення заяви про надання права виконувати батьківські обов'язки, так і для рівності сторін. Імміграційні питання не були враховані в оцінці справедливого судового розгляду.

56. Уряд стверджував, що спочатку питання полягало в тому, чи позбавила фізична відсутність на слуханні заявника розумної можливості ознайомитися із зауваженнями або доказами, наданими іншою стороною, чи поставило це його в істотно менш вигідне становище порівняно з його опонентом у викладі його аргументації. Не кожне невигідне становище призведе до порушення положень пункту 1 статті 6 Конвенції.

57. Щодо фактів цієї справи Уряд стверджував, що заявник не мав абсолютного права бути фізично присутнім на слуханні. З огляду на це він наголошував, що справа відрізняється від справи «Карпенко проти Росії» (Karpenko v. Russia) (№ 5605/04, 13 березня 2012 р.), зокрема, оскільки національне провадження у справі заявника, на відміну від справи Карпенко, стосувалося встановлення, а не припинення батьківських обов'язків. Він також підкреслив, що в рішенні від 11 лютого 2019 року Вищий суд установив, що навички батьківства у заявника є нерелевантними для питання про батьківські обов'язки, оскільки він не подавав заяви про надання права щоденно піклуватися про Ґ.

58. Щодо присутності заявника на судових слуханнях у Норвегії за допомогою Skype Уряд стверджував, що це не підірвало позиції заявника порівняно з його опонентами. Уряд також зазначив, що адвокат заявника був присутній особисто і давав згоду на продовження розгляду у тих випадках, коли з'єднання за допомогою Skype не працювало. Лист Вищого суду від 22 листопада 2018 року, у якому Вищий суд наголосив на важливості особистої участі заявника, слід було розглядати

з огляду на той факт, що на той момент не було зрозумілим, що заявник подав заяву лише про надання йому права виконувати батьківські обов'язки, а не щоденно піклуватися про Ґ.

2. Оцінка Суду

59. Суд повторно наголошує, що принцип змагальності та принцип рівності сторін, які тісно пов'язані, є основоположними елементами концепції «справедливого судового розгляду» за змістом положень пункту 1 статті 6 Конвенції. Вони вимагають «справедливого балансу» між сторонами: кожній стороні має бути надана розумна можливість викласти свою точку зору на умовах, які не ставлять її в істотно менш вигідне становище порівняно з її опонентом або опонентами. Проте права, що випливають із цих принципів, не є абсолютними. Суд уже виніс низку рішень щодо справ, у яких пріоритет віддається переважаючим державним інтересам у відмові стороні в проведенні повного змагального розгляду. Тут Договірні сторони мають певні дискреційні повноваження. Проте саме Суд в останній інстанції повинен визначити, чи були дотримані вимоги Конвенції (див., наприклад, «Регнер проти Чеської Республіки» (Regner v. the Czech Republic) [ВП], № 35289/11, §§ 146–47, 19 вересня 2017 р., і посилання в ньому).

60. У цій справі Суд зазначає, що підставою для тверджень заявника, що стосуються несправедливості й нерівності у правах, власне, є те, що йому було відмовлено у в'їзній візі до Норвегії. Далі Суд зазначає, що рішення не надавати заявнику візи було ухвалено на основі міркувань суспільного інтересу, зокрема, що стосуються імміграційного контролю. Проте питання, яке має вирішити Суд, полягає не в тому, чи повинна була бути видана віза, щоб забезпечити заявнику справедливий судовий розгляд, а в тому, чи був судовий розгляд, в конкретних обставинах справи, справедливим щодо заявника, враховуючи, що йому не дозволили в'їхати до Норвегії, щоб бути фізично присутнім.

61. Насамперед Суд не може не взяти до уваги, що справа, яку розглядав Вищий суд, стосувалась особистих інтересів заявника, а також той факт, що Вищий суд під час підготовки справи надіслав лист до Імміграційного управління, у якому наголошено на необхідності фізичної присутності заявника для того, щоб забезпечити йому справедливий судовий розгляд (див. пункт 30 вище). Зокрема, Суд зазначає, що, оскільки А.Дж. також подала заяву про надання права виконувати батьківські обов'язки щодо Ґ., у своєму листі Вищий суд підкреслив необхідність рівності сторін; заявнику мала бути надана можливість поставити запитання до А.Дж. і тих чи інших свідків, яких остання могла би побажати представити, і мати можливість обговорювати це зі своїм адвокатом, що було б складніше, якби йому не було дозволено фізично бути присутнім зі своїм адвокатом у суді. До того ж

заявник повинен був сам постати перед судом, і йому повинна була бути надана можливість дати свідчення і бути допитаним. На той час Вищий суд визнав, що надання свідчень за допомогою Skype не буде оптимальним рішенням (див. пункти 30–32 вище).

62. Проте Суд також зазначає, що Вищий суд, після того як стало зрозуміло, що заявнику не буде дозволено в'їзд до Норвегії, провів нові й оновлені оцінювання та, зрештою, визнав прийнятним, також і з точки зору права заявника на справедливий судовий розгляд, продовжити заплановане слухання за участю заявника за допомогою Skype і за фізичної присутності на слуханні його адвоката. Він зробив це у двох рішеннях від 9 та 10 січня 2019 року на підставі певних міркувань, а саме: зацікавленість Ґ. у врегулюванні питання; той факт, що з моменту ухвалення рішення міським судом сплинуло вже більше року; було роз'яснено, що заявник не прагнув щоденно піклуватися про Ґ. (що було незрозуміло, коли суд уперше вийшов на зв'язок з імміграційною владою); і що в заявника буде адвокат, який представлятиме його в суді (див. пункти 36 і 37 вище).

63. Суд зазначає, що оскільки фізична присутність заявника більше не була можливою, Вищий суд на практиці мав вибір між відкладанням розгляду справи на невизначений період без видимого рішення або сприянням забезпеченню присутності заявника за допомогою відеозв'язку. З огляду на причини, надані Вищим судом, у Суду немає підстав критикувати Вищий суд за його вибір у цьому питанні. З огляду на це Суд наголошує, зокрема, на таких факторах:

64. По-перше, Вищий суд сам вказав на недоліки у відкладенні розгляду справи, зокрема, на те, що це суперечить найкращим інтересам Ґ. Крім того, як Суд постановив у різних контекстах, присутність у суді за допомогою відеозв'язку як така не завжди становить проблему, якщо цей засіб у конкретному випадку слугує легітимній меті і якщо організаційні моменти сумісні з вимогою дотримання належної правової процедури [див., наприклад, з відповідними змінами, «Дійкхайзен проти Нідерландів» (Dijkhuizen v. the Netherlands), № 61591/16, § 53, 08 червня 2021 р.; «Біволару проти Румунії» (Bivolaru v. Romania) (№ 2), № 66580/12, § 138, 02 жовтня 2018 р.); «Ічетовкіна та ін. проти Росії» (Ichetovkina and Others v. Russia), № 12584/05 та 5 інших, § 37, 04 липня 2017 р.; «Євдокимов та ін. проти Росії» (Yevdokimov and Others v. Russia), № 27236/05 і 10 інших, §§ 41–43, 16 лютого 2016 р.; та «Марчелло Віола проти Італії» (Marcello Viola v. Italy), № 45106/04, §§ 67 та 73–74, ЄСПЛ 2006-XI (витяги)].

65. По-друге, Суд нагадує, що справа, яку розглядав Вищий суд, зрештою, обмежувалася ухваленням рішення лише про виконання батьківських обов'язків, а не про опіку над Ґ., тобто про повсякденну відповідальність

за нього. З аргументації в рішенні Вищого суду випливає, що рішення про виконання батьківських обов'язків у цій справі вирішальною мірою не залежало від безпосереднього враження суддів про сторони через їхню фізичну присутність (див. пункти 39–45 вище).

66. По-третє, Суд бере до уваги той факт, що хоча заявник не погодився з тим, що Вищий суд розглядав справу за його фізичної відсутності, він через свого адвоката не скаржився на конкретні проблеми під час розгляду. Попри те, що в судових протоколах виникали певні проблеми зі з'єднанням, загалом вони показують, що адвокат не мав заперечень стосовно процедури розгляду (див. пункт 38 вище). З огляду на це Суд також зазначає, що представник заявника не подавав скарг до Вищого суду на те, що заявник не зміг конфіденційно поспілкуватися з ним під час розгляду.

67. По-четверте, Суд підкреслює, що заявникові, який брав участь у розгляді за допомогою Skype, допомагав його адвокат, який був постійно присутній на розгляді. Дійсно, навіть попри те, що заявнику було технічно складніше, наприклад, проконсультуватися з адвокатом щодо опитування свідків, ніж якби він знаходився у тій самій кімнаті, йому були надані широкі можливості викласти свою точку зору (див. пункти 36 і 37 вище).

68. Відповідно, хоча Суд приймає твердження заявника про те, що його фізична відсутність певною мірою зумовила те, що А.Дж. апріорі опинилася у легшій ситуації, ніж він завдяки її фізичній присутності, Суд не вважає, що застосоване технічне рішення поставило його в те чи інше «суттєво невигідне становище», як це вимагається згідно з практикою Суду про встановлення порушення статті 6 Конвенції у справі, подібній до цієї, або що у нього не було належної можливості висловити свою точку зору у Вищому суді. Суд зазначає, що А.Дж. не була опонентом заявника у справі, і Вищий суд не ухвалив рішення на її користь.

69. Щодо аргументів заявника про те, що він не міг у належний спосіб підготувати свою справу, оскільки йому не дозволили в'їзд до Норвегії, або тому що висновки призначених судом експертів (див. пункти 27 і 33 вище) не було перекладено, Суд зазначає, що звіти було подано до розгляду у Вищому суді 10 та 11 січня 2019 року і ніщо не свідчить про те, що заявник не міг поспілкуватися з адвокатом чи іншими особами на етапі підготовки справи, навіть якщо він не міг зробити це особисто на засіданнях. Експерт, який підготував звіти, також був присутній на розгляді у Вищому суді, де вона докладно пояснила свої звіти і де її можна було опитати (див. пункт 37 вище). Суд не вбачає жодних ознак того, що розгляд був несправедливим.

70. Викладених вище міркувань достатньо, щоб Суд мав можливість зробити висновок про відсутність порушення статті 6 Конвенції.

II. СТВЕРДЖУВАНЕ ПОРУШЕННЯ ПОЛОЖЕНЬ СТАТТІ 8 КОНВЕНЦІЇ

71. Заявник скаржився на те, що відмова надати йому право виконувати батьківські обов'язки щодо Ґ. порушила його право на повагу до його сімейного життя, встановлене у статті 8 Конвенції, у якій зазначено таке:

«1. Кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції.

2. Органи державної влади не можуть втручатись у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб».

72. За твердженням Уряду скарга за статтею 8 Конвенції була неприйнятною ratione materiae, оскільки у цьому разі «сімейного життя» не було. Він також стверджував, що в тому, що стосується суті справи, оцінка Вищим судом цього питання цілком вкладалася в межі розсуду, що надається державам-членам у подібних до поточної справах. На думку Уряду, заява заявника не містила вказівок на те, у який спосіб він зможе забезпечити Ґ. «турботу й увагу», проживаючи у Гамбії, або на якій підставі він вирішуватиме питання за Ґ., що стосуються його особистих інтересів і потреб.

73. Заявник стверджував, що у нього було сімейне життя на момент, коли у 1999 році народився брат Ґ., Т., і що родинні зв'язки не припинилися через те, що батьки розлучилися й одружилися з іншими людьми. Для припинення сімейного життя були потрібні виняткові обставини, а у цьому разі таких обставин не було. На думку заявника, мало місце порушення положень статті 8 Конвенції, а доводи Уряду були дискримінаційними тією мірою, якою саме відмова у видачі заявнику в'їзної візи становила перешкоду для його піклування про Ґ. і виконання ним батьківських обов'язків.

74. Суд наголошує, що лише біологічна спорідненість між одним із біологічних батьків і дитиною, без жодних додаткових юридичних або фактичних елементів, що свідчать про існування тісних особистих стосунків, є недостатньою для застосування захисту за статтею 8 Конвенції. Зазвичай обов'язковою умовою для стосунків, що прирівнюються до сімейного життя, є спільне проживання. У виняткових випадках доказом того, що стосунки є достатньо міцними для створення de facto «сімейних зв'язків» [див., наприклад, «А.Б.В. Проти Росії» (A.B.V. v. Russia), № 56987/15, § 65, 02 жовтня 2018 р. та «Анайо проти Німеччини» (Anayo v. Germany), № 20578/07, § 56, 21 грудня 2010 р., з додатковими посиланнями], можуть бути інші фактори. У цьому разі

Ґ. є біологічним сином заявника. Ґ. народився в Норвегії у 2011 році. Заявник ніколи не бував у Норвегії і на підставі наданої Суду інформації їхні стосунки полягали загалом у тому, що заявник познайомився з Ґ. під час двотижневої відпустки останнього у Гамбії, коли йому було чотири роки, і яка мала місце за два роки до смерті матері Ґ. та за чотири роки до ухвалення державним судом рішення. Також заявник і Ґ. могли підтримувати певний контакт телефоном (див. пункти 10–11 вище). Проте, навіть припускаючи, що такого обмеженого контакту було б достатньо для наявності de facto «сімейного життя» в контексті статті 8 Конвенції, Суд вважає, що скарга у будь-якому разі є однозначно необґрунтованою з таких причин.

75. У частині, що стосується процесуальних гарантій, які випливають зі статті 8 Конвенції у справах щодо стверджуваного втручання у право на повагу до сімейного життя, Суд установив вище, що твердження заявника про те, що судовий розгляд був несправедливим і що він постраждав від нерівності сторін у справі, не може бути успішним з точки зору положень статті 6 (див. пункти 59–70 вище). Суд не вважає, що розгляд процедур з точки зору статті 8 Конвенції може привести до іншого висновку.

76. Стосовно рішення по суті не надавати заявнику права на виконання батьківських обов'язків щодо Ґ. Суд зазначає, що основоположним елементом має бути те, що зв'язок між заявником і Ґ. на момент ухвалення рішення, яке оскаржується, був дуже обмеженим. Беручи це за вихідну точку, Суд зазначає, що Вищий суд ґрунтував своє рішення не надавати заявникові права виконувати батьківські обов'язки щодо Ґ. на міркуваннях, які містили той факт, що батьківські обов'язки були питанням окремим від встановлення контакту між заявником і Ґ., яке Вищий суд, дійсно, міг розглядати як необхідне, і що заявник, ураховуючи відстань між ним і Ґ. та брак знань про нього та його ситуацію, не відповідатиме критеріям для участі у вирішенні питань, що має належати до компетенції особи, наділеній правом виконувати батьківські обов'язки у спосіб, який відповідав би найкращим інтересам Ґ. (див. пункти 42–44 вище). За оцінкою Суду, причини, що їх надав Вищий суд, були як відповідними, так і достатніми, і немає жодних ознак того, що органи державної влади не керувались найкращими інтересами дитини або не змогли встановити справедливого балансу між конкуруючими інтересами у цій справі.

77. З огляду на зазначені обставини Суд вважає, що заява не свідчить про порушення статті 8 Конвенції й відповідно до цього положення є однозначно необґрунтованою в контексті підпункту (a) пункту 3 статті 35 Конвенції і має бути відхилена згідно з положеннями пункту 4 статті 35 Конвенції.

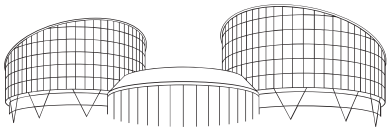
З ЦИХ ПРИЧИН СУД ОДНОСТАЙНО

1. Оголошує скаргу за статтею 6 Конвенції прийнятною, а скаргу за статтею 8 Конвенції неприйнятною.
2. Постановляє одностайно, що не було порушення за статтею 6 Конвенції.

Оформлено англійською мовою та нотаріально засвідчено в письмовій формі 02 грудня 2021 року відповідно до пунктів 2, 3 правила 77 Регламенту Суду.

Віктор Соловейчик
Секретар секції Суду

Сіофра О'Лірі
Головуючий суддя



EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

FIFTH SECTION

CASE OF JALLOW V. NORWAY

(Application no. 36516/19)

JUDGMENT

Art 6 (civil) • Fair hearing • No substantial disadvantage or inequality of arms for appearance through video-link in proceedings for parental responsibility, where applicant was not able to enter the country to be physically present

STRASBOURG

2 December 2021

FINAL

02/03/2022

In the case of Jallow v. Norway,

The European Court of Human Rights (Fifth Section), sitting as a Chamber composed of:

Síofra O'Leary, *President,*

Mārtiņš Mits,

Stéphanie Mourou-Vikström,

Lətif Hüseynov,

Jovan Ilievski,

Lado Chanturia,

Arnfinn Bårdsen, *judges,*

and Victor Soloveytchik, *Section Registrar,*

Having regard to:

the application (no. 36516/19) against the Kingdom of Norway lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by a Gambian national, Mr Ebrima Pa Jallow ("the applicant"), on 1 July 2019;

the decision to give notice of the application to the Norwegian Government ("the Government");

the parties' observations;

Having deliberated in private on 2 November 2021,

Delivers the following judgment, which was adopted on that date:

INTRODUCTION

1. The case concerns complaints lodged with the Court under Articles 6 and 8 of the Convention relating to proceedings through which the applicant sought to be granted parental responsibilities for his child of whom he had never had custody, after the child's mother had died.

THE FACTS

2. The applicant was born in 1972 and lives in Gambia. Before the Court, he was represented by Ms Schjatvet, a lawyer practising in Oslo.

3. The Norwegian Government ("the Government") were represented by Mr M. Emberland of the Attorney General's Office (Civil Matters) as their Agent, assisted by Mr J. Vangsnes and Mr T. Midttun Tobiassen, attorneys at the same office.

4. The facts of the case, as submitted by the parties, may be summarised as follows.

I. BACKGROUND

5. The applicant has two children living in Norway, T. and G., born in 1999 and 2011 respectively. He lives in Gambia and is married and has five children there.

6. The applicant was married to K.J. when their oldest son, T., was born in Gambia in 1999.

7. The applicant and K.J. divorced around 2003. K.J. married another man in Norway who successfully applied for family reunification with her there in 2003. K.J. was given an independent residence permit in 2004. The oldest son, T., was given a residence permit in Norway in 2007. Until then he had resided with his grandmother in Gambia.

8. G. was conceived when K.J. visited Gambia for three weeks in 2010. K.J. returned to Norway, and G. was born there in 2011.

9. In 2011 or 2012 the Norwegian Labour and Welfare Directorate (*Arbeids- og velferdsdirektoratet*) contacted K.J. to clarify who G.'s father was. She informed them that it was the applicant and the Directorate therefore sent a request to the Norwegian embassy in Ghana, who tried to track down the applicant through the consulate in Gambia. They were able to reach the applicant's brother, who stated that the applicant had moved to Guinea-Bissau. As they were unable to reach the applicant himself, the matter was put on hold in 2012. K.J. was informed that she should contact the Directorate if she received new information about the father. As the applicant himself has not recognised paternity of G., he is listed with an unknown father in the Norwegian National Population Register.

10. The applicant has never been to Norway, and neither has he ever had parental responsibilities for G. From his birth in 2011, G. lived with his mother and brother in Norway.

11. G. met with the applicant in Gambia in 2015, when K.J. took her children on a two-week holiday there. The parties' accounts of the degree of contact between the applicant and G. differ. The applicant submitted that K.J. and the children stayed close to where he lived, and that the applicant and G. saw each other every two to three days during that period. G. had probably also been to Gambia and met the applicant once prior to that. Moreover, the applicant maintained that he also had telephone contact with the children until K.J. died on 25 June 2017; the Government have argued, however, that it is undisputed that G. did not speak English at this time, and that he would therefore not have been able to communicate with the applicant in a shared language.

12. After the death of their mother, G. lived with a friend of the family, G.N., whom they call an "uncle", and his family. At some point, G.'s maternal uncle, M.J., arrived in Norway from England to look after G. and they moved into K.J.'s flat together. T. then moved out.

II. THE PROCEEDINGS CONCERNING PARENTAL RESPONSIBILITIES FOR G.

13. On 20 August 2017 G.N. (see paragraph 12 above), applied to the City Court (*tingrett*) to be given parental responsibilities for G. That application was withdrawn on 29 August 2017. The City Court notified the child welfare services of the situation; they had already been informed of K.J.'s death.

14. On 19 September 2017 the sister of G.'s late mother, A.J., who lived in England, applied to the City Court to have parental responsibilities for G.

15. On 10 October 2017 the City Court received an email from the applicant, also applying for parental responsibilities for G.

16. The City Court appointed a lawyer to assist G., who submitted a response to the applications on 13 October 2017.

17. The applicant further explained his application for parental responsibilities for G. in a letter of 23 October 2017.

18. On 25 October 2017 the City Court held a planning meeting which a court-appointed expert, G's uncle M.J. (see paragraph 12 above), G.'s guardian, A.J.'s lawyer (see paragraph 14 above) and the lawyer appointed by the City Court to assist G. (see paragraph 16 above) attended. It was decided that the expert should examine the situation in England further. The expert was given a mandate and asked to prepare a written report.

19. In the meantime, on 22 November 2017, the applicant applied for a Schengen visa at the Norwegian embassy in Accra. On 29 November 2017 the embassy rejected the application, giving the following explanation:

> "Where our and the local Schengen Cooperation's experience with specific groups and nationalities indicates that many fail to leave Norway or the Schengen area upon expiration of their visas, it has become our practice to issue a visa only in exceptional cases. Probability of return is assessed individually, and importance is attached to both the emigration potential in the applicant's country of origin and to the individual factors regarding the applicant."

20. The applicant lodged an appeal against the decision not to issue a visa with the Directorate of Immigration (*Utlendingsdirektoratet* — UDI), which rejected it on 6 April 2018.

21. In the meantime, on 17 December 2017, the City Court had received a further written communication from the applicant, in which he explained that he had not been granted a visa at that time.

22. The court-appointed expert (see paragraph 18 above) submitted her written report on 2 January 2018. The City Court held a hearing on 4 January 2018. A.J. attended and gave evidence and one witness was heard. The expert also gave evidence about her work on the case. G.'s guardian opposed the applications from both A.J. and the applicant.

23. The City Court gave judgment on 8 January 2018. It reiterated that G's mother, K.J., had had sole parental responsibilities for G. when she died. G.'s father, the applicant, had at no time lived with the family in Norway. As a result of this, there was, within the meaning of section 38 of the Children Act, no longer anyone with parental responsibilities for G. and, as provided in section 63 of the Children Act, the City Court had to decide on the applications from those who had applied to have parental responsibilities granted to them (see paragraph 49 below).

24. The City Court found that there would be a danger of G. not being given adequate care and maintenance, or that he would suffer in other ways, if A.J. were granted parental responsibilities for him. Her application was therefore dismissed. The court then moved on to assess the applicant's application, and noted in that context that he had never been to Norway and had expressed the wish that G. should move to Gambia. Moreover, G. knew little of the applicant — he had probably only met him once and spoken to him on the telephone a few times. In addition, the applicant had failed to show much interest in assisting G. after his mother's death. There was in the City Court's assessment a significant danger of G. not being given adequate care and maintenance if the applicant were to be granted parental responsibilities for G.

25. After assessing all the information that had been presented to it, the City Court found that the minimum standards referred to in the third and fourth paragraphs of section 63 of the Children Act had clearly not been met (see paragraph 49 below) and the applicant's application to be granted parental responsibilities for G. was therefore dismissed.

26. Since the City Court had dismissed both of the applications for parental responsibilities for G., it notified the child welfare services in accordance with section 63 of the Children Act (see paragraph 49 below). G. had already been placed in a foster home by that time.

27. G.'s aunt, A.J., appealed against the City Court's judgment to the High Court (*lagmannsrett*). The applicant wrote a letter to the City Court following its judgment. The High Court did not, however, consider that by writing the letter the applicant had intended to appeal against the City Court's judgment and he was therefore not included as a party to the case. A preparatory meeting before the High Court was held in June 2018, at which the applicant was accordingly not present or represented. The High Court scheduled the hearing of the appeal for 11 and 12 September 2018.

The High Court reappointed the expert that had been appointed by the City Court (see paragraph 18 above), who submitted a first report to the High Court on 31 August 2018.

28. In the meantime, on 27 June 2018, the applicant applied again for a Schengen visa. The Directorate of Immigration rejected the application on 25 July 2018. The applicant appealed against that decision on 17 October 2018.

29. It became clear that the applicant had intended to appeal against the City Court's judgment and he instructed counsel, who presented herself at the High Court on 30 October 2018. A new preparatory meeting was held on 15 November 2018 and the hearing was rescheduled for 10 and 11 January 2019.

30. On 22 November 2018 the High Court wrote a letter to the Directorate of Immigration. It confirmed that the applicant was a party to a case before it concerning parental responsibilities for his son, following the death of the child's mother, and stated that the hearing of the appeal had been scheduled for 10 and 11 January 2019 and that it was desirable that the applicant be present throughout the whole hearing. It was expected that he would give evidence, and both the court-appointed expert, members of the bench and the parties' counsel would want to put questions to him. Given the far-reaching character of the case, the High Court considered that evidence given by Skype would not be an optimal solution.

31. In the letter, the High Court further stated that it was of the view that it was important for the elucidation of the case and for the equality of arms between the parties that the applicant be present throughout the whole hearing. The applicant had opposed A.J.'s application and he had to be given the opportunity to question her and any witnesses she might wish to present. It would be difficult to ensure these rights as a party for the applicant if he were not present.

32. The High Court stated furthermore that, in purely technical terms, the proceedings could be transmitted to Gambia via video-link so that the applicant could follow them, providing that compatible equipment could be found. But the applicant would have to be able to discuss with his counsel when questions were put and, as they could not discuss openly in front of the whole court, it was difficult to picture how it would be possible to carry out the hearing without numerous interruptions.

33. On 3 January 2019 the expert appointed by the High Court submitted a second report (see paragraph 27 above).

34. The Immigration Appeals Board (*Utlendingsnemnda* — UNE) dismissed the applicant's appeal against the rejection of his application for a Schengen visa (see paragraph 28 above) on 7 January 2019. The Appeals

Board concluded that the likelihood of the applicant returning to his home country was not sufficiently high to enable a visa to be granted. The decision included, *inter alia*, the following considerations:

> "UNE notes the statement from [the High Court], dated 22 November 2018. Furthermore, UNE holds that taking part in a child custody case in court is in many cases considered to be a strong welfare reason for issuing a visa. However, as this case stands now, UNE considers there is a great potential for emigration. UNE therefore agrees with UDI in its assessment that there are not sufficiently strong welfare reasons in this case to outweigh the appellant's lack of necessary ties to his country of origin. In its assessment UNE emphasised the fact that it is technically possible for the appellant to follow the proceedings via Skype. Further, his attorney can attend the proceedings and safeguard the appellant's legal interest. UNE does not consider that not granting a visa breaches Article 3 of the Convention on the Rights of the Child or section 104 of the Constitution."

The applicant since several times requested that the decision be revised, and one of the decisions taken in response to a request to that effect was made on 29 May 2019.

35. In a letter received by the High Court on 8 January 2019, the applicant requested that the appeal hearing be rescheduled, due to the negative decision of the Immigration Appeals Board. He argued that the refusal to grant him a visa was invalid, and that the High Court had to reschedule the hearing until a visa had been granted, so that he could attend it.

36. The High Court refused the request in a decision of 9 January 2019, in which it noted that it was not likely that the visa decision was flawed. It also took note of the fact that the applicant had understood that he might not get a visa and that the possibility of following the proceedings by Skype had been outlined already in the planning meeting in November 2018 (see paragraph 29 above). For the High Court, the applicant following the proceedings via Skype was not a perfect solution, but acceptable in the circumstances. The High Court, moreover, distinguished the applicant's case from that in *Cılız v. the Netherlands* (no. 29192/95, ECHR 2000-VIII), *inter alia* on the grounds that it was not a similar issue of interference with family life in the applicant's case, since he had never lived with G. and had only met him twice. In addition, the High Court stated that the fact that the expert reports (see paragraphs 27 and 33 above) had not been translated did not give grounds for rescheduling and pointed out that the first report dated from as early as 31 August 2018. Lastly, the High Court emphasised that it was important for G. that the matter relating to parental responsibilities for him be decided — since more than a year since the City Court had given judgment had already passed — and that the applicant had counsel who would protect his interests during the appeal proceedings.

37. The appeal hearing was held in the High Court on 10 and 11 January 2019. A.J. attended with counsel, as did G.'s guardian and lawyer, the court-appointed expert, and the applicant's counsel. In addition to the parties and the court-appointed expert, five witnesses gave evidence. On 10 January 2019 the applicant asked *in limine litis* for his appeal and that of A.J.'s to be split, so that his appeal could be examined at a later point in time. The High Court refused the request. The court records include the following order:

"On 8 January 2019, Attorney Schjatvet [(the applicant's counsel)] petitioned for the appeal proceedings to be rescheduled. On 9 January 2019, the Court of Appeal refused the petition. Among other things, it was stressed that [G.] was in need of peace and stability, that it was vital for him that the matter of parental responsibilities be decided straight away, and that further rescheduling of the matter would be a burden to him. The same arguments apply now.

Before the Court of Appeal, it has been clarified that Ebrima Pa Jallow is not applying for day-to-day care of the child, but only parental responsibilities. However, this makes no difference to the burden the matter places on the boy.

It has been argued that Ebrima Pa Jallow was not assessed by the expert witness. The Court of Appeal refers in this context to the fact that the appeal proceedings were rescheduled because the father had not made a statement, and he was given the chance to identify reference persons/informants for the expert's assessment.

The Court of Appeal has unanimously found that the matter should not be subdivided, and that the petition for parental responsibilities on Ebrima Pa Jallow's behalf will not be rescheduled."

38. Moreover, it appears from the court records that the issue of the applicant's participation via Skype was returned to on several occasions, *inter alia* by way of the following notes:

"The presiding judge raised the question of how Ebrima Pa Jallow would follow the proceedings in a technical sense. It was clarified that, technically, it would be difficult to get the translation into English to him via Skype. Technical assistance would have to be called, which would be organised in a later break. Following this, attorney Schjatvet agreed that the opening statements could be made without her client, Ebrima Pa Jallow, being able to follow the proceedings on Skype.

...

The court adjourned for a break from 11.05 a.m. to 11.25 a.m. Things were still not ready for Ebrima Pa Jallow to be able to follow the proceedings via Skype, but attorney Schjatvedt still allowed the proceedings to continue without the Skype transmission.

...

The technology for transmission by Skype was now ready so the interpreter translated while sitting beside the person testifying, using the laptop belonging to attorney Schjatvet which had Skype.

...

On Friday 11 January 2019, the appeal proceedings continued in the same location with the same persons present. Ebrima Pa Jallow was not on Skype from the commencement of the day's proceedings, but it was decided that contact would be attempted later.

Attorney Schatvet gave her consent that the proceedings could continue without Ebrima Pa Jallow being on Skype.

...

After the lunch break, Ebrima Pa Jallow came on Skype and was able to follow the proceedings. ..."

39. In its judgment of 11 February 2019, the High Court dismissed the appeals. The High Court concluded that it was not in G.'s best interests that his aunt, A.J., or the applicant be given parental responsibilities for him. After describing the legal framework, the High Court first set out G.'s situation, before turning to the applications of A.J. and the applicant, respectively.

40. In respect of G.'s situation, it stated among other things that G. was well aware of the ongoing dispute about him and that it had been an additional burden on him. According to the expert (see paragraph 27 above), G. needed peace, stability and predictability going forward. He was a child with special needs both in terms of emotional and social development and the expert recommended that he live with people with special skills regarding children and development, care persons who would be particularly sensitive to his signals and able to recognise and interpret his fundamental needs and emotional states. Moreover, the expert reported that G., who was by then nine years old, had found his place in his foster family and called them "mummy, daddy and big brother". He had stated clearly that he wanted to live with them in Norway and the expert considered that removing him from them would represent a risk to his development.

41. The High Court went on to find that it would not be in G.'s best interests for A.J. to be given parental responsibilities for him. In that context it took note that A.J.'s application to be given parental responsibilities had been made on the assumption that she would also have daily care of him. Turning, then, to the applicant's application, the High Court noted that it had become clear that he did not wish to be responsible for the daily care of G. and for G. to move to his home in Gambia. It appeared uncertain to the High Court whether the applicant intended to come to

Norway and claim responsibility for the daily care of G. at a later point in time.

42. Furthermore, the High Court emphasised that as the question before it was whether it would be in G.'s best interests for the applicant to be given parental responsibilities for him without also being given daily care of him, the applicant's parenting skills were not relevant. According to the expert, it would be positive if the applicant gained parental responsibilities for G. provided he did not want G. to move, but otherwise it would in her opinion be unnatural for the applicant to participate in parental-responsibility decisions. A potential future case concerning daily care would be a heavy burden on G., but the expert stated that if the applicant were granted parental responsibilities, she would expect him to maintain a low profile, and to introduce him and his family cautiously. The expert further asserted that what was important to G. at the time was where and with whom he lived. Who had parental responsibilities for him was less important.

43. The High Court stated that it agreed with the expert that it would not have any immediate practical consequences for G. whether or not the applicant was granted parental responsibilities, and that what seemed important was that the applicant become a part of G.'s life in due course, in a way that was useful for G. In the first place, this could be by sending photographs, showing an interest in G.'s daily life, and being there if G. was interested in contact. Gradually they could become better acquainted. Such contact would not depend on the applicant having parental responsibilities.

44. As to parental-responsibility decisions, the High Court noted that the applicant had little knowledge about G. and therefore lacked the qualifications to participate in those decisions in a manner that would be in G.'s best interests. In addition, the geographical and cultural gulf between the applicant and G.'s care provider in Norway would make shared parental responsibilities between the applicant and G.'s guardian difficult.

45. The High Court also stated that it had to be mindful of the fact that the applicant would, were he given parental responsibilities for G., be more easily able to initiate future proceedings concerning G. It referred to the applicant having made different statements about what he wished for G. with regard to where and with whom he was to live. The High Court stated, lastly, that it considered that the Court's judgment in *Gül v. Switzerland* (19 February 1996, *Reports of Judgments and Decisions* 1996-I) did not provide guidance, as the applicant's case concerned only issues of parental responsibilities, not daily care, whereas the case of *Gül* had concerned family reunification.

46. The applicant appealed against the High Court's judgment to the Supreme Court (*Høyesterett*). The Supreme Court's Appeals Committee (*Høyesteretts ankeutvalg*) refused him leave to appeal in a decision of 10 April 2019.

III. JUDICIAL REVIEW OF THE APPLICANT'S VISA DECISIONS SUBSEQUENT TO THE APPLICATION LODGED WITH THE COURT

47. On 4 October 2019 the applicant applied to the City Court for judicial review of the visa decision of 7 January 2019 of the Immigration Appeals Board, that had not been refused revised in, *inter alia*, a decision of 29 May 2019 (see paragraph 34 above) by way of a civil lawsuit against the Norwegian State. He also requested a declaratory judgment holding that there had been a violation of Article 8 of the Convention on the grounds of that decision.

48. The court hearing took place on 5 May 2020, and the City Court delivered its judgment on 10 June 2020. It concluded that the relationship between G. and the applicant did not amount to "family life" within the meaning of Article 8 of the Convention. The visa rejection therefore did not violate Article 8. However, it found that there had been a procedural error in the decision of the Immigration Appeals Board. The Board had originally been under the assumption that the applicant had not documented his family relations in Gambia. This point had been rectified in one of several motions for reversal, but the City Court found that the Immigration Appeals Board had not assessed the case on the correct factual grounds. The decision was therefore found to be invalid.

RELEVANT LEGAL FRAMEWORK

49. Section 38 of the Children Act of 8 April 1981 (*barneloven*), as worded at the time of the facts of the case brought before the Court, provided that parental responsibilities for a child who had lost a parent was transferred to the other parent if the latter already shared parental responsibilities or the child was living with him or her. Section 63 set out at the relevant time that if there was no longer anyone with parental responsibilities for a child, persons who wanted to be given it were to contact the court in the area where the child lived. If only one application to have parental responsibilities was received, the court was to grant the application unless there was a danger of the child not being given adequate care and maintenance, or if he or she would suffer in other ways. If no one applied to have parental responsibilities, or the court dismissed all the applications, the court was to inform the child welfare services in order for them to make a decision on the placement of the child.

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 6 OF THE CONVENTION

50. The applicant complained that the proceedings through which he sought to be granted parental responsibilities for his child were not conducted fairly in violation of Article 6 of the Convention, which reads as follows:

"In the determination of his civil rights and obligations ... everyone is entitled to a fair ... hearing ... by [a] ... tribunal ..."

A. Admissibility

51. The Court observes that the applicant and another relative of G., A.J., both applied before the courts to have parental responsibilities for G. given to them. The Court also notes that G. — through his guardian — opposed the applications from both A.J. and the applicant. In the light of these circumstances, the Court proceeds on the basis that Article 6 of the Convention was applicable in respect of the proceedings that are the subject of the complaint brought before the Court.

52. Furthermore, the Court notes that this complaint is neither manifestly ill-founded nor inadmissible on any other grounds listed in Article 35 of the Convention. It must therefore be declared admissible.

B. Merits

1. The parties' submissions

53. The applicant submitted that he had not only not been allowed to be physically present during the domestic court's hearing, he had also been refused entry to Norway for the purpose of preparing for the hearing and, in that connection, to meet in person with G., the expert witness, the child welfare services and his lawyer. The applicant had thereby also been put at a significant disadvantage *vis-à-vis* G.'s aunt, A.J., who had been allowed to meet G., the expert, the child welfare services and her lawyer in the context of the proceedings before both levels of jurisdiction.

54. Furthermore, the applicant submitted that his not having been granted parental responsibilities for G. had entailed a severing of the biological ties between them since the County Social Welfare Board had thereby become competent to authorise G.'s adoption in accordance with the Child Welfare Act. The applicant's presence in court had been necessary since his personal character and way of life had been in play.

55. The applicant also argued that the reasons the domestic court had given for its judgment were insufficient to demonstrate that the applicant's physical presence had been unnecessary and he pointed out, *inter alia*, that it had not given any reasons as to why it had changed its mind from the position taken in its letter of 22 November 2018 to the Directorate

of Immigration, in which it had argued that the applicant's presence was of great importance both for the elucidation of the application for parental responsibilities and for the equality of arms between the parties. Immigration concerns had no place in the fair-trial assessment.

56. The Government maintained that, as a starting-point, the question was whether the applicant's physical absence from the hearing had deprived him of a reasonable opportunity to have knowledge of and comment on the observations made or evidence adduced by the other party, or whether it had put him at a substantial disadvantage *vis-à-vis* his opponent in presenting his case. Not every disadvantage would lead to an infringement of Article 6 § 1 of the Convention.

57. As to the facts of the instant case, the Government submitted that the applicant had not had an absolute right to be physically present at the hearing. They asserted in that connection that the case differed from that in *Karpenko v. Russia* (no. 5605/04, 13 March 2012), *inter alia* as the domestic proceedings in the applicant's case had, unlike in *Karpenko*, concerned the establishment, not the termination, of parental responsibilities. They also emphasised that in its judgment of 11 February 2019 the High Court had found that the applicant's parental competence had been of no interest to the question of parental responsibilities since he had not lodged an application for the daily care of G.

58. As to the applicant's presence at the court hearings in Norway via Skype, the Government submitted that this had not undermined his position *vis-à-vis* his opponents. They also pointed out that the applicant's counsel had been present in person and had consented to the proceedings continuing on the occasions when the Skype connection had not been working. The High Court's letter of 22 November 2018 in which it had emphasised the importance of the applicant's participation in person had to be read in the light of the fact that it had not at that point in time been clear that the applicant had only lodged an application for parental responsibilities, not the daily care of G.

2. The Court's assessment

59. The Court reiterates that the adversarial principle and the principle of equality of arms, which are closely linked, are fundamental components of the concept of a "fair hearing" within the meaning of Article 6 § 1 of the Convention. They require a "fair balance" between the parties: each party must be afforded a reasonable opportunity to present his case under conditions that do not place him at a substantial disadvantage *vis-à-vis* his opponent or opponents. However, the rights deriving from these principles are not absolute. The Court has already ruled, in a number of judgments, on the particular case in which precedence is given to superior national interests when denying a party fully adversarial proceedings.

The Contracting States enjoy a certain margin of appreciation in this area. However, it is for the Court to determine in the last instance whether the requirements of the Convention have been complied with (see, for example, *Regner v. the Czech Republic* [GC], no. 35289/11, §§ 146–47, 19 September 2017, and the references therein).

60. In the instant case, the Court notes that the background for the applicant's submissions relating to unfairness and inequality of arms is essentially his having been refused an entry visa to Norway. The Court further notes that the decision not to grant the applicant a visa was taken on the basis of public interest considerations, notably relating to immigration control. However, the question before the Court is not whether a visa should have been granted in order to secure the applicant a fair hearing, but whether the hearing was, in the particular circumstances of the case, fair in respect of the applicant, given that he was not allowed to enter Norway in order to be physically present.

61. At the outset the Court cannot but take note that the case before the High Court concerned interests of a personal character for the applicant, and of the fact that the High Court, while preparing the case, sent a letter to the Directorate of Immigration emphasising the need for the applicant's physical presence in order to ensure a fair trial for him (see paragraph 30 above). In particular, the Court observes that, as A.J. had also lodged an application to be given parental responsibilities for G., in its letter the High Court emphasised the need for equality of arms between the parties; the applicant was to be given the opportunity to question A.J. and any witnesses the latter might wish to present, and to be able to discuss with his counsel in that connection, which would be more difficult were he not allowed to be physically present with his counsel in court. In addition, the applicant was to appear before the bench himself and be given the opportunity to give evidence and be questioned. At the time, the High Court considered that giving evidence by Skype would not be the optimal solution (see paragraphs 30–32 above).

62. However, the Court also observes that the High Court, after it had become clear that the applicant would not be allowed entry into Norway, made new and updated assessments, and ultimately considered it acceptable also from the perspective of the applicant's right to a fair hearing to proceed with the scheduled hearing with the applicant present by Skype, and with his lawyer physically present at the hearing. It did so in two decisions of 9 and 10 January 2019 on the basis of considerations which included: G.'s interest in having the matter settled; the fact that more than a year had already passed since the City Court had delivered its judgment; it having been clarified that the applicant was not seeking to have the daily care of G. (something which had not been clear when the court

had first contacted the immigration authorities); and that he would have counsel present to secure his interests (see paragraphs 36 and 37 above).

63. The Court notes that the High Court, since the physical appearance of the applicant was no longer an option, in practice had the choice between postponing the case for an indefinite period with no solution in view, or to facilitate the attendance of the applicant through video-link. In the light of the reasons provided by the High Court, the Court has no basis for criticising the High Court for its choice in this regard. In that respect, the Court emphasises in particular the following factors:

64. Firstly, the High Court itself emphasised the negative sides of postponing the case, notably being at odds with the best interests of G. Moreover, as the Court has held in different contexts, the appearances by video-link are as such not necessarily problematic, as long as this measure in any given case serves a legitimate aim and that the arrangements are compatible with the requirement for due process (see, for example, *mutatis mutandis*, *Dijkhuizen v. the Netherlands*, no. 61591/16, § 53, 8 June 2021; *Bivolaru v. Romania (no. 2)*, no. 66580/12, § 138, 2 October 2018); *Ichetovkina and Others v. Russia*, nos. 12584/05 and 5 others, § 37, 4 July 2017; *Yevdokimov and Others v. Russia*, nos. 27236/05 and 10 others, §§ 41–43, 16 February 2016; and *Marcello Viola v. Italy*, no. 45106/04, §§ 67 and 73–74, ECHR 2006-XI (extracts)).

65. Secondly, the Court recalls that the case before the High Court was ultimately limited to deciding on parental responsibilities only, not the custody for G.; that is, the day-to-day responsibility for him. It transpires from the reasoning in the High Court's judgment that the decision on parental responsibilities in this case did not to a decisive extent depend on the judges' immediate impression of the parties through their physical presence (see paragraphs 39–45 above).

66. Thirdly, the Court takes note of the fact that although the applicant disagreed with the High Court proceeding with the case without him being physically present, it appears that he did not — via his counsel — complain of specific problems during the hearing. Even though some connectivity issues were noted in the court records, they generally show that counsel had no objections to the hearing proceeding (see paragraph 38 above). The Court also notes in this respect that the applicant's representative made no complaints to the High Court that the applicant was unable to communicate confidentially with her during the hearing.

67. Fourthly, the Court emphasises that the applicant participating in the proceedings via Skype, was assisted by his lawyer present at the hearings at all times. Indeed, even though it was technically more complicated for the applicant to, for example, consult with counsel in connection with the questioning of witnesses than had he been in the same

room, he was afforded broad opportunities to present his case (see paragraphs 36 and 37 above).

68. Accordingly, while the Court accepts the applicant's assertion that his lack of physical presence had to some degree entailed that A.J. was *a priori* in an easier situation than him owing to her being physically present, the Court does not find that the technical solution employed placed him at any "substantial disadvantage" as required by the Court's case-law for there to be a violation of Article 6 of the Convention in a case such as the present one, or that he did not have a reasonable opportunity to present his case to the High Court. The Court notes that A.J. was not as such the applicant's opponent in the said proceedings, nor did the High Court find in favour of her.

69. As concerns the applicant's arguments that he could not adequately prepare his case because he was not allowed entry into Norway or because the court-appointed expert reports (see paragraphs 27 and 33 above) had not been translated, the Court observes that the reports were made available ahead of the High Court hearing on 10 and 11 January 2019 and there is nothing to indicate that the applicant was unable to communicate with counsel or others during the case-preparation stage even if he was not able to do so in person at the meetings. The expert who had prepared the reports also attended the High Court's hearing where she elaborated on her reports and was available for questioning (see paragraph 37 above). The Court does not find that these matters give any indication that the trial was unfair.

70. The foregoing considerations are sufficient to enable the Court to conclude that there has been no violation of Article 6 of the Convention.

II. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

71. The applicant complained that the refusal to give him parental responsibilities for G. had violated his right to respect for his family life as provided in Article 8 of the Convention, which reads as follows:

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

72. The Government submitted that the complaint under Article 8 of the Convention was inadmissible *ratione materiae* as there had been no "family life" in the instant case. They also maintained that, as concerned

the substance, the High Court's assessment of the matter had fallen well within the margin of appreciation afforded to member States in a case such as the present one. According to the Government, the applicant's application had not demonstrated how he would be able to provide "care and consideration" for G. while living in Gambia or on what basis he would take decisions for G. in his personal matters and in accordance with his interests and needs.

73. The applicant submitted that there had been family life when G.'s brother T. was born in 1999 and that the family ties had not ceased to exist because the parents had divorced and remarried other people. Exceptional circumstances were required for family life to cease to exist and no such circumstances had been present in this case. In the applicant's view, there had been a violation of Article 8 of the Convention and the Government's arguments were discriminatory in so far as it was the refusal to give the applicant an entry visa that represented the hurdle as to why he could not provide G. with care and exercise his parental responsibilities.

74. The Court reiterates that a biological kinship between a natural parent and a child alone, without any further legal or factual elements indicating the existence of a close personal relationship, is insufficient to attract the protection of Article 8. As a rule, cohabitation is a requirement for a relationship amounting to family life. Exceptionally, other factors may also serve to demonstrate that a relationship has sufficient constancy to create *de facto* "family ties" (see, for example, *A.B.V. v. Russia*, no. 56987/15, § 65, 2 October 2018, and *Anayo v. Germany*, no. 20578/07, § 56, 21 December 2010, with further references). In the instant case, G. is the applicant's biological son. G. was born in Norway in 2011. The applicant has never been to Norway and, based on the information provided to the Court, their relationship consisted principally of the applicant having met G. on the occasion of a two-week holiday of the latter in Gambia when he was aged four and which took place two years before his mother died and four years before the domestic court decisions. In addition to that, the applicant and G. possibly had some telephone contact (see paragraphs 10–11 above). Nevertheless, even assuming that such limited contact would suffice to create *de facto* "family life" within the meaning of Article 8, the Court finds that the complaint is in any event manifestly ill-founded for the following reasons.

75. As concerns the procedural guarantees that flow from Article 8 of the Convention in cases concerning alleged interferences with the right to respect for family life, the Court has found above that the applicant's assertion that the trial was unfair and that he has been the victim of an inequality of arms cannot succeed from the angle of Article 6 (see paragraphs 59–70 above). It does not consider that viewing the procedures from the perspective of Article 8 can lead to a different conclusion.

76. As concerns the substantive decision not to give the applicant parental responsibilities for G., the Court notes that it has to be a fundamental element that the connection between the applicant and G. at the time of the impugned decision was very limited. Taking that as its starting-point, the Court observes that the High Court based its decision not to give the applicant parental responsibilities for G. on considerations which included the fact that parental responsibilities was a separate matter from establishing contact between the applicant and G. — which the High Court does indeed appear to have considered should be done — and that the applicant, given the distance between him and G. and the lack of knowledge about him and his situation — would not have the qualifications to participate in taking the decisions that fall within the competence of the person having parental responsibilities in a way that would be in G.'s best interests (see paragraphs 42–44 above). In the Court's assessment, the reasons provided by the High Court were both relevant and sufficient and there are no indications to suggest that the domestic authorities did not pursue the best interests of the child or failed to strike a fair balance between the competing interests in the case.

77. In the light of the above circumstances, the Court considers that the application discloses no appearance of a violation of Article 8 of the Convention and that the complaint under that provision is manifestly ill-founded within the meaning of Article 35 § 3 (a) and must be rejected in accordance with Article 35 § 4 of the Convention.

FOR THESE REASONS, THE COURT, UNANIMOUSLY,

1. *Declares* the complaint under Article 6 of the Convention admissible, and the complaint under Article 8 inadmissible;

2. *Holds*, unanimously, that there has been no violation of Article 6 of the Convention.

Done in English, and notified in writing on 2 December 2021, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Victor Soloveytchik
Registrar

Síofra O'Leary
President

UKR

www.coe.int

Рада Європи є провідною організацією із захисту прав людини на континенті. Вона нараховує 46 держав-членів, включно з усіма державами – членами Європейського Союзу. Усі держави – члени Ради Європи приєдналися до Європейської конвенції з прав людини – договору, спрямованого на захист прав людини, демократії та верховенства права. Європейський суд з прав людини здійснює нагляд за виконанням Конвенції у державах-членах.

cepej

European Commission for the Efficiency of Justice

Commission européenne pour l'efficacité de la justice

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE