Пам’ятка

щодо особливостей обробки та захисту персональних даних осіб, постраждалих від сексуального насильства, пов’язаного з конфліктом

для використання слідчими, прокурорами, суддями, правозахисниками у практичній діяльності з метою оптимізації процесів розслідування та судового переслідування на національному і міжнародному рівнях

Ця пам'ятка підготовлена науковим та експертним середовищем, за ініціативою та сприяння Офісу Віцепрем'єрки з питань європейської та євроатлантичної інтеграції та за підтримки Фонду ООН в галузі народонаселення UNFPA, реалізовано громадською організацією «UAExperts» для використання слідчими, прокурорами, суддями, соціальними працівниками, правозахисниками у практичній діяльності щодо кваліфікації СНПК та з метою оптимізації розслідування та судового переслідування на національному та міжнародному рівнях.

ЗМІСТ

ВСТУП

Особливого значення тема захисту персональних даних набуває для України під час війни. Коли порушення безпеки персональних даних може мати наслідком не тільки втручання у приватне життя особи, але і спричинити загрозу для її фізичної безпеки і навіть становити загрозу її життю.

В цьому контексті особливу увагу необхідно приділити питанням обробки і захисту персональних даних осіб, постраждалих від сексуального насильства, пов'язаного з конфліктом (СНПК).[1]

З початку повномасштабного вторгнення РФ в Україні офіційно зафіксовано 303 факти сексуального насильства, пов'язаного з конфліктом (СНПК). Реальна цифра осіб, які стали жертвами СНПК, значно більша.

Уповноважений Верховної Ради України з прав людини Дмитро Лубінець наголошує на тому, що СНПК – це грубе порушення одного з фундаментальних прав людини на особисту недоторканність. СНПК може кваліфікуватися не тільки як воєнний злочин, злочин проти людяності чи грубе порушення прав людини, але й бути частиною актів геноциду.[2]

1 Проміжні репарації для постраждалих від сексуального насильства, вчиненого військовослужбовцями Росії. URL: https://ombudsman.gov.ua/news_details/groshova-dopomoga-dlya-postrazhdalih-vid-seksualnogo-nasilstva-vchinenogo-vijskovoslu-zhbovcyami-rosiyi

2 Фонд Global Survivors Fund запускає в Україні проєкт виплати репарацій людям, що постраждали від сексуального насильства, пов'язаного з конфліктом (СНПК). URL: https://www.ukrinform.ua/rubric-society/3852612-postrazdali-vid-seksualnogo-nasilstva-pid-cas-vijni-v-ukraini-otrimaut-reparacii-vid-fondu.html

За словами Генерального прокурора Андрія Костіна: «Постраждалим притаманне почуття сорому за те, що з ними сталося, хоча насправді провина завжди лежить на злочинцеві. Однак потерпілі вкрай рідко самі заявляють про сексуальне насильство. Це заважає правоохоронцям розслідувати такі випадки, а органам прокуратури – представляти звинувачення у суді. Як наслідок – зло залишається непокараним. І це – масове зло, а не поодинокі випадки». [3]

Один із найголовніших моментів, що заважає особам-жертвами СНПК відкрито звертатися до правоохоронних органів і давати свідчення, – страх того, що інформація про злочин стане відомою суспільству.

На думку заступниці голови Представництва Міжнародної організації з міграції (МОМ) в Україні Елізабет Ворн стигматизація постраждалих залишається одним із ключових аспектів, що потребують уваги: «Стигма заважає глибше зануритися у найбільш чутливі аспекти цієї проблеми, зокрема пов'язані з тим, що жертвами насильства стають чоловіки або ветерани. Певні особи потерпають від регулярного ґендерно зумовленого насильства у колі родини, але ці самі особи можуть страждати не лише від ґендерно зумовленого насильства, а й від військових злочинів. Ми маємо чітко визначитись: СНПК – це порушення прав людини, що може зачепити людей з будь-яких сфер життя».[4]

Як наголосила Регіональна координаторка з питань біженців Посольства США в Україні Рене Ларів'єр, за відсутності належних механізмів реагування, конфлікт ніколи не закінчиться для постраждалих від СНПК: «Вони повинні отримати спеціалізовану допомогу, зокрема правову, медичну, економічну та психосоціальну підтримку. Також необхідно продовжувати дискусію у суспільстві, яке повинно усвідомити, що таке насильство трапляється і важливо створити умови для всебічного реагування на нього». [5]

Пам'ятка щодо особливостей обробки та захисту персональних даних осіб, постраждалих від сексуального насильства, пов'язаного з конфліктом (далі – Пам'ятка), має стати прикладним інструментом для органів державної влади, особливо правоохоронних органів та суддів, у їх взаємодії з особами, які постраждали від СНПК. Інструментом, який при належному застосуванні на практиці дасть змогу побудувати міст довіри між державою і особою, що стала жертвою СНПК.

---

3 В Офісі Генерального прокурора створено управління, яке займатиметься розслідуванням фактів сексуального насильства, вчиненого російськими військовими в Україні. URL: https://www.ukrinform.ua/rubric-ato/3579034-v-ogp-stvorili-upravlinna-z-rozsliduvanna-seksualnih-zlociniv-armii-rf-v-ukraini.html

4 Сексуальне насильство в умовах конфлікту та міжнародний досвід: дискусія за сприяння МОМ шукала відповіді на чутливі питання. URL: https://ukraine.iom.int/uk/news/seksualne-nasylstvo-v-umovakh-konfliktu-ta-mizhnarodnyy-dosvid-dyskusiya-za-spryyannya-mom-shukala-vidpovidi-na-chutlyvi-pytannya

5 Сексуальне насильство в умовах конфлікту та міжнародний досвід: дискусія за сприяння МОМ шукала відповіді на чутливі питання. URL: https://ukraine.iom.int/uk/news/seksualne-nasylstvo-v-umovakh-konfliktu-ta-mizhnarodnyy-dosvid-dyskusiya-za-spryyannya-mom-shukala-vidpovidi-na-chutlyvi-pytannya

ЗАГАЛЬНІ ПОЛОЖЕННЯ ЩОДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Міжнародно-правові зобов'язання України у сфері захисту персональних даних

Підготовка Пам'ятки обумовлена тим, що дотримання найвищих стандартів захисту персональних даних у правоохоронній галузі має першочергове значення для дотримання безпеки і захисту прав кожного громадянина, зокрема права на приватність.

Гармонізація українського законодавства з європейськими стандартами у сфері захисту персональних даних шляхом імплементації Регламенту Європейського парламенту та Ради про захист фізичних осіб в зв'язку з обробкою персональних даних і про вільний рух таких даних 2016/679 (Загальний регламент про захист персональних даних) є одним із ключових завдань України відповідно пункту 11 Плану заходів з виконання Угоди про асоціацію, затвердженого постановою Кабінету Міністрів України від 25 жовтня 2017 р. № 1106.

Крім того, Україна є стороною Конвенції про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108). У травні 2018 року Рада Європи прийняла Протокол CETS № 223, яким було внесено зміни до Конвенції 108. Модернізована Конвенція 108+ враховує більшість викликів, спричинених розвитком інформаційних і комунікаційних технологій, та посилює вимоги щодо її імплементації. Таким чином, перед Україною постало питання ратифікації вказаного Протоколу, та

приведенням законодавства у відповідність до вимог оновленої Конвенції 108+.

Угода про асоціацію між Україною та Європейським Союзом вимагає приведення законодавства України у відповідність до європейських стандартів, що стосується також сфери захисту персональних даних. Так, розділом III Угоди про асоціацію передбачається співробітництво у сфері юстиції, свободи та безпеки. Згідно зі статтею 15 Угоди про асоціацію «Україна та Європейський Союз погодились співпрацювати з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів, зокрема відповідних документів Ради Європи».

Угодою про співробітництво між Україною та Європейською організацією з питань юстиції (ратифікована у 2017 році), а саме статтею 11, Україна взяла на себе зобов'язання щодо гарантій рівня захисту персональних даних, еквівалентному тому, що випливає із застосування принципів, які містяться у Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року і наступних змін до неї, а також принципів, закладених у Рішенні щодо Євроюсту та у Регламенті Євроюсту щодо захисту даних.

Угода між Україною та Європейським поліцейським офісом (Європол) про оперативне та стратегічне співробітництво, ратифікована у 2017 році зобов'язує Сторони надавати одна одній лише ту інформацію, що зібрана, зберігається і передається відповідно до правових актів Європейського Союзу та отримана без порушень чинного законодавства ЄС щодо захисту прав людини. У цьому контексті Європол буде зобов'язаний статтею 20(4) Рішення Ради Європейського Союзу від 30 листопада 2009 року про прийняття імплементаційних правил, які регулюють відносини Європолу з партнерами, включаючи обмін персональними даними та інформацією з обмеженим доступом.

Укладання угод про співробітництво між Україною та Європолом і Євроюстом сприятиме розширенню формату співпраці, обміну оперативною інформацією і необхідним досвідом, а також підвищенню ефективності роботи українських правоохоронних органів у боротьбі з тяжкими злочинами.

Національне законодавство у сфері захисту персональних даних

Важливим кроком у розвитку сфери захисту персональних даних стало прийняття в 1996 році Конституції України. В статті 32 Конституції України зазначається, що «ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини».

До 2010 року захист персональних даних на законодавчому рівні розвивався фрагментарно в рамках конституційного, цивільного та інформаційного права. У 2010 році, з метою реалізації положень Конституції та наближення законодавства України до

стандартів Ради Європи, було прийнято Закон України «Про захист персональних даних», який до сьогодні залишається базовим актом у національному регулюванні сфери захисту персональних даних. Цей Закон в цілому розроблений відповідно до положень Директиви 95/46/ЄС та регламентує функціонування системи захисту персональних даних в Україні.

Набрання чинності Законом України «Про захист персональних даних» від 2010 року стало важливою передумовою для ратифікації Україною Конвенції Ради Європи № 108 та Додаткового протоколу до неї. Після ратифікації Конвенції Ради Європи № 108 Україна зобов'язується дотримуватися принципів і стандартів Ради Європи щодо обробки та передачі персональних даних.

У Конвенції Ради Європи № 108 викладено ключові принципи обробки персональних даних, права особи у зв'язку з обробкою її персональних даних, базові норми щодо їх транскордонної передачі та окремо виділено «чутливі» категорії персональних даних. Додатковий протокол деталізує положення Конвенції в частині транскордонної передачі даних та містить нові положення щодо необхідності створення Учасниками Конвенції наглядового органу, який би здійснював контроль за додержанням законодавства про захист персональних даних на національному рівні.

Закон України «Про захист персональних даних» – це правова основа для регулювання відносин, які стосуються передачі та обробки особистих даних, забезпечуючи при цьому захист прав і свобод особи. У зв'язку з новизною, різноманітністю та складністю проблеми захисту персональних даних, вони повинні розглядатися як найважливіші елементи регулювання інформаційних відносин у зазначеній сфері.

Метою захисту персональних даних є забезпечення за допомогою законодавчих, регуляторних і організаційних заходів гарантій захисту прав та інтересів особи під час передачі та обробки її особистих даних.

В Законі України «Про захист персональних даних» персональні дані визначаються як «відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована». Таке визначення є достатньо лаконічним і чітким та відповідає існуючим міжнародним підходам до розуміння цього поняття.

Ключовим у наведеному визначенні також є поняття «ідентифікованої особи або особи, яка може бути ідентифікована». У зв'язку з цим потрібно зазначити, що ідентифікованою особа вважається, якщо її можна безпомилково виділити серед інших. Зазвичай для того, щоб вважати особу ідентифікованою, необхідні її ім'я, прізвище, по батькові та реквізити документа, що посвідчує особу/цифровий номер, що присвоюється особі (наприклад, ідентифікаційний номер фізичної особи). Однак, за певних умов наявність меншої кількості інформації чи певного об'єму іншої інформації є достатніми для того, щоб ідентифікувати особу. Також фотографія особи чи відеозапис з участю особи є інформацією достатньою для того, щоб ідентифікувати особу.

ЩО НАЛЕЖИТЬ ДО ПЕРСОНАЛЬНИХ ДАННИХ

Важливим моментом, особливо в контексті СНПК, є також характер даних про особу, що оприлюднюються. Так, чим чутливішими є дані, тим більшим буде ступінь втручання в право особи на повагу до її приватності. Саме тому із загального переліку персональних даних виділяються спеціальні, чутливі категорії персональних даних, до яких належать персональні дані про:

- расове або етнічне походження;
- політичні, релігійні або світоглядні переконання;
- членство в політичних партіях та професійних спілках;
- засудження до кримінального покарання;
- дані, що стосуються здоров'я, статевого життя, а також біометричні або генетичні дані.

Обробка персональних даних – «будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем».

Обробка персональних даних щодо особи, яка постраждала від СНПК, є обробкою, що становить особливий ризик для прав і свобод суб'єктів персональних даних. Така обробка персональних даних вважається «чутливою».

Важливо зазначити, що відповідно до статті 6 Конвенції Ради Європи 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних»: «Персональні дані, що свідчать про расову приналежність, політичні, релігійні чи інші переконання, а також дані, що стосуються здоров'я або статевого життя, не можуть піддаватися автоматизованій обробці, якщо внутрішнє законодавство не забезпечує відповідних гарантій. Це правило також застосовується до персональних даних, що стосуються засудження в кримінальному порядку».

Принципи обробки персональних даних

Під час обробки персональних даних осіб, які постраждали від сексуального насильства, пов'язаного з конфліктом, варто обов'язково дотримуватися основних принципів щодо конфіденційності і захисту персональних даних. [6]

ПРИНЦИПИ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

6 Лілія Олексюк та Андрій Ніколаєв. «Принципи захисту персональних даних та ризики їх порушення при використанні технології зв'язку 5G» URL: http://perspectives.pp.ua/index.php/vp/article/view/807/809

ПРИНЦИП ПЕРШИЙ: «ЗАКОННІСТЬ, ПРАВОМІРНІСТЬ І ПРОЗОРІСТЬ».

Персональні дані повинні оброблятися у законний, правомірний і прозорий спосіб відносно до суб'єкта даних («законність, правомірність і прозорість»). Будь-яка обробка персональних даних має бути законною та справедливою. До фізичної особи має бути прозоро донесено те, що її персональні дані збираються, використовуються, переглядаються або іншим чином обробляються, а також те, в якому обсязі персональні дані обробляються або будуть оброблятися.

Передбачено необхідність інформування суб'єктів персональних даних про особу володільця, про цілі (мету) обробки персональних даних, а також додаткове інформування для забезпечення справедливої та прозорої обробки даних в частині, що стосується відповідних фізичних осіб і права на отримання підтвердження, та відомостей про ті персональні дані, які обробляються на їх основі.

ПРИНЦИП ДРУГИЙ: «ОБМЕЖЕННЯ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ МЕТОЮ»

Персональні дані можуть збиратися лише для конкретних, чітких і законних цілей і не повинні оброблятися в подальшому у спосіб, що є несумісним із визначеними цілями («конкретність цілей»). Мета обробки обов'язково має бути чітко визначеною до початку обробки. Необхідно переконатися, що дії, які планується здійснювати з персональними даними, є цілком законними. Також мета має бути задокументована, тобто прописана у відповідних документах, які регламентують обробку (порядок обробки, політика конфіденційності тощо).

Можна обробляти персональні дані з іншою метою тільки якщо вона сумісна з початковою метою, або отримано згоду суб'єкта на обробку з новою метою, або обробка необхідна для виконання зобов'язання, встановленого законом, або обробка здійснюється для реалізації повноважень, встановлених законом.

ПРИНЦИП ТРЕТІЙ: «МІНІМІЗАЦІЯ ОБСЯГУ ДАНИХ»

Персональні дані повинні бути адекватними, відповідними і ненадмірними, та обмежуватися тим, що є необхідним для цілей, з якими вони обробляються («мінімізація персональних даних»). Можна виділити такі показники:

- дані є адекватними, якщо вони є достатніми для досягнення мети обробки;
- дані є відповідними, якщо вони мають раціональний зв'язок із метою обробки та сприяють її досягненню;
- дані є ненадмірними, якщо їх обсяг не більший, ніж це необхідно для досягнення мети обробки;
- не можна збирати дані «про всяк випадок».

ПРИНЦИП ЧЕТВЕРТИЙ: «ОБМЕЖЕННЯ ЗБЕРІГАННЯ ПЕРСОНАЛЬНИХ ДАНИХ В ЧАСІ»

Персональні дані не повинні зберігатися довше, ніж вони потрібні для цілей, для яких ці дані обробляються («обмеження строків зберігання»). Після того, як мета була досягнута, персональні дані повинні бути знищені або знеособлені. Знеособлені персональні дані - це дані, зі складу яких вилучили усі відомості, та які вже не дають змогу будь-яким чином ідентифікувати конкретну особу - суб'єкта персональних даних. Персональні дані можуть зберігатися протягом більш тривалого часу винятково для досягнення цілей суспільних інтересів, наукового чи історичного дослідження або статистичних цілей за умов вжиття відповідних технічних і організаційних заходів, передбачених законодавством, для гарантування прав і свобод суб'єкта даних.

ПРИНЦИП П'ЯТИЙ: «ЦІЛІСНІСТЬ ТА КОНФІДЕНЦІЙНІСТЬ»

Персональні дані повинні оброблятися таким чином, щоб забезпечити їх цілісність та конфіденційність.

Персональні дані повинні оброблятися таким чином, щоб забезпечити належний рівень безпеки та конфіденційності цих персональних даних, у тому числі для запобігання несанкціонованому доступу або несанкціонованого використання персональних даних та обладнання, що використовується для обробки.

Володільці та розпорядники зобов'язані вживати технічні та організаційні заходи безпеки, на рівні, що відповідає законодавчим вимогам.

ПРИНЦИП ШОСТИЙ: «ТОЧНІСТЬ»

Персональні дані мають бути точними, достовірними та оновлюватися, якщо це необхідно для мети їх обробки («точність»). Необхідно вживати всіх раціональних заходів для того, щоб забезпечити точність персональних даних, які обробляються, а також усіх відповідних заходів для того, щоб неточні персональні дані було негайно видалено або виправлено.

ПРИНЦИП СЬОМИЙ: «ПІДЗВІТНІСТЬ»

Володілець несе відповідальність за дотримання принципів обробки персональних даних та має бути здатним це довести («підзвітність»). Обов'язок доведення дотримання цих принципів покладається на володільця.

Організаційні та технічні заходи захисту персональних даних

Під час обробки персональних даних особи, яка постраждала від СНПК, володільцю персональних даних (фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки) необхідно забезпечити захист персональних даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних. Володілець персональних даних вживає заходів щодо забезпечення захисту персональних даних на всіх етапах їх обробки, у тому числі за допомогою організаційних та технічних заходів.

ДО ОСНОВНИХ ОРГАНІЗАЦІЙНИХ ЗАХОДІВ МОЖНА ВІДНЕСТИ:

В контексті СНПК необхідно визначити наступні організаційні заходи:

- визначити правові підстави для обробки та її мету;
- визначити порядок обробки і захисту персональних даних;
- визначити порядок доступу до персональних даних працівників володільця/розпорядника;
- визначити порядок ведення обліку операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них;
- розробити план дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій;
- регулярно навчати співробітників, які працюють з персональними даними;
- отримати від осіб, які обробляють таку чутливу інформацію, письмове зобов'язання про нерозголошення.

З метою дотримання безпеки обробки персональних даних вживаються технічні заходи захисту, у тому числі щодо виключення несанкціонованого доступу до персональних даних, що обробляються, та роботі технічного та програмного комплексу, за допомогою якого здійснюється обробка персональних даних.

Для того, щоб контролювати цей процес та здійснювати обробку персональних даних законно й прозоро, потрібно упорядкувати цю роботу за допомогою відповідних внутрішньорозпорядчих документів.[7]

7 Захист персональних даних: роз'яснення для суб'єктів владних повноважень від Уповноваженого Верховної Ради України з прав людини. URL: https://ombudsman.gov.ua/storage/app/media/27012023/37676120-9a08-47d9-a376-b498d-d07ede5.pdf

ДО ПЕРЕЛІКУ ВНУТРІШНЬО-РОЗПОРЯДЧИХ ДОКУМЕНТІВ МОЖНА ВІДНЕСТИ:

1. Порядок обробки персональних даних
2. Загальна внутрішня інструкція роботи з персональними даними, де визначені чіткі вимоги для персоналу, залежно від їхніх повноважень щодо роботи з даними.
3. Правила здійснення внутрішнього контролю за процесами обробки даних
4. Правила роботи зі знеособленими даними
5. Перелік місць зберігання матеріальних носіїв персональних даних
6. Посадові інструкції осіб, відповідальних за організацію обробки даних, де буде також міститися зобов ' язання про нерозголошення персональних даних
7. Правила щодо передачі персональних даних третім особам або їх поширення

Вагома роль у забезпеченні захисту персональних даних відводиться обов'язку володільця здійснювати облік операцій (реєстр операцій), пов'язаних з обробкою персональних даних. Згідно з Типовим порядком обробки персональних даних з цією метою володільцем/розпорядником зберігається інформація про дату, час та джерело збирання персональних даних суб'єкта.

РЕЄСТР ПОВИНЕН ВКЛЮЧАТИ ІНФОРМАЦІЮ ПРО:

1. Правові підстави та джерела збору даних
2. Цілі обробки даних
3. Види та категорії персональних даних, що збираються
4. Перелік осіб, які мають доступ до даних та беруть участь в їх обробці
5. Перелік третіх осіб, кому було або буде розкрито дані, включаючи треті країни або міжнародні організації, а також законні підстави та цілі надання інформації
6. Строки зберігання та видалення даних
7. Організаційні заходи безпеки даних

В цьому контексті варто відзначити, що згідно з положеннями статті 32 Загального Регламенту з захисту персональних даних ЄС (GDPR) контролер (прим. володілець) і процесор (прим. розпорядник) зобов'язані «впроваджувати належні технічні й організаційні заходи», враховуючи «останні досягнення технічного прогресу й витрати на таке впровадження», а також «характер, межі, обставини й цілі обробки, і ризики й загрози для прав і свобод фізичних осіб».

Загальний Регламент з захисту персональних даних ЄС містить положення щодо видів захисних заходів, які можуть розглядатися «виходячи з наявних ризиків», в тому числі:

- псевдонімізацію й шифрування персональних даних;
- здатність постійного забезпечення конфіденційності, цілісності, доступності та стійкості систем і послуг з обробки;

- здатність своєчасного відновлення доступу до персональних даних у випадку технічної несправності обладнання;
- процедуру регулярного тестування, оцінки й аналізу ефективності технічних і організаційних заходів задля забезпечення захисту даних під час обробки.

Загальний Регламент з захисту персональних даних ЄС вимагає від контролера (прим. володілець) і процесора (прим. розпорядник) впровадження належних технічних і організаційних заходів для забезпечення пропорційності рівня захисту персональних даних наявним ризикам, забезпечуючи конфіденційність та надійність систем обробки даних та застосування процедур з регулярної перевірки ефективності цих заходів.

Крім того, відповідно до вимог національного законодавства, має бути призначено відповідальну особу, яка організовує роботу, пов'язану із захистом персональних даних під час їх обробки. Відомості про відповідальну особу, а також про обробку персональних даних, які становлять особливий ризик для прав і свобод суб'єктів персональних даних, необхідно повідомити Уповноваженому Верховної Ради України з прав людини.

ВІДПОВІДАЛЬНА ОСОБА ІЗ ЗАХИСТУ ДАНИХ

Закон в окремих випадках вимагає призначати відповідальних осіб або навіть структурний підрозділ, який має контролювати процес обробки персональних даних та їх захист. Наприклад, у європейському Регламенті (GDPR) така посада називається — Data Protection Officers (DPO).

До основних завдань відповідальної особи із захисту персональних даних входять:

- аналіз діяльності та контроль за проведенням заходів щодо захисту персональних даних;
- ведення обліку процесів обробки даних;
- розробка та підтримання в актуальному стані відповідної внутрішньої документації;
- здійснення оцінки ризиків та внутрішнього контролю за дотриманням законодавства про захист персональних даних;
- організація приймання та розгляд звернень (запитів) суб'єктів персональних даних, а також запитів третіх осіб та Уповноваженого Верховної Ради України з прав людини;

- організація і проведення службових перевірок за фактами порушень вимог до обробки та
- захисту персональних даних;
- підготовка органу до перевірок контролюючих інстанцій;
- взаємодія з Уповноваженим Верховної Ради України з прав людини, іншими державними органами контролю та неурядовими громадськими організаціями у питаннях забезпечення прав, свобод і законних інтересів громадян.

Під час обробки персональних даних осіб, які постраждали від сексуального насильства, пов'язаного з конфліктом, важливо дотримуватися керівних принципів щодо конфіденційності, поваги та недискримінації, а також завжди дотримуватися правила «не нашкодь».

Необхідно чітко усвідомлювати, що розголошення «чутливих» персональних даних:

- може спричинити непередбачувані наслідки для особи, зокрема, втручання у приватне життя, загрожувати її особистій безпеці (в тому числі її здоров'ю та життю, соціальним комунікаціям тощо);
- є порушенням законодавства;
- передбачає адміністративну (стаття 188-39 Кодексу України про адміністративні правопорушення) або кримінальну (статті 182, 145, 387 Кримінального кодексу України) відповідальність.

НАЦІОНАЛЬНІ ЗАКОНОДАВЧІ ІНІЦІАТИВИ ЩОДО СНПК

Проект Закону про облік осіб, життю та здоров'ю яких завдано шкоди внаслідок збройної агресії Російської Федерації проти України (законопроєкт № 10256)

25 квітня 2024 року Верховна Рада України прийняла у першому читанні проєкт Закону про облік осіб, життю та здоров'ю яких завдано шкоди внаслідок збройної агресії Російської Федерації проти України.

Законопроєкт розроблено з метою забезпечення створення Державного реєстру осіб, постраждалих внаслідок збройної агресії Російської Федерації проти України (далі – Реєстр постраждалих осіб), в якому здійснюватимуться:

1) облік громадян, життю та здоров'ю яких завдано шкоди внаслідок збройної агресії Російської Федерації проти України;

2) інформаційні обміни між державними інформаційними системами в частині обмінів інформацією про фіксацію шкоди життю та здоров'ю громадян, якої було завдано внаслідок збройної агресії Російської Федерації проти України;

3) облік видатків державного та місцевих бюджетів, бюджетів соціальних фондів, пов'язаних з наданням допомоги та підтримки громадянам, які постраждали внаслідок збройної агресії Російської Федерації проти України.

Відповідно до частини третьої статті 4 цього законопроекту[8]: «Сукупність відомостей про фізичних осіб (персональні дані), що містяться в реєстрі, є інформацією з обмеженим доступом. Обробка цих відомостей здійснюється з дотриманням вимог Закону України «Про захист персональних даних».

Варто підкреслити, що відповідно до статті 6 Закону України «Про доступ до публічної інформації» інформацією з обмеженим доступом є[9] :

1) конфіденційна інформація
(інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов);

2) таємна інформація
(інформація, яка містить державну, професійну, банківську, розвідувальну таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю);

3) службова інформація
(інформація, що міститься в документах суб'єктів владних повноважень, які становлять внутрішньовідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень).

Перелік відомостей, що становлять службову інформацію, який складається органами державної влади, органами місцевого самоврядування, іншими суб'єктами владних повноважень, у тому числі на виконання делегованих повноважень, не може бути обмеженим у доступі.

Важливо відзначити, що згідно зі статтею 8 Закону України «Про захист інформації в інформаційно-комунікаційних системах»[10] «Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності комплексної системи захисту інформації здійснюється за результатами державної експертизи, яка проводиться з урахуванням галузевих вимог та норм інформаційної безпеки у порядку, встановленому законодавством».

8 Проєкт Закону № 10256 «Про облік осіб, життю та здоров'ю яких завдано шкоди внаслідок збройної агресії Російської Федерації проти України» від 13.11.2023. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/43188

9 Закон України «Про доступ до публічної інформації» URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text

10 Закон України «Про захист інформації в інформаційно-комунікаційних системах». URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

Проєкт Закону про статус осіб, постраждалих від сексуального насильства, пов'язаного зі збройною агресією Російської Федерації проти України, та невідкладні проміжні репарації (законопроєкт № 10132)[11]

19 червня 2024 року Верховна Рада України ухвалила рішення щодо прийняття за основу законопроєкту №10132, який передбачає підтримку та відновлення прав постраждалих від сексуального насильства внаслідок російської збройної агресії.

Цим законопроєктом пропонується на законодавчому рівні визначити правовий статус осіб, постраждалих від сексуального насильства, пов'язаного зі збройною агресією Російської Федерації проти України, та членів сімей загиблих (померлих) таких осіб, а також правові основи надання їм невідкладних проміжних репарацій.

Проєкт закону визначає порядок обліку інформації про таких осіб та захист їхніх персональних даних, зокрема інформації про особисте та сімейне життя. Відповідні дані пропонується вносити до Державного реєстру осіб, постраждалих внаслідок збройної агресії Російської Федерації проти України, який створюватиметься на підставі окремого закону.

Стаття 8 законопроєкту про статус осіб, постраждалих від сексуального насильства, пов'язаного зі збройною агресією Російської Федерації проти України, та невідкладні проміжні репарації містить наступні положення:

(1) Персональні дані та інформація про постраждалих осіб та членів сім'ї загиблої (померлої) постраждалої особи фіксуються в Державному реєстрі осіб, постраждалих внаслідок збройної агресії Російської Федерації проти України.

(2) Збирання, накопичення, захист, облік, відображення, оброблення такої інформації та персональних даних осіб, визначених в частині першій цієї статті, здійснюється з метою фіксації інформації про шкоду життю та здоров'ю, сприяння наданню невідкладних проміжних репарацій, та забезпечення можливості подальшого відшкодування такої шкоди за рахунок репарацій чи інших стягнень з Російської Федерації, в тому числі в рамках реалізації концепції спеціального компенсаційного механізму відшкодування збитків, завданих збройною агресією Російської Федерації проти України.

(3) Державний реєстр осіб, постраждалих внаслідок збройної агресії Російської Федерації проти України, створюється на підставі закону.

Стаття 9 законопроекту про статус осіб, постраждалих від сексуального насильства, пов'язаного зі збройною агресією Російської Федерації проти України, та невідкладні проміжні репарації передбачає, що:

(1) персональні дані, інформація про особисте та сімейне життя, особистість постраждалих осіб, членів сім'ї загиблої (померлої) постраждалої особи, а також осіб, які звернулися із заявою у порядку, передбаченому статтями 6, 7 цього Зако-

11 Проект Закону № 10132 «Про статус осіб, постраждалих від сексуального насильства, пов'язаного зі збройною агресією Російської Федерації проти України, та невідкладні проміжні репарації» від 09.10.2023 URL: https://itd.rada.gov.ua/billInfo/Bills/Card/42862

ну, віднесені до конфіденційної інформації про особу та повинні охоронятися суб'єктами відносин, пов'язаними із персональними даними.

(2) Обробка та користування персональними даними осіб, визначених частиною першою цієї статті, здійснюються з дотриманням вимог Конституції України, Закону України «Про захист персональних даних».

(3) Обробка відомостей про фізичних осіб, що містяться в Державному реєстрі осіб, постраждалих внаслідок збройної агресії Російської Федерації проти України, здійснюється з дотриманням вимог Закону України «Про захист персональних даних», «Про публічні реєстри», «Про захист інформації в інформаційно комунікаційних системах».

(4) Особи, винні у розголошенні персональних даних осіб, визначених у частині першій цієї статті, та посадові особи, винні у порушенні вимог цього Закону, несуть кримінальну, адміністративну та іншу відповідальність, передбачену законодавством.

Проєкт Закону про внесення змін до Кримінального процесуального кодексу України щодо удосконалення порядку здійснення досудового розслідування та судового розгляду у кримінальних провадженнях щодо злочинів, які пов'язані із сексуальним насильством, яке вчинене в умовах збройного конфлікту (законопроект № 9351)[12]

Метою законопроєкту є удосконалення порядку розслідування та судового розгляду справ щодо сексуального насильства, вчиненого в умовах збройної агресії Російської Федерації проти України, забезпечення конфіденційності потерпілих під час досудового розслідування та судового розгляду вказаної категорії справ.

Питання недопущення ретравматизації та вторинної віктимізації жертв СНПК є одним з найважливіших для роботи з такими потерпілими. З цією метою законопроєктом пропонується доповнити статтю 27 Кримінального процесуального кодексу України такою нормою: «Розгляд слідчим суддею заяв, клопотань та скарг у кримінальному провадженні щодо злочинів, які пов'язані із сексуальним насильством, яке вчинене в умовах збройного конфлікту, а також судовий розгляд кримінальних проваджень цієї категорії, здійснюється у закритому судовому засіданні, крім випадків, коли суд за письмовим клопотанням потерпілого прийме рішення про кримінальне провадження у відкритому судовому засіданні». Це обумовлено закріпленими у міжнародних протоколах стандартами «не завдавати шкоди», поваги до потерпілих, поваги до автономії потерпілих, забезпечення конфіденційності.

12 Ірина Гловюк. Проєкт Закону України 9351 від 05.06.2023 та орієнтація на постраждалих від СНПК». URL: https://www.hsa.org.ua/lectors/glovyuk-iryna/articles/projekt-zakonu-ukrayini-9351-vid-05062023-ta-orijentaciia-na-postrazdalix-vid-snpk

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ОСІБ, ПОСТРАЖДАЛИХ ВІД СЕКСУАЛЬНОГО НАСИЛЬСТВА, ПОВ'ЯЗАНОГО З КОНФЛІКТОМ, У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Відповідно до положень статті 104 Кримінального процесуального кодексу України (далі – КПК), яка встановлює вимоги щодо оформлення протоколів, у вступній частині протоколу мають бути зазначені прізвища, імена, по батькові, дати народження, місця проживання всіх осіб, які присутні під час проведення процесуальної дії.

На практиці, в протоколах слідчих дій, особливо в протоколах допиту учасників кримінального провадження, часто зазначають також контактні номери телефонів, відомості про документ, за допомогою якого встановлено особу-учасника слідчої дії тощо, хоча законодавство прямої вимоги про це не містить. Таку інформацію також можна віднести до персональної, оскільки вона може сприяти ідентифікації особи-учасника кримінального провадження. А отже, вся перелічена вище персональна інформація про будь-якого учасника кримінального провадження підлягає захисту.

Способи захисту персональних даних осіб, постраждалих від СНПК, у кримінальному провадженні

По-перше, варто зауважити, що будь-яка інформація у кримінальному провадженні захищена таємницею досудового розслідування.

Так, відповідно до частини 1 статті 222 КПК, відомості досудового розслідування можна розголошувати лише з письмового дозволу слідчого або прокурора і в тому обсязі, в якому вони визнають можливим. Згідно із частиною 2 вказаної статті слідчий, прокурор попереджає осіб, яким стали відомі відомості досудового розслідування, у зв'язку з участю в ньому, про їх обов'язок не розголошувати такі відомості без його дозволу. Незаконне розголошення відомостей досудового розслідування тягне за собою кримінальну відповідальність, встановлену законом.

Відповідно до положень Кримінального кодексу України (далі – КК) така відповідальність установлена статтею 387 «Розголошення даних оперативно-розшукової діяльності, досудового розслідування».

По-друге, до постраждалих осіб можна застосовувати положення Закону України «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві» (далі – Закон), якщо вони набули статусу свідка, потерпілого чи іншого учасника кримінального провадження.

Стаття 7 вказаного Закону передбачає такі заходи забезпечення безпеки:

а) особиста охорона, охорона житла і майна;

б) видача спеціальних засобів індивідуального захисту і сповіщення про небезпеку;

в) використання технічних засобів контролю і прослуховування телефонних та інших переговорів, візуальне спостереження;

г) заміна документів та зміна зовнішності;

д) зміна місця роботи або навчання;

е) переселення в інше місце проживання;

є) поміщення до дошкільної виховної установи або установи органів соціального захисту населення;

ж) забезпечення конфіденційності відомостей про особу;

з) закритий судовий розгляд.

Вказаний перелік не є вичерпним.

Найбільш швидким у застосуванні, економічно доступним, достатньо ефективним і таким, що захищає персональні дані учасника кримінального провадження, можна назвати такий захід забезпечення безпеки, як забезпечення конфіденційності відомостей про особу.

Відповідно до статті 15 Закону, яка безпосередньо регулює питання забезпечення конфіденційності даних про особу, нерозголошення відомостей про осіб, взятих під захист, може здійснюватися шляхом:

а) обмеження відомостей про особу в матеріалах перевірки (заявах, пояснен-

нях тощо), а також протоколах слідчих дій та інших матеріалах кримінального провадження, заміни прізвища, імені, по батькові в цих документах псевдонімами за постановою органу, що здійснює оперативно-розшукову діяльність, слідчого, дізнавача, прокурора або за ухвалою слідчого судді, суду про зміну анкетних даних. Ці постанови (ухвали) до матеріалів справи не приєднуються, а зберігаються окремо в органі, у провадженні якого знаходиться кримінальне провадження;

б) проведення упізнання особи поза візуальним та аудіоспостереженням того, кого впізнають, з дотриманням вимог кримінального процесуального законодавства;

в) неоголошення будь-яким способом дійсних анкетних даних про осіб, які взяті під захист і підлягають виклику в судове засідання;

г) виклику до суду цієї особи виключно через орган, який здійснює заходи безпеки;

д) накладення тимчасової заборони на видачу відомостей про особу, взяту під захист, адресними бюро, паспортними службами, підрозділами державтоінспекції, довідковими службами АТС та іншими державними інформаційно-довідковими службами.

Найбільше складнощів на практиці викликають положення пункту "а" частини 1 статті 15 Закону, адже право прийняти рішення про застосування забезпечення конфіденційності відомостей про особу у кримінальному провадженні надано одразу слідчому, дізнавачу, прокурору, слідчому судді та суду, а постанови чи ухвали про такі рішення, відповідно до вказаної норми, мають зберігатися тільки в органі, який здійснює досудове розслідування у відповідному кримінальному провадженні. Крім того, серед практиків зустрічається різне розумінням де саме «окремо» в органі досудового розслідування мають знаходитися ці постанови чи ухвали та як, власне, обмежити відомості про захищену особу в матеріалах кримінального провадження чи замінити її персональні дані.

Також варто звернути увагу, що закон розділяє обмеження відомостей про особу та заміну її персональних даних. Під обмеженням відомостей мається на увазі нерозголошення частини інформації, відображеної в протоколі слідчої дії (місця проживання, дати народження тощо). Але необхідно враховувати, що в окремих ситуаціях це може бути неефективним, бо ми живемо в епоху цифрових технологій та незаконних ресурсів, які продають персональні дані.

Заміна персональних даних (прізвища, імені, по батькові, в будь-якому випадку будуть замінені відомості про дату народження та місце проживання) на псевдонім видається більш ефективним способом захисту.

Але як це реалізувати?

Відповідно до пункту 4.1.6 наказу Служби безпеки України від 23 грудня 2020 р. № 383 «Про затвердження Зводу відомостей, що становлять державну таємницю» (далі – ЗВДТ) *«відомості про зв'язок ознак особи, яка бере участь у кримінальному судочинстві і взята під захист згідно з чинним законодавством України у зв'язку з виникненням загрози її життю чи*

здоров'ю і стосовно якої проводяться або проведено заходи щодо зміни персональних даних або зовнішності чи місця проживання, з її попередніми індивідуальними ознаками, мають бути захищені грифом секретності «цілком таємно».

Отже, рішення (постанова) про застосування до постраждалої особи (учасника/учасниці кримінального провадження) заходу забезпечення безпеки, передбаченого статтею 15 Закону, має бути «цілком таємним», а процесуальні документи зі справжніми даними особи, до якої застосовано відповідний захід забезпечення безпеки, мають бути вилучені з матеріалів кримінального провадження та зберігатися в режимно-секретному відділі (частині) органу досудового розслідування (дізнання) разом із постановою чи ухвалою, якою прийнято відповідне рішення (долучити ці документи до «цілком таємної» справи можна на підставі рапорту). Замість вилучених процесуальних документів мають бути виготовлені аналогічні, але замість справжніх персональних даних особи, до якої застосовано відповідний захід забезпечення безпеки, будуть вказані вже вигадані. Хоча на практиці частіше до особи спочатку застосовують заходи забезпечення безпеки, а потім проводять з нею слідчі та процесуальні дії, тому такі «підміни» документів трапляються не часто.

Крім того, іноді практикують виготовлення одночасно процесуальних документів зі справжніми анкетними даними учасника кримінального провадження, до якого застосовано забезпечення конфіденційності відомостей про особу, та які зберігаються в режимно-секретному відділі (частині) разом із цілком таємною постановою, ухвалою, та окремо – аналогічні процесуальні документи, де зазначають псевдонім взятої під захист особи.

Крім того, варто звернути увагу, що пунктом 4.1.6 ЗВДТ звужує коло осіб, наділених повноваженням прийняти «цілком таємне» рішення про заміну персональних даних на псевдонім у кримінальному провадженні, передбачаючи лише органи досудового розслідування (дізнання). В такому випадку використання прокурором вказаного пункту ЗВДТ також не буде вважатись порушенням, хоча потрібно визнати, що ЗВДТ в цій частині потребує доопрацювання.

Окремо варто зауважити, що стаття 3 Закону поділяє органи, які забезпечують безпеку учасників кримінального судочинства, на ті, що приймають рішення про застосування заходів безпеки, та ті, що здійснюють заходи безпеки.

Так, рішення про застосування заходів безпеки приймається слідчим, дізнавачем, прокурором, судом, у провадженні яких знаходяться кримінальні провадження щодо кримінальних правопорушень, у розслідуванні чи судовому розгляді яких брали або беруть участь особи, зазначені у статті 2 цього Закону.

Здійснення заходів безпеки покладається за підслідністю на органи служби безпеки, Державного бюро розслідувань, органи внутрішніх справ, органи Національної поліції або Національне антикорупційне бюро України, у складі структур яких з цією метою створюються спеціальні підрозділи. Безпеку осіб, яких беруть під захист, якщо кримінальні провадження знаходяться у

провадженні Бюро економічної безпеки України або суду, забезпечує за їх рішенням відповідно орган служби безпеки, Державного бюро розслідувань, орган внутрішніх справ, орган Національної поліції, Національне антикорупційне бюро України або орган чи установа виконання покарань, слідчий ізолятор. Безпеку особи, взятої під захист, якщо її тримають в установі виконання покарань чи слідчому ізоляторі, забезпечує відповідний підрозділ такої установи чи слідчого ізолятора незалежно від того, у провадженні якого органу знаходиться кримінальне провадження.

У статті 22 Закону, яка регулює порядок прийняття рішення про застосування заходів безпеки, вказано, що орган, який здійснює оперативно-розшукову діяльність, слідчий, дізнавач, прокурор, слідчий суддя, суд, одержавши заяву або повідомлення про загрозу безпеці учаснику кримінального судочинства, зобов'язані перевірити цю заяву (повідомлення) і в строк не більше трьох діб, а у невідкладних випадках – негайно, прийняти рішення про застосування або про відмову у застосуванні заходів безпеки. Для забезпечення такого рішення приймається мотивована постанова чи ухвала і передаються для виконання органу, на який покладено здійснення заходів безпеки. Ця постанова чи ухвала є обов'язковою для виконання вказаними органами.

Орган, якому доручено здійснення заходів безпеки, встановлює перелік необхідних заходів і способів їх реалізації, керуючись при цьому конкретними обставинами справи і необхідністю усунення існуючої загрози.

Таким чином, слідчому, прокурору чи суду не обов'язково одразу приймати рішення про застосування якогось конкретного заходу забезпечення безпеки. Конкретний захід забезпечення безпеки можуть обрати оперативні підрозділи органів, що перелічені в статті 3 Закону (зазвичай це орган, який здійснює оперативне супроводження конкретного кримінального провадження), і в буквальному розумінні норм Закону це може бути і такий захід, як забезпечення конфіденційності відомостей про особу.

Разом з тим, якщо слідчий або прокурор в одному рішенні (постанові) приймуть рішення про застосування заходу забезпечення безпеки особи (задовольнивши заяву особи, яка про це звернулась, та засвідчивши, що для цього є підстави), одночасно визначивши, що таким заходом буде саме забезпечення конфіденційності відомостей про особу, це не буде вважатись помилкою.

Необхідно відзначити, що закінчення досудового розслідування кримінального провадження, зокрема у формі звернення до суду з обвинувальним актом, не є автоматичною підставою для скасування вже застосованих заходів безпеки. Під час судового розгляду кримінального провадження реальна загроза життю, здоров'ю, житлу і майну таких осіб об'єктивно продовжує існувати, адже показання учасників кримінального провадження, у тому числі тих, до яких застосовано заходи безпеки, суд повинен сприймати безпосередньо (стаття 23 КПК). Водночас, у такому випадку можуть виникнути труднощі з процедурою допиту, впізнання чи іншими видами процесуальних дій з особами, до яких застосовано забезпечення конфіденційності їхніх даних.

Як уже було зазначено, процесуальні документи, у яких вказано справжні персональні дані особи, мають зберігатися в режимно-секретному відділі органу досудового розслідування (прокуратури), захищені грифом «цілком таємно». Допоки заходи забезпечення безпеки у кримінальному провадженні не скасовані, підстави для розсекречення відповідних матеріальних носіїв інформації відсутні – адже саме державна таємниця у цьому випадку є гарантією безпеки захищених осіб. Відтак, виникає питання: яким чином суд має проводити процесуальні дії з учасниками кримінального провадження, до яких застосовано положення стаття 15 Закону України «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві», встановлювати особу, приводити її до присяги, попереджати про відповідальність за завідомо неправдиві показання (стаття 384 КК) тощо.

Так, можливість допитувати свідків зі зміненими анкетними даними передбачена у пункті "в" частини 1 статті 15 Закону України «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві», який, серед іншого, гарантує неоголошення будь-яким способом дійсних анкетних даних про осіб, які взяті під захист і підлягають виклику в судове засідання. Крім того, пункт 9 частини 2 статті 65 КПК забороняє допитувати свідків, до яких застосовані заходи безпеки, щодо дійсних даних про їх особи.

Проведення інших процесуальних дій у режимі відеоконференції під час судового провадження урегульовано положеннями статті 336 КПК.

Вказані гарантії можуть бути реалізовані шляхом застосування частини 9 статті 352 КПК, згідно із якою у виняткових випадках для забезпечення безпеки свідка, який підлягає допиту, суд за власною ініціативою або за клопотанням сторін кримінального провадження чи самого свідка постановляє вмотивовану ухвалу про проведення допиту свідка з використанням технічних засобів з іншого приміщення, у тому числі за межами приміщення суду, або в інший спосіб, що унеможливлює його ідентифікацію та забезпечує сторонам кримінального провадження можливість ставити запитання і слухати відповіді на них. У тому випадку, якщо існує загроза ідентифікації голосу свідка, допит може супроводжуватися створенням акустичних перешкод. Разом із тим, перед постановленням відповідної ухвали суд зобов'язаний з'ясувати наявність заперечень сторін кримінального провадження проти проведення допиту свідка в умовах, що унеможливлюють його ідентифікацію, та в разі їх обґрунтованості – відмовити у проведенні допиту свідка в порядку, визначеному вказаною нормою.

Надалі можна скористатися таким алгоритмом допиту учасника кримінального провадження, до якого застосовано забезпечення конфіденційності відомостей про особу:

1) у разі заявлення прокурором клопотання про виклик до суду для участі у процесуальних діях учасника кримінального провадження, до якого застосовано забезпечення конфіденційності відомостей про особу, суд покладає на сторону обвинувачення обов'язок виклику і доставлення такої особи до суду, у тому числі шляхом

винесення ухвали, якою задовольняє клопотання прокурора та зобов'язує орган, який забезпечує безпеку особи, доставити її до приміщення суду, який суддя визначає для здійснення дистанційного провадження;

2) вирішуючи питання про визначення суду для дистанційного провадження, суд має враховувати наявність у штаті такого суду секретарів судового засідання з допуском до державної таємниці не менше другої форми («цілком таємно», що відповідає пункту 4.1.6 ЗВДТ), а також приміщення, що відповідає вимогам режимно-секретного відділу (це можуть бути місцеві суди, які відповідають заявленим вимогам, або суди апеляційної інстанції, які в такому випадку залучаються виключно для окремих процесуальних дій);

3) маючи відомості щодо суду, з якого буде відбуватись допит свідка зі зміненими анкетними даними, та отримавши інформацію про секретаря, якому необхідно буде відкрити матеріали кримінального провадження, які містять відомості, що становлять державну таємницю, прокурору відповідно до вимог частини 4 статті 517 КПК необхідно вжити заходів щодо видання наказу або письмового розпорядження про надання доступу до конкретної таємної інформації та її матеріальних носіїв (документи щодо застосування до конфідента заходу забезпечення безпеки – забезпечення конфіденційності відомостей про особу) конкретному секретарю судового засідання;

4) прокурор вживає заходів для виконання ухвали про допит взятого під захист учасника кримінального провадження в дистанційному режимі шляхом направлення листа та копії ухвали до органу досудового розслідування, де зберігається цілком таємна інформація про справжні персональні дані такого учасника, або звертається до режимно-секретної частини органу прокуратури, якщо вказані матеріали зберігаються у прокуратурі, та забезпечує направлення до режимно-секретної частини суду, з якого відбуватиметься участь у процесуальних діях з використанням технічних засобів, за допомогою фельд'єгерського чи іншого виду спеціального зв'язку матеріалів, у яких зафіксовано застосування до учасника провадження забезпечення конфіденційності відомостей про особу, вказано справжнє ім'я та псевдонім такого учасника відповідно;

5) відкриваючи судове засідання, у якому буде брати участь особа зі зміненими анкетними даними, головуючий суддя має роз'яснити учасникам кримінального провадження, що: (а) така особа буде допитана з іншого приміщення із використанням технічних засобів; (б) особа такого учасника провадження буде перевірена секретарем судового засідання, який має допуск до державної таємниці і доступ до матеріальних носіїв секретної інформації, у яких зафіксовано справжні персональні дані такої особи; (в) такого учасника провадження буде приведено секретарем до присяги у випадках і порядку, передбачених КПК;

6) секретар судового засідання, який забезпечує участь у процесуальних діях особи, взятої під захист, з використанням технічних засобів з іншого приміщення, перед початком процесуальної дії має ознайомитися з рішенням, яким особі змінено справжні анкетні дані, та встановити їх відповідність даним особи, яка доставлена для участі у процесуальних діях; вручити цій особі пам'ятку про її права та обов'язки відповідно до процесуального статусу; допускається в письмовому порядку приведення такої особи під справжніми анкетними даними у випадках і порядку, передбачених КПК; роз'яснити такій особі, що вона не повинна відповідати на питання, що можуть зашкодити її безпеці; про проведені вищевказані дії з такою особою секретар доповідає суду до початку участі особи в процесуальних діях під час судового засідання, а також повідомляє інформацію про програмно-технічне забезпечення, яке буде використано під час проведення цієї процесуальної дії; присутність у кімнаті, з якої процесуальну дію буде проведено дистанційно, будь-яким особам, крім учасника кримінального провадження, до якого застосовано заходи безпеки, та секретаря – заборонено;

По-третє, 30.05.2023 Генеральним прокурором підписано Наказ № 141 «Про затвердження Порядку організації публікації в засобах масової інформації загальнодержавної сфери розповсюдження та на офіційному вебсайті Офісу Генерального прокурора повісток про виклик, повідомлень про підозру та відомостей щодо підозрюваних, стосовно яких надано дозвіл на здійснення спеціального досудового розслідування», у частині 4 розділу III якого зазначено, що у повідомленні про підозру, яке публікується на офіційному вебсайті Офісу Генерального прокурора, не може розголошуватися (знеособлюється) інформація про потерпілого та свідка, яка дає можливість ідентифікувати особу (прізвище, ім'я, по батькові, дата і місце народження, адреса (місце) проживання або перебування, номери телефонів чи інших засобів зв'язку, адреси електронної пошти, реєстраційні номери облікової картки платника податків, реквізити документів, що посвідчують особу, реєстраційні номери транспортних засобів, номери банківських рахунків, номери платіжних карток тощо).

Процесуально це можна оформити постановою слідчого, прокурора, наприклад, «про використання зашифрованих даних, а також про недопустимість розголошення відомостей досудового розслідування та шифрування даних про обставини вчинення кримінального правопорушення» (можуть бути інші варіанти назви).

Такий спосіб «шифрування» даних є законним і не впливає на допустимість доказів, що засвідчено у постанові Верховного Суду від 10.06.2024 у справі № 727/5573/20: «... орган досудового розслідування вчинив дії, які не передбачено нормами Кримінального процесуального кодексу України та Положенням про порядок ведення Єдиного реєстру досудових розслідувань, а саме – виніс постанови про використання зашифрованих даних, а також про недопустимість розголошення відомостей досудового розслідування та шифрування даних про обставини вчинення кримінального правопорушення, суд касаційної інстанції враховує нижченаведене.

Частиною 3 статті 110 Кримінального процесуального кодексу України передбачено, що рішення слідчого, дізнавача, прокурора приймається у формі постанови. Постанова виноситься у випадках, передбачених цим Кодексом, а також коли слідчий, дізнавач, прокурор визнає це за необхідне.

У зв'язку з викладеним суд касаційної інстанції відхиляє доводи захисників про те, що жодною нормою Кримінального процесуального кодексу України не передбачено винесення вказаних постанов, оскільки такі постанови слідчого відповідають загальним положенням, передбаченим частинами 1, 3 статті 110 Кримінального процесуального кодексу України.

Крім того, суд касаційної інстанції вважає за потрібне зазначити, що законодавець не може врахувати всі потреби практики, які виникають під час досудового розслідування, а тому цілком обґрунтовано дозволив виносити постанови, які прямо не передбачені законом, однак які слідчий чи прокурор визнали необхідними. Процесуальне рішення слідчого є законним, обґрунтованим та вмотивованим».

Забезпечення справедливого правосуддя у кримінальному провадженні за участі осіб, постраждалих від СНПК, а також гарантії їхньої безпеки

Важливі гарантії дотримання прав тих, кого держава взяла під захист у кримінальному провадженні, містяться також у Кримінальному кодексі України (КК).

Так, у Розділі XVIII КК передбачено два склади кримінальних правопорушень, пов'язаних із забезпеченням безпеки осіб, які беруть участь у кримінальному судочинстві: стаття 380 «Невжиття заходів безпеки щодо осіб, взятих під захист» та стаття 381 «Розголошення відомостей про заходи безпеки щодо особи, взятої під захист».

Крім того, Рекомендація Rec (2005) 9 Комітету Міністрів Ради Європи державам-членам щодо захисту свідків та осіб, які співпрацюють з правосуддям, ухвалена 20.04.2005 на 924-у засіданні заступників міністрів, для своїх цілей дає визначення важливих у контексті анонімізації свідків та потерпілих понять:

- «свідок» означає будь-яку особу, що володіє інформацією, істотною для кримінального провадження, про яку вона дала та (або) може дати свідчення в його рамках (незалежно від того, за якими нормами національного права визначається статус такої особи та форма таких свідчень – прямі чи непрямі, усні чи письмові), і не охоплена визначенням «особа, яка співпрацює з правосуддям»;

- «особа, яка співпрацює з правосуддям» означає будь-яку особу, переслідувану або засуджену за участь у злочинному співтоваристві, або в будь-якій іншій злочинній організації, або в злочинах, вчинених організованою злочинністю, яка, однак, погоджується співробітничати з органами кримінального правосуддя, зокрема даючи показання проти злочинної асоціації або організації, або щодо якого-небудь правопорушення, що має зв'язок з організованою злочинністю або з іншими тяжкими злочинами;
- «анонімність» означає, що ознаки, які уможливлюють ототожнення особи свідка, як правило, не розголошуються ні протилежній стороні, ні суспільству в цілому.

Досить чіткі критерії для прийняття рішення про надання свідкові анонімності у кримінальному провадженні встановлює Рекомендація Rec (2005) 9 Комітету Міністрів Ради Європи державам-членам щодо захисту свідків та осіб, які співпрацюють з правосуддям:

«18. Будь-яке рішення про надання свідкові статусу анонімного в кримінальному провадженні повинно ухвалюватися відповідно до норм внутрішньодержавного права і європейського права щодо прав людини.

19. Анонімність особам, які здатні надати докази, у тих випадках, коли вона передбачена й не суперечить нормам внутрішньодержавного права, потрібно надавати як виняток. У випадках, коли гарантій анонімності вимагає свідок та/або їх одержує тимчасово за рішенням компетентних органів, кримінальний процес має передбачати процедуру перевірки, що дозволяє зберігати справедливий баланс між вимогами кримінального правосуддя й правами сторін. Сторонам завдяки цій процедурі потрібно дати можливість оспорити твердження про необхідність надання свідкові анонімності, надійність свідка і джерело походження його відомостей.

20. Будь-яке рішення про надання анонімності необхідно ухвалювати в тому випадку, коли компетентний судовий орган вважає, що життю або свободі відповідної особи або її близьких існує серйозна загроза, що його показання, очевидно, є суттєво важливими, а його особистість заслуговує довіри.

21. У випадку надання анонімності засудження не має ґрунтуватися винятково або вирішальною мірою на доказах, отриманих від анонімних свідків».

Важливим джерелом європейських стандартів у цьому аспекті є також практика Європейського суду з прав людини (ЄСПЛ). Так, на шляху європеїзації вітчизняного кримінального процесу одним із обов'язкових кроків було прийняття Закону України «Про виконання рішень та застосування практики Європейського Суду з прав людини» № 3477-IV від 23.02.2006, який врегулював відносини, що виникають у зв'язку з обов'язком держави виконати рішення ЄСПЛ у справах проти України, з необхідністю усунення причин порушення Україною Конвенції про захист

прав людини і основоположних свобод (КЗПЛ) і протоколів до неї, з упровадженням в українське судочинство та адміністративну практику європейських стандартів прав людини, зі створенням передумов для зменшення числа заяв до ЄСПЛ проти України.

Враховуючи, що з моменту прийняття вказаного закону рішення ЄСПЛ стали невід'ємною частиною законодавства, яким керуються правоохоронці та судді під час розслідування і розгляду кримінальних проваджень відповідно, доречно згадати рішення, які регламентують використання конфіденційних співробітників під час розслідування злочинів, особливо тих, до яких застосовані правила анонімності.

Крім того, аналіз рішень ЄСПЛ дозволяє нам виокремити ряд критеріїв, за умови дотримання яких показання «таємних свідків» (відповідно до українського законодавства – учасників кримінального провадження, до яких застосовано такий захід забезпечення безпеки як конфіденційність відомостей про особу), будуть вважатися належними та допустимими доказами.

В аспекті забезпечення справедливого правосуддя та уникнення повторної травматизації потерпілих особливу увагу для нас становлять такі гарантовані КЗПЛ права, як право підозрюваного, обвинуваченого на справедливий суд, передбачене статтею 6 КЗПЛ, право постраждалої особи на життя, гарантоване статтею 2 КЗПЛ, право на повагу до приватного і сімейного життя, гарантоване статтею 8 КЗПЛ.

Так, згідно із частиною 1 статті 6 КЗПЛ, 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 або встановить обґрунтованість будь-якого висунутого проти нього кримінального обвинувачення. Відповідно до частини 3 цієї статті кожний обвинувачений у вчиненні кримінального правопорушення має такі права: допитувати свідків обвинувачення або вимагати, щоб їх допитали, а також вимагати виклику й допиту свідків захисту на тих самих умовах, що й свідків обвинувачення (пункт d).

Так, КЗПЛ не виключає можливості використання на ранніх стадіях досудового розслідування анонімних показань у тих випадках, коли цього вимагає характер злочину, що розслідується. Однак подальше використання таких джерел судом для засудження особи в кримінальному порядку – це зовсім інше питання: воно допустиме лише за наявності адекватних і достатніх гарантій відсутності зловживань.

Отже, щоб запобігти порушенням статті 6 КЗПЛ, допускаючи «анонімних свідків» (потерпілих), ЄСПЛ напрацював ряд критеріїв, які забезпечать справедливість судового розгляду:

- *засудження не може ґрунтуватись виключно чи переважною мірою на показаннях, які сторона захисту не може заперечити на будь-якій стадії розгляду справи* (рішення ЄСПЛ у справах «Доорсон проти Нідерландів», «Аль-Хавайя і Тахєрі проти Сполученого Королівства», «Шачашвілі проти Німеччини»);

- *надання підсудному відповідної та належної можливості заперечувати докази свідка обвинувачення і допитати його або під час надання останнім своїх показань, або пізніше* (рішення ЄСПЛ у справах «Люді проти Швейцарії», «Аш проти Австрії», «Якуба проти України», «Леас проти Естонії», «Колесник проти України», «Карпюк проти України», «Рудніченко проти України»);
- *анонімність свідка має бути виправдана вагомими причинами* (рішення ЄСПЛ у справі «Корнєв і Карпенко проти України», «Люді проти Швейцарії» та інші.

МІЖНАРОДНО-ПРАВОВІ СТАНДАРТИ ЗАХИСТУ І ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ ОСІБ, ПОСТРАЖДАЛИХ ВІД СНПК

Анн Адамська-Галлант[13], керівниця компоненту «Судова реформа» Проєкту ЄС "Право-Justice", відзначає: «Важливим інструментом для справедливого та ефективного правосуддя щодо злочинів сексуального насильства, пов'язаного з війною, став Міжнародний протокол із документування та розслідування сексуального насильства в конфлікті. Він викладає основні принципи документування сексуального насильства як однієї з форм тяжких порушень міжнародного гуманітарного права. Документ використовують юристи, правоохоронці, медичні працівники та неурядові організації під час збору доказів для розслідування цих жахливих злочинів в різних країнах».

Правильне документування сексуального насильства, пов'язаного з конфліктом та звірствами, базується на ретельному процесі планування документування: спланувати процес документування сексуального насильства, пов'язаного з конфліктом та звірствами, означає продумати та організувати усі види діяльності, необхідні для досягнення конкретної мети щодо відповідальності.[14]

Міжнародний протокол із документування та розслідування сексуального насильства в умовах конфлікту[15-16]

Ключовий етичний принцип, що лежить в основі документування сексуального насильства, пов'язаного з конфліктом та звірствами, — зобов'язання, щонайменше, не завдавати шкоди. Це означає, що спеціалісти-практики повинні повністю усвідомлювати можливі негативні наслідки документування таких свідчень для постраждалих та інших

13 Анн Адамська-Галлант та Ольга Срібняк. Трибунал по Югославії та кодекс Мурад: міжнародний досвід у роботі з потерпілими від сексуального насильства під час війни. URL: https://lb.ua/blog/pravo_justice/561223_tribunal_yugoslavii_kodeks.html

14 Міжнародний протокол із документування та розслідування сексуального насильства в конфлікті: план документування. URL: https://www.hsa.org.ua/blog/mizhnarodnyj-protokol-iz-dokumentuvannya-ta-rozsliduvannya-seksualnogo-nasylstva-v-konflikti-plan-dokumentuvannya

15 Міжнародний протокол із документування та розслідування сексуального насильства в конфлікті: план документування. Друге видання березень 2017 року. URL: https://nmc-vfpo.com/wp-content/uploads/2022/05/mizhnarodnyj-protokol-iz-dokumentuvannya-ta-rozsliduvannya-seksualnogo-nasylstva-v-konflikti-2017_compressed.pdf

16 Міжнародний протокол із документування та розслідування сексуального насильства в конфлікті: план документування. Перше видання червень 2014 року. URL: https://www.wicc.net.ua/media/int_protokol.pdf

свідків, ширшої спільноти та самих слідчих, бути готовими до шкоди, яку можуть завдати такі наслідки, і вживати заходів, щоб запобігти такій шкоді або мінімізувати її.

Слідчі повинні пам'ятати, що безпека та гідність тих, хто вижив, складають основу всього процесу документування. Це означає забезпечення пріоритетності їх потреб та прохань у процесі документування, особливо коли йдеться про питання безпеки. Водночас, ризик додаткової шкоди повинен балансуватися необхідністю врахування бажання потерпілого розповісти свою історію, віднайти правосуддя та отримати відшкодування збитків.

Дотримання принципу «не завдати шкоди» не повинно автоматично інтерпретуватися як причина не здійснювати документування сексуального насильства, пов'язаного з конфліктом та звірствами. Навпаки, воно може прокласти шлях до безпечного та етичного надання постраждалим можливості бути почутими, одночасно визначаючи можливі механізми підтримки для них. Це, в першу чергу, означає повагу та підтримку потерпілих.

Показання

Показання потерпілих/свідків – це, найчастіше, найдоступніший для практиків тип інформації, але це також інформація, до якої треба підходити з найбільшою обережністю. Потерпілі/свідки можуть надавати практикам критично важливу інформацію про сам напад – або переживши його, або ставши йому свідком – але вони можуть надати інформацію і про контекстні елементи, що супроводжували напад, та про злочинців і їхнє залучення до злочинних діянь, про які йдеться. "Перегляд" таких свідків, як лікарі, медичні сестри, консультанти та місцеві лідери, які можуть інформацію щодо багатьох потерпілих/свідків, часу та місця діянь, має особливе значення для встановлення контекстних елементів потенційно скоєних злочинів.

Інформована згода

Дотримання принципу "інформованої згоди" має вирішальне значення під час збору інформації про сексуальне насильство, незалежно від характеру отриманої інформації. Усі потерпілі та свідки повинні дати свою інформовану згоду на проведення інтерв'ю та огляду, на фотографування, на те, що їхня інформація буде записуватися, що їх буде перенаправлено до будь-яких сервісів підтримки, а також що їхня інформація та контактні дані можуть передаватися третім особам.

Отримання інформованої згоди свідків до документування інформації гарантує те, що потерпілий/свідок зберігатиме повний контроль і владу над власним досвідом і що він буде добре обізнаним і добровільним учасником процесу здійснення правосуддя. Неотримання інформованої згоди порушує права потерпілого/свідка, свідчить про неповагу до нього та завдає йому шкоди. Результати інтерв'ю, проведених без забезпечення належної та інформованої згоди, також можуть не прийняті в певних судових процесах на тій підставі, що інформація була надана в межах якогось тиску або примусу, чи на основі оманливих запевнень.

Інформована згода є не лише основоположним принципом участі в процесі здійснення правосуддя, це – етичне зобов'язання будь-кого, хто збирає інформацію у потерпілих/свідків про злочини в межах міжнародного права, в тому числі щодо грубих порушень прав людини.

ЗГОДА

Згода повинна мати три обов'язкові ознаки:

- добровільність: відсутність прямого чи опосередкованого примусу під час надання згоди. Суб'єкт може відкликати свою згоду в будь-який час;
- поінформованість: перед наданням згоди суб'єкт повинен отримати достовірну інформацію про те, хто і з якою метою буде обробляти його персональні дані, кому будуть передаватися дані, які саме дані (склад даних) будуть передаватися, а також інформацію щодо його прав, визначених законодавством. Така інформація повинна бути надана суб'єкту в доступному вигляді, а володілець даних повинен бути готовим за будь-яких умов надати підтвердження, що така інформація була наданим ним суб'єкту;
- довільність форми: форма надання згоди може бути будь-якою, однак однозначність згоди не повинна викликати сумнівів, а володілець даних повинен бути готовим підтвердити її наявність протягом усього часу проведення обробки персональних даних."

Значення інформованої згоди

Усі особи, які надають інформацію про сексуальне насильство або дають згоду на збір даних, повинні бути поінформовані та розуміти наступне:

- мету та зміст роботи зі збору даних;
- смисл конфіденційності та як вона застосовується чи не застосовується до наданої інформації;
- процедури, які будуть проводитися, в тому числі – можлива необхідність розкриття в подальшому наданої інформації та способи її використання;
- ризики та переваги для учасників збору даних.

Для того, щоб забезпечити інформовану згоду, практики повинні:

1. **Виділити час, щоб пояснити потерпілим/свідкам усі відповідні умови:**
   - Назвіть присутніх членів команди, їхні функції, на кого вони працюють і для кого здійснюється збір інформації.
   - Повністю поясніть мету та характер роботи зі збору інформації, а також склад, приналежність і мандат команди.

- Опишіть всі можливі способи використання наданої інформації, в тому числі можливість того, що інформацію потрібно буде розкрити, незалежно від типу провадження в межах якого особа погоджується дати свідчення.
- Наведіть типи питань, які можуть задати потерпілому/свідку.
- Презентуйте інформацію таким чином, щоб вона була зрозумілою потерпілому/свідку, та переконайтеся, що потерпілий/свідок її зрозумів. З цією метою може бути корисним попросити потерпілого/ свідка озвучити що саме він/вона зрозуміли щодо процесу.

2. Переконайтеся, що згода, надана потерпілим/свідком, ґрунтується на його власній волі

- Створюйте ситуації справжньої довіри, які дозволять потерпілому/свідку вільно та добровільно погоджуватися або почуватися достатньо комфортно, щоб відмовити. Деякі пропозиції щодо того, як на практиці досягти необхідного рівня довіри, викладені в Додатку 3 "Інтерв'ю: основоположні принципи й основні практичні поради".
- Чітко поясніть потерпілому/свідку, що у нього є вибір – говорити з практиком чи ні – та що цим вибором можна скористатися в будь-який час протягом усього процесу.
- Використовуйте авторитет вашої позиції як практика з обережністю та взаємодійте з потерпілим/свідком з повагою.
- Переконайтеся в тому, що потерпілий/свідок має достатньо часу, щоб прийняти рішення. При цьому необхідно враховувати значні та складні наслідки участі у процесі для потерпілих, їхніх сімей та громад як на цей час, так і в майбутньому. Потрібно також розуміти складність для потерпілого/свідка задачі з оцінки ризиків, знаходячись у вразливій ситуації та в мінливих умовах конфлікту.
- Кожного разу, коли ви спілкуєтеся із потерпілим/свідком, підтверджуйте у нього чи не змінив він свою думку з приводу використання його заяв або передачі інформації третім особам.
- Виберіть мову, яку легко зрозуміти потерпілому/свідку, зокрема, забезпечте надання потерпілому/свідку будь-які письмових документів для заповнення його рідною мовою.
- Використовуйте перекладачів, компетентних у дослівному перекладі, переконайтеся, що вони повною мірою розуміють вимоги інформованої згоди.

3. Отримати чітку згоду на конкретні заходи

- Згода має бути надана на використання під час інтерв'ю таких пристроїв, як магнітофон або відеокамера. Переконайтеся в тому, що потерпілий/свідок знає, що ведеться аудіо- або відеозапис.
- Потерпілі/свідки повинні надати чітку згоду на передачу особистих даних, контактів і основної інформації третім сторонам, зокрема національним або міжнародним слідчим або організаціям, судам і поліції.

4. Під час опитування дітей забезпечте належну згоду на надання свідчень

- Усі діти повинні давати свою згоду на участь в опитуванні.
- Отримання інформованої згоди дитина має проводитися з урахуванням її віку, потреб та рівня розуміння (наприклад, інформовану згоду осіб, молодших 18 років, як правило, отримують у їхніх батьків, однак старші підлітки можуть самі давати інформовану згоду).
- Забезпечте інформовану згоду батьків або опікунів дитини на її участь.
- Враховуйте, що діти можуть не мати сміливості виступити та поділитися подробицями з батьками або опікунами; цілком можливо, що ні діти, ні опікуни чи батьки не усвідомлювали, що дитина піддавалася сексуальному насильству.
- Діти повинні бути поінформовані про ризики, пов'язані з наданням інформації, з урахуванням необхідності не налякати їх. Перед початком будь-якого інтерв'ю з дитиною рекомендується провести окрему бесіду з опікунами або батьками без присутності дитини.
- Підготовлений персонал, ознайомлений з індивідуальними особливостями дітей, має представити їм усі можливі варіанти опитування та їх можливі наслідки. Діти мають право знати які права вони мають відповідно до Конвенції ООН про права дитини та Декларації щодо основних принципів правосуддя для жертв злочинів і зловживання владою. Практики зобов'язані ретельно пояснювати дітям що саме відбувається на кожному етапі процесу опитування та що від них очікують.

Конфіденційність

Конфіденційність є етичним принципом документування сексуального насильства, який вимагає щоб практики захищали отриману ними чутливу інформацію та застосовували цей принцип протягом усього періоду документування. Дотримання умов конфіденційності часто є необхідним для того, щоб сформувати в потерпілого/свідка довіру до практиків. Проте, існують певні обмеження конфіденційності, які треба чітко роз'яснити постраждалому/свідку. Зокрема, практики повинні:

1. Переконатися, що всі члени команди розуміють і застосовують параметри конфіденційності, встановлені для роботи з документування, та не обговорюють деталі справи з рідними, друзями або колегами, які не є членами команди.

2. Забезпечити впровадження заходів із захисту інформації щодо всієї отриманої інформації про потерпілого/свідка та його показань, а також будь-яких варіантів перенаправлення або захисних заходів.

3. Повністю та зрозуміло пояснити потерпілим/свідкам умови та обмеження конфіденційності, а саме:

- які заходи конфіденційності вживатимуться (якщо такі є) та як буде захищена їхня інформація;
- обмеження конфіденційності, що забезпечуються збирачами інформації, в тому числі різницю між практичними заходами щодо збереження конфіденційності інформації та неспроможністю забезпечити конфіденційність як законне право.
- що конфіденційність може бути порушена, якщо виникає ризик самогубства/самоушкодження потерпілого/свідка або необхідність захистити дитину.
- межі конфіденційності, включаючи конкретні алгоритми розкриття інформації, якщо потерпілий/свідок дасть згоду на те, щоб отримана від нього інформація могла передаватися третім особам, в тому числі поліції, слідчим і судам.

Інтерв'ю

Після ідентифікації потерпілих та свідків їх інтерв'ювання є найпоширенішим і часто найкориснішим методом збору інформації. Однак з цим методом пов'язані і найбільші ризики можливого негативного впливу на добробут, створення додаткових ризиків, і, якщо це здійснюється неналежним чином, негативний вплив на якість і надійність наданої інформації.

Іноді інтерв'ювання потерпілих/свідків не є необхідним і не рекомендується. Практики повинні бути в змозі чітко обґрунтувати необхідність проведення інтерв'ю.

Для проведення інтерв'ю практики повинні мати відповідну підготовку та спеціальний досвід інтерв'ювання потерпілих/свідків сексуального насильства. Зокрема, проводячи інтерв'ю з дітьми, практики повинні вміти належним чином реагувати на індивідуальні потреби та особливості дитини.

Пам'ятайте, що інформована згода – це процес: вибір, який потерпілий/свідок робить до, під час і після інтерв'ю, повинен ґрунтуватися на його повній поінформованості. Якщо ви не впевнені чи потерпілий/свідок вас цілком зрозумів, попросіть його пояснити якусь частину інформації своїми словами.

Запис інформації під час інтерв'ю

При опитуванні потерпілих/свідків і веденні записів переконайтеся, що, як мінімум, ви зробили таке:

1. Занотовуйте ваші коментарі, думки і аналіз окремо від запису самого інтерв'ю.
2. Ведіть записи від першої особи: так, як каже потерпілий/свідок.
3. Не підсумовуйте, не скорочуйте і не вирізайте частини інформації потерпілих/свідків.
4. Зачитайте занотовані вами показання потерпілому/свідку до завершення інтерв'ю. Незважаючи на те, що це забирає багато часу, така дія має вирішальне значення для гарантування того, що інформація, яку ви отримали від свідка, є максимально точною.

5. Вказуйте в показаннях будь-які інші свідчення, отримані від цього потерпілого/свідок (фотографії речових доказів), а також використовуйте систему нумерації, щоб включати перехресні посилання.

6. Занотовуйте ПІБ та інші особисті дані окремо від заяв з міркувань безпеки.

7. Використовуйте стандартну систему іменування заяв, наведених в інтерв'ю.

8. Зберігайте показання кожного потерпілого/свідка окремо.

9. Зберігайте іншу інформацію про потерпілого/свідка (проблеми безпеки, умови проживання, проблеми зі здоров'ям або інші проблеми, які має потерпілий/свідок) окремо від отриманих від нього свідчень.

10. Тримайте імена потенційних респондентів, наведені потерпілим/свідком, окремо від інших нотаток (список потенційних респондентів є робочим документом і повинен зберігатися в безпечному відокремленому місці).

Документальні свідчення

Документи (як офіційні, так і неофіційні) можуть бути джерелом надзвичайно актуальної інформації при документуванні та розслідуванні сексуального насильства.

В цьому контексті особливо важливо дотримуватися конфіденційності:

• будь-яке спільне використання записів, звітів, досліджень і статистики випадків сексуального насильства має проводитися безпечно та етично, з повагою до права потерпілого на конфіденційність;

• статистична інформація повинна бути анонімною, при цьому, з метою запобігання негативних наслідків для потерпілих/свідків, практики повинні оцінити чи є ризик відстеження навіть анонімної інформації до конкретної особи, групи або спільноти;

• інформація на індивідуальному рівні повинна надаватися тільки з інформованої згоди потерпілого/свідка.

Збереження інформації

Якщо практики збирають інформацію про сексуальне насильство (наприклад, фотографії місця злочину або документ, що відображає хід інтерв'ю з потерпілим/свідком), вкрай важливо, щоб ця інформація вони документувалася та зберігалася таким чином, щоб не поставити під сумнів доброчесність практиків та не створити загрозу для потерпілих і свідків.

Чутливий характер інформації про сексуальне насильство та потенційна шкода, яку може бути завдана у разі неправильного використання такої інформації, визначають надзвичайну важливість дотримання збирачами цієї інформації принципу пріоритетності безпеки потерпілого/свідка, громади та осіб, які збирають інформацію.

Для забезпечення повного і всебічного дотримання цього принципу практики повинні:

1. Спланувати де буде зберігатися інформація та хто матиме контроль над нею. В ідеалі практики повинні використо-

вувати централізоване місце зберігання, яке контролюватиме особа, відповідальна за збереження інформації, навіть якщо організація зберігає «право власності» на інформацію.

2. Зберігати інформацію, яка ідентифікує потерпілого/свідка, надійно та окремо від заяв і доказів, наданих цим потерпілим/свідком (наприклад, індекс для співставлення кодів, що позначають інформацію/імена потерпілих/свідків).

3. Там, де це можливо, уникати зберігання публічної та секретної інформації разом, щоб забезпечити ефективніший захист останньої.

4. Впорядковувати інформацію таким чином, щоб її можна було легко знайти, коли вона знадобиться в подальшому.

5. Навчати персонал відповідним процедурам: (i) переміщення збереженої інформації після того, як файли будуть закриті; (ii) убезпечення інформації під час надзвичайних ситуацій.

6. В подорожах, які можуть передбачати проходження контрольно-пропускних пунктів, мати з собою лише абсолютно необхідну інформацію, адже практиків можуть попросити розкрити або передати інформацію, яку вони мають при собі або в своєму автомобілі. Розглянути можливість використання сучасних цифрових технологій для зберігання та/або шифрування інформації.

Зберігання документів та іншої фізичної інформації

- Якщо практики зберігають інформацію у вигляді документів або інших фізичних предметів, вони повинні тримати інформацію в замкненій шафі або сейфі з обмеженим доступом. Повинна існувати чітка політика щодо того, хто може отримати доступ до інформації та з якою метою.
- В умовах надзвичайної ситуації може виникнути необхідність забезпечення особистої безпеки співробітників, які мають доступ до сховищ інформації.
- Ведіть облік доступу, який надавався до сховища інформації (наприклад, фіксація ПІБ особи, дати, часу і мети доступу).
- Якщо носії інформації є такими, що швидко псуються (наприклад, звичайні негативи фотографій), тримайте їх подалі від джерел тепла та світла.
- Якщо інформація є частиною певного набору (наприклад, набір документів або роздрукованих фотографій), зв'яжіть його із зазначенням того, що це повний комплект.
- Усі фотографії та відеозаписи (та інша фізична інформація) повинні бути каталогізовані згідно впровадженої системи нумерації, і така система нумерації повинна посилатися на інші підтверджуючі докази цього конкретного фото/відео (наприклад, доказів потерпілого/свідка).
- Якщо аудіо- чи відеозапис робили для інших цілей, ніж просто запис інтерв'ю, відповідальна особа повинна

бути в змозі обґрунтувати їхнє подальше зберігання та передбачити збереження конфіденційності тих осіб, що фігурують у записах, особливо якщо ці записи мають зберігатися протягом тривалого часу.

Зберігання цифрової інформації

- Переваги використання системи зберігання цифрової даних (де це можливо) над ручною системою зберігання даних полягають у тому, що цифрова система не займає менше фізичного простору, полегшує пошук і аналіз, її легше оновлювати та формувати звіти з неї, і, певною мірою, її можна захистити. Проте, недоліками цифрової системи зберігання даних є те, що введення даних до неї забирає більше часу, доступ залежить від наявності електроенергії, веб-доступу, система вразлива до злому та вірусів. Крім того, якщо інформація передається за допомогою мобільних телефонів або через Інтернет, існує ризик того, що органи влади можуть зобов'язати операторів мобільного зв'язку або інтернет-послуг передати їм чутливу інформацію.
- Перед тим, як почати збір інформації, яка буде зберігатися в цифровому вигляді, оцініть ризики та впровадьте протокол цифрової безпеки. Варто проконсультуватися з фахівцями з управління інформацією та безпеки цифрових технологій.
- Уся цифрова інформація повинна бути захищена паролями (доступ до паролів – обмеженим) та зашифрована. Там, де це можливо, практики повинні вжити додаткових заходів для захисту конфіденційної інформації за допомогою більш складних процедур.
- В умовах надзвичайної ситуації може виникнути необхідність забезпечення особистої безпеки співробітників, які мають доступ до паролів.
- Якщо інформація буде зберігатися в цифровому вигляді, потрібно завантажити контент на комп'ютер, записати CD у форматі WORM (Write Once, Read Many) або зберегти інформацію на карту пам'яті, зробивши дві копії.
- Застосовуйте відповідні запобіжні заходи: використання антивірусного програмного забезпечення та створення резервних копій файлів із бази даних.
- Розгляньте можливість використання новітніх методів збору даних, таких як камери GPS, додатки для мобільної документації, які збирають спектр метаданих (тобто інформацію про те, коли, де та як були зібрані дані), а також додатки для мобільної документації, які за замовчуванням шифрують усі дані.
- Розгляньте можливість використання мобільних додатків для збору даних, які не зберігають копії даних на мобільному телефоні, тим самим зводячи до мінімуму ризик розкриття чутливих даних в разі втрати, крадіжки або конфіскації пристрою.

Зберігання судово-медичних/судових доказів

- Зберіганням судово-медичних/судових доказів (зразків крові, сперми або забрудненого одягу) повинні займатися фахівці, які пройшли спеціальну підготовку. Збір таких доказів без належних знань може призвести до заподіяння значної шкоди (див. Додаток 6 «Речові докази: принципи порядку передачі та зберігання» та Додаток 10 «Зразок медичної довідки про сексуальний напад»).
- Судово-медична експертиза/збір судово-медичних доказів повинні проводитися водночас із наданням медичної допомоги, бажано одною особою (див. Додаток 10 «Зразок медичної довідки про сексуальний напад»).
- У зв'язку з особливостями зберігання біологічних доказів (кров, сперма або одяг), вони поміщаються в окремі контейнери, запечатуються та доставляються до лабораторії одразу після їх збору.
- Необхідні рекомендації щодо збору судово-медичних доказів практики можуть отримати з:

• Керівних принципів ВООЗ щодо клінічного ведення жертв зґвалтування: керівництво з розробки протоколів для використання в роботі з біженцями та внутрішньо переміщеними особами, 2004 р.;

• PHR, УВКПЛ, Стамбульський протокол: керівництво щодо ефективного розслідування та документування катування та іншого жорстокого, нелюдського або такого, що принижують гідність, поводження та покарання, 1999 р.

ГЛОБАЛЬНИЙ КОДЕКС ПОВЕДІНКИ ЩОДО ЗБОРУ ТА ВИКОРИСТАННЯ ІНФОРМАЦІЇ ПРО СИСТЕМАТИЧНЕ СЕКСУАЛЬНЕ НАСИЛЬСТВО, ПОВ'ЯЗАНЕ З КОНФЛІКТОМ (КОДЕКС МУРАД) [17]

Це добровільний кодекс, у якому виокремлені наявні мінімальні стандарти безпечного, ефективного й етичного збирання та використання інформації, отриманої від жертви або особи, яка потерпіла від системного сексуального насильства («потерпіла особа») в умовах конфлікту («ССНУК»). Кодекс призначений для тих, хто займається документуванням, розслідуванням, розповсюдженням, дослідженням, моніторингом та іншими видами діяльності, пов'язаної зі збиранням та використанням такої інформації.

Мінімізувати ризики розкриття конфіденційної інформації

Кодекс Мурад[18] наголошує на необхідності мінімізувати ризики розкриття конфіденційної інформації. Важливо запитати потерпілу особу про попередні опитування або випадки передання інформації і обговорити з нею ризики, пов'язані з подальшими діями, та альтеративні варіанти. До таких ризиків належить виникнення непослідовних версій подій, що може завдати шкоду праву потерпілої особи на доступ до правосуддя і піддати її ризику повторної травматизації, порушення приватності та стигматизації. Необхідно обговорювати з потерпілою особою доступ до будь-яких попередніх заяв у якості можливого варіанту або альтернативи повторному опитуванню. Якщо потерпіла особа вирішить пройти опитування, докладати активних зусиль для пом'якшення ризиків, пов'язаних з повторним опитуванням.

Передання інформації

Потрібно обговорювати з потерпілими можливість передання їхньої інформації довіреним суб'єктам, щоб уникнути зайвого дублювання у збиранні інформації, ризику повторного травмування чи інших ризиків, пов'язаних з подальшою безпосередньою взаємодією. Важливо забезпечити, щоб будь-яке рішення, прийняте потерпілою особою щодо передання її даних, спиралось на інформовану згоду, було підтримане результатами оцінки ризиків, а також виконувалось у безпечний та ефективний спосіб згідно з бажаннями потерпілої особи.

Зменшення обсягів даних

Необхідно збирати, зберігати та використовувати персональні дані потерпілих, включаючи цифрову інформацію, тільки якщо це обґрунтовано чіткою метою, необхідно для досягнення цієї мети, пропорційно можливостям досягнення цієї мети, і якщо можливо захистити ці дані.

17 Глобальний кодекс поведінки щодо збору та використання інформації про систематичне сексуальне насильство, пов'язане з конфліктом (Кодекс Мурад). URL: https://www.muradcode.com/uk/murad-code

18 Глобальний кодекс поведінки щодо збору та використання інформації про систематичне сексуальне насильство, пов'язане з конфліктом (Кодекс Мурад). URL: https://www.un.org/sexualviolenceinconflict/wp-content/uploads/2022/06/report/auto-draft/202205-Murad_Code_Ukranian.pdf

Створювати процедури захисту конфіденційності

Необхідно розробити протоколи та заходи із забезпечення конфіденційності, щоб захистити дані, приватність та безпеку потерпілих, у тому числі вживати спеціальних заходів з убезпечення цифрових комунікацій, управління даними та зберігання даних.

Поважати вибір потерпілої особи

Важливо поважати індивідуальну свободу вибору потерпілих як фундаментальну основу для всіх аспектів та етапів взаємодії. Забезпечувати надання потерпілим повної, чіткої та правдивої інформації про мету, методологію, доступні для них варіанти, їхні права та ризики, у тому числі про конфіденційність та знеособлення, використання, передання та публікацію їх даних. Надавати інформацію в зрозумілій і доступній формі, щоб потерпілі могли прийняти рішення щодо взаємодії й умов такої взаємодії. Чітко давати потерпілим зрозуміти, що вони можуть у будь-який момент припинити взаємодію і не відповідати на будь-які запитання. Поважати рішення потерпілих не брати або припинити участь у процесі.

Давати змогу потерпілим зберігати контроль над своєю інформацією

Необхідно поважати та підтримувати право потерпілої особи на приватність, яке, за нашим розумінням, передбачає контроль та автономію у питаннях, що стосуються її персональної історії. Захищати конфіденційність будь-яких персональних відомостей або даних потерпілої особи (у будь-якій формі). Не використовувати і не передавати цю інформацію без їх явно вираженої інформованої згоди.

ВИСНОВОК

Захист персональних даних осіб, які постраждали від сексуального насильства, пов'язаного з конфліктом, вимагає специфічних підходів та заходів забезпечення конфіденційності та безпеки таких осіб.

Важливо усвідомлювати, що злочин СНПК негативно впливає не лише на потерпілу особу, але також на її близьких і членів родини.

Тому дотриманню права на приватність постраждалих осіб, гарантованого статтею 8 Конвенції про захист прав людини і основоположних свобод, Конституцією України та Законом України «Про захист персональних даних» має бути приділено особливу увагу.

Необхідно чітко розуміти, що розголошення персональних даних про потерпілу особу може мати непередбачувані наслідки для цієї особи.

Під обробці персональних даних осіб, які постраждали від сексуального насильства, пов'язаного з конфліктом, необхідно послідовно дотримуватися керівних принципів щодо конфіденційності, поваги і недискримінації та неухильно дотримуватися правила «не нашкодь».

Залучення осіб, членів їхніх сімей та громад з метою вивчення та документування інформації щодо сексуального насильства має проводитися таким чином, щоб забезпечити максимальний доступ до правосуддя для постраждалих і звести до мінімуму будь-який негативний вплив, який на них може мати процес документування. При документуванні інформації про сексуальне насильство правоохоронні органи повинні прагнути "не нашкодити" або звести до мінімуму шкоду, яку вони можуть ненавмисно заподіяти через свою присутність або мандат.

При плануванні документування та розслідування сексуального насильства правоохоронні органи повинні оцінити загрози (реальні, уявні чи такі, що передбачаються), які потенційно можуть завдати шкоди потерпілим й іншим свідкам, а також ризик того, що ці загрози будуть реалізовані. До початку розробки плану документування практики також повинні оцінити ризики та проблеми безпеки для всіх членів команди, що займатиметься документацією, та всіх тих, хто буде проходити інтерв'ю. Міркування щодо кадрової політики, матеріально-технічного забезпечення, усного та письмового перекладу, систем організації інформації та стратегій доступу до потерпілих/свідків будуть більш обґрунтованими після проведення оцінки ризиків для потерпілих/свідків і самої інформації.

Використання правильних методів, поведінки та установок під час інтерв'ю має вирішальне значення для того, щоб потерпілий/свідок відчував повагу до себе, своїх прав і міг комфортно ділитися інформацією.

Конфіденційність є етичним принципом документування злочинів сексуального насильства, який вимагає, щоб правоохоронні органи захищали інформацію, яку вони збирають про такі злочини, та застосовували цей принцип протягом усього періоду документування. Дотримання умови

конфіденційності необхідне для формування в потерпілого/свідка довіри до практиків. Водночас, постраждалому/свідку потрібно надати чіткі роз'яснення щодо наявних обмежень конфіденційності та умов їх виникнення.

Таким чином, забезпечення конфіденційності і дотримання положень законодавства про захист персональних даних є ключовим аспектом у забезпеченні безпеки осіб, постраждалих від СНПК, та формуванні довіри, необхідної для надання постраждалими максимально повних свідчень і відповідно – розкриття злочинів та покарання злочинців.

Редакція:

Громадська організація «UA Experts»

Адреса редакції: 01001, м. Київ, вул. Трьохсвятительська, 11В, тел.: +38 066 760 3131

Адреса для листування: info@ua-experts.org

Тираж: 500 примірників

Друк: ТОВ «Вістка», м.Київ, вул. Миколи Василенка, 1, тел.: +380677090225.

#ActingForSurvivors

За підтримки Фонду Організації Об'єднаних Націй
у галузі народонаселення в Україні (UNFPA)