Асоціація
УМДПЛ
UMDPL
Association

МАЙЖЕ СТАРШИЙ БРАТ СТЕЖИТЬ ЗА ТОБОЮ

ВІДЕОСПОСТЕРЕЖЕННЯ ЗА ДОТРИМАННЯМ ПУБЛІЧНОГО ПОРЯДКУ В УКРАЇНІ

Резюме до звіту за результатами дослідження

Асоціація українських моніторів
дотримання прав людини в діяльності правоохоронних органів
(Асоціація УМДПЛ)

МАЙЖЕ СТАРШИЙ БРАТ СТЕЖИТЬ ЗА ТОБОЮ:

ВІДЕОСПОСТЕРЕЖЕННЯ ЗА ДОТРИМАННЯМ ПУБЛІЧНОГО ПОРЯДКУ В УКРАЇНІ

Резюме до звіту за результатами дослідження

Київ
2019

МІЖНАРОДНИЙ ФОНД ВІДРОДЖЕННЯ

Асоціація УМДПЛ UMDPL Association

Відомості про авторів:

Михайло Каменєв — юрист, експерт Асоціації УМДПЛ з конституційного та адміністративного права

Степан Золотар — юрист, аналітик Асоціації УМДПЛ

(Майже) Старший брат стежить за тобою: відеоспостереження за дотриманням публічного порядку в Україні. Резюме до звіту за результатами дослідження / М. Каменєв, С. Золотар. — К.: Асоціація УМДПЛ: 2019. — 24 с.

Дослідження підготовлене експертами Асоціації УМДПЛ за підтримки Міжнародного фонду «Відродження» у межах проєкту «Напрацювання нормативно-правових актів для використання систем відеоспостереження для охорони громадського порядку». Дослідження відображає позицію авторів і не обов'язково збігається з позицією Міжнародного фонду «Відродження».

© М. Каменєв, С. Золотар, 2019
© Асоціація УМДПЛ, 2019

ЗМІСТ

Передмова **4**

Методологія дослідження **5**

Нормативно-правове регулювання діяльности систем відеоспостереження **9**

Міжнародні стандарти 9

Національне законодавство 9

Акти органів місцевого самоврядування 12

Функціональне призначення систем відеоспостереження **14**

Попередження про відеозйомку **15**

Обмін інформацією між суб'єктами владних повноважень **17**

Захист інформації **18**

Відеозаписи як допустимі докази **20**

Рекомендації **21**

ПЕРЕДМОВА

Технологічний прогрес призводить до появи нових викликів для прав людини, адже правове регулювання, як правило, регулює існуючі правовідносини і не розраховане на появу нових форм. Яскравим прикладом цього є поширення в геометричній прогресії відеоспостереження за дотриманням громадського порядку.

Подібні системи впроваджуються в багатьох країнах світу і використовуються як цілком легально і правомірно, так і для побудови поліцейської держави (наприклад, в Китаї).

В Україні системи відеоспостереження створюються і утримуються органами місцевого самоврядування, органами правопорядку, юридичними та фізичними особами.

На даному етапі розвитку ця сфера правовідносин в Україні не має жодного правового регулювання, що може становити загрозу для прав і свобод людини. Не заперечуючи можливості і важливість сучасних систем відеоспостереження в публічних місцях, вкрай важливо створити ефективну систему правил і гарантій.

Тому метою дослідження є з'ясування таких питань:

1. Яке існує нормативно-правове регулювання функціонування комплексних систем відеоспостереження, включаючи правила захисту та обробки даних?

2. Які є підходи до організації діяльності комплексних систем відеоспостереження, включаючи обмін інформацією з цих систем між різними суб'єктами владних повноважень?

3. Якою може бути оптимальна схема побудови та інтеграції комплексних систем відеоспостереження?

4. Як забезпечити дотримання прав людини при використанні комплексних систем відеоспостереження?

МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ

Основною метою дослідження є аналіз та оцінка існуючого нормативно-правового регулювання функціонування комплексних систем відеоспостереження, а також підходів до організації їх діяльності, з наданням на основі отриманих даних рекомендацій щодо можливих оптимальних схем нормативно-правового забезпечення, побудови та інтеграції комплексних систем відеоспостереження.

Під час роботи були застосовані такі кількісні та якісні методи, як аналіз статистичних даних, контент-аналіз, інтерв'ю.

Першим етапом дослідження було вивчення існуючих міжнародних стандартів, викладених у деклараціях та рекомендаціях органів Ради Європи. Також досліджено практику Європейського суду з прав людини, який має усталені позиції у сфері захисту права на повагу до приватного і сімейного життя.

Другим етапом стало вивчення національного законодавства в частині наявних конституційних гарантій та регулювання на рівні законів та підзаконних актів.

Третім етапом стала розсилка запитів на доступ до публічної інформації до органів місцевого самоврядування, оскільки гіпотезою дослідження було те, що локальні системи відеоспостереження встановлюються саме силами міських, селищних та сільських рад. Було направлено близько 550 запитів на електронні пошти міських та селищних рад — дослідженням охоплено всю територію України, окрім тимчасово окупованих територій АР Крим та окремих районів Донецької та Луганської областей. Запити було направлено до органів місцевого самоврядування міста Києва та всіх обласних центрів, районних центрів та міст обласного значення. Після отримання першої хвилі відповідей було направлено повторні електронні запити до населених пунктів, які не надали відповіді, а після цього — також паперові запити до обласних центрів та міст обласного значення.

Запити містили питання щодо місцевих програм, які передбачають встановлення камер відеоспостереження, кількості камер, що працюють в межах населеного пункту та/або планується для встановлення, правила збору, обробки, зберігання, видачі інформації, яка записується відеокамерами та порядок взаємодії з іншими державними органами та зацікавленими суб'єктами.

В процесі виконання цього етапу було виявлено, що в Україні відсутня єдина база електронних адрес органів місцевого самоврядування

для направлення запитів на доступ до публічної інформації. Відтак, було сформовано і в подальшому відкориговано відповідну базу, яка розміщена за посиланням і може стати в нагоді журналістам і активістам.

На наступних етапах дослідження було виявлено, що системи відеоспостереження в окремих регіонах встановлюються за рахунок обласних програм. Відтак, було направлено запити до обласних рад, частина з яких була ними переадресована до міських, селищних та подекуди сільських рад відповідної області. В окремих випадках запити були переадресовані до обласних та районних державних адміністрацій. Таким чином, було отримано інформацію з деяких населених пунктів, які не надали інформацію на попередньому етапі. Також було отримано інформацію від частини обласних рад щодо обласних програм, які передбачають встановлення відеокамер.

Запити до обласних рад містили аналогічні питання про наявність обласних програм, кількість встановлених камер, наявність правил збору та обробки отриманої інформації тощо.

В цілому, було отримано інформацію від міських рад усіх обласних центрів і міста Києва, а також більшості міст обласного значення та районних центрів.

Великі системи відеоспостереження створюються по всій країні силами органів місцевого самоврядування. Тому наступним етапом після вивчення відповідей на запити стали ознайомчі візити експертів проєкту до різних населених пунктів.

Загалом було відвідано 14 населених пунктів — місто Київ, обласні центри: Житомир, Вінниця, Дніпро, Львів, Івано-Франківськ, Одеса, Рівне, Чернівці, Ужгород; міста обласного значення: Мукачево (Закарпатська обл.), Маріуполь (Донецька обл.); районні центри: Перечин (Закарпатська обл.), Тростянець (Сумська обл.).

Міста були обрані таким чином, щоб дослідження охопило населені пункти з центру України (Вінниця, Дніпро), заходу (Рівне, Львів, Івано-Франківськ, Чернівці та міста Закарпатської области), сходу (Маріуполь), півдня (Одеса) та півночі (Київ, Житомир, Тростянець).

Також було ранжирувано міста за кількістю населення та обрано різні за масштабами системи відеоспостереження (за кількістю встановлених камер).

При цьому, слід відзначити, що деякі системи мають доступ не тільки до камер відповідного міста, а й до камер з інших населених пунктів у області (Одеса, Рівне, Маріуполь), або навіть з інших областей (Київ).

Також було обрано системи з різними підходами до організаційного забезпечення: з лідируючою роллю комунальних підприємств міських рад (Київ, Дніпро, Одеса, Житомир, Івано-Франківськ, Мукачево), концентрацією у міських рад (Львів, Вінниця, Перечин, Ужгород), домінуванням поліції (Маріуполь, Рівне, Чернівці), а також з передачею систем у користування громадського формування з охорони громадського порядку і державного кордону (Тростянець, Сумська обл.).

В ході ознайомчих візитів було встановлено, що гіпотеза про існування комплексних систем відеоспостереження, які перебувають на балансі органів Нацполіції, хибна.

В різних населених пунктах в ході ознайомчих візитів було проведено зустрічі з представниками різних суб'єктів владних повноважень та дотичними структурами (детальний перелік органів наведено у додатку). Серед них - службовці міських рад, поліцейські з ГУНП, відділів поліції, управлінь патрульної поліції, працівниками комунальних підприємств міських рад. Зустрічі проводились у формі напівструктурованих інтерв'ю. Загалом було проведено інтерв'ю з 42 особами, відвідано 36 підприємств, установ та організацій.

В ході ознайомчих візитів експерти проєкту самостійно досліджували розміщення камер відеоспостереження на вулицях міст. В більшості випадків експерти змогли оглянути ситуаційні центри, через які координується робота систем відеоспостереження. В окремих випадках можна було ознайомитись із роботою ситуаційних центрів відеоспостереження в ГУНП, відділів поліції та управлінь патрульної поліції (перелік).

Після проведення ознайомчих візитів було проведено робочі зустрічі з зацікавленими державними органами - Національною поліцією (ДОАЗОР), Державною службою спеціального зв'язку та захисту інформації (Департамент захисту інформації) та Секретаріатом Уповноваженого Верховної Ради України з прав людини (Департамент у сфері захисту персональних даних).

Під час візиту до ДОАЗОР було відвідано Ситуаційний центр НПУ, який має доступ до систем відеоспостереження низки великих міст України.

Між ознайомчими візитами експерти проєкту взяли участь у вінницькому Форумі "Безпечне місто Вінниця", де представили та обговорили перші результати дослідження з представниками органів державної влади та місцевого самоврядування з різних регіонів України, а також виробниками та постачальниками систем відеоспостереження.

Під час одного з останніх ознайомчих візитів у місто Чернівці експерти проєкту взяли участь у регіональному семінарі-нараді з питань впровадження та забезпечення технічної підтримки систем відеонагляду та відеоаналітики, організованому ДОАЗОР на базі Головного управління Національної поліції в Чернівецькій області, де представили попередні результати дослідження та обговорили їх з представниками Департаменту зв'язку та телекомунікацій Нацполіції, ГУНП у Львівській, Закарпатській, Івано-Франківській, Рівненській, Волинській, Тернопільській, Хмельницькій та Чернівецькій областях, а також представниками Чернівецької міської та обласної рад і Чернівецької облдержадміністрації.

Дослідження було здійснене протягом січня-жовтня 2019 року.

НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ДІЯЛЬНОСТИ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

Міжнародні стандарти

Проблемі дотримання прав людини при функціонуванні систем відеоспостереження присвячене дослідження Венеційської комісії № 404/2006 CDL(2007)011 «The extent to which video surveillance is compatible with human rights» та позиція CDL-AD(2007)014 «On video surveillance in public places by public authorities and the protection of human rights».

Цій темі була приділена увага і в позиції Data Protection Working Party, яка є незалежним дорадчим органом Європейського Союзу. European Data Protection Supervisor видав у 2010 році керівні принципи використання систем відеоспостереження. European Forum for Urban Security у 2013 році досліджував відповідне регулювання у низці міст Європи. Комісар Канади із захисту приватності у 2006 році розробив керівні принципи з цього питання в контексті використання даних органами правопорядку

Національне законодавство

Законодавство України, хоч і містить деякі приписи, які б регулювали діяльність систем відеоспостереження, навряд чи це можна назвати належним регулюванням.

Відповідно до статті 32 Конституції України ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України (частина перша). 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 (частина друга).

Конституційний Суд України у своєму рішенні від 20 січня 2012 року № 2-рп/2012 у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України дійшов висновку, що збирання, зберігання, використання та поширення державою, органами місцевого самоврядування, юридичними або фізичними особами конфіденційної інформації про особу без її згоди є втручанням в її особисте та сімейне життя, яке допускається винятково у визначених законом випадках і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Правові засади захисту інтересів фізичної особи при проведенні фото-, кіно-, теле- та відеозйомок визначені у статті 307 Цивільного кодексу України. Відповідно до частини першої зазначеної статті фізична особа може бути знята на фото-, кіно-, теле- чи відеоплівку лише за її згодою. Згода особи на знімання її на фото-, кіно-, теле- чи відеоплівку припускається, якщо зйомки проводяться відкрито на вулиці, на зборах, конференціях, мітингах та інших заходах публічного характеру.

Фізична особа не може відмовитися від особистих немайнових прав, а також не може бути позбавлена цих прав (частина третя статті 269 Цивільного кодексу України).

Втім, на нашу думку, відкритість зйомки передбачає поінформованість фізичної особи про те, що така зйомка здійснюється. Відповідні положення Цивільного кодексу України були прийняті в часи, коли не існувало технічної можливості побудови комплексних систем відеоспостереження, а існуючі вуличні камери відеоспостереження не дозволяли отримати якісне зображення. Необхідність попереджень про здійснення відеоспостереження буде детально висвітлена в одному з наступних розділів дослідження.

Слід нагадати, що відповідно до частини другої статті 19 Конституції України органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України.

Враховуючи, що більшість систем встановлюється органами місцевого самоврядування, постає питання — на підставі якої норми закону це здійснюється?

Основною декларованою метою, з якою встановлюються системи відеоспостереження, є забезпечення публічного порядку. Закон України "Про місцеве самоврядування в Україні" передбачає такі повноваження органів місцевого самоврядування в цій сфері:

— вжиття у разі надзвичайних ситуацій необхідних заходів відповідно до закону щодо забезпечення державного і громадського порядку, життєдіяльності підприємств, установ та організацій, врятування життя людей, захисту їх здоров'я, збереження матеріальних цінностей (підпункт 2 пункту "б" частини першої статті 38);

— вирішення відповідно до закону питань про проведення зборів, мітингів, маніфестацій і демонстрацій, спортивних, видовищних та інших масових заходів; здійснення контролю за забезпеченням

при їх проведенні громадського порядку (підпункт 3 пункту “б” частини першої статті 38);

— заслуховування інформації прокурорів та керівників органів Національної поліції про стан законності, боротьби із злочинністю, охорони громадського порядку та результати діяльності на відповідній території (пункт 36 частини першої статті 43).

В інших законах немає положень, які наділяли б органи місцевого самоврядування повноваженнями у цій сфері.

Отже, як бачимо, законодавство не передбачає для органів місцевого самоврядування повноважень щодо встановлення систем відеоспостереження.

Не краща ситуація і з використанням таких систем органами Національної поліції. Закон України “Про Національну поліцію” містить положення, що дозволяють органам НПУ використовувати інформацію з систем відеоспостереження, що знаходяться в чужому володінні (частина перша статті 40). Водночас, стаття 25 цього закону наділяє НПУ повноваженнями користуватись базами (банками) даних МВС та інших органів державної влади. Органи місцевого самоврядування та комунальні підприємства до органів державної влади не належать і окремо у вищезазначеній статті не згадуються. Відтак, навіть Закон України “Про Національну поліцію” містить неузгодженість, яка стоїть на заваді використання НПУ інформації з систем відеостереження органів місцевого самоврядування. Але навіть якщо до цієї статті будуть внесені відповідні зміни, інформація з систем відеоспостереження, які перебувають у віданні органів місцевого самоврядування, все одно не буде вважатись отриманою на законних підставах, допоки відповідними повноваженнями не будуть наділені органи місцевого самоврядування.

Цікавим є приклад організації відеоспостереження на виборчих дільницях під час парламентських виборів 2012 року. Для створення системи відеоспостереження був прийнятий окремий Закон України “Про особливості забезпечення відкритості, прозорості та демократичності виборів народних депутатів України 28 жовтня 2012 року”, а на його виконання — постанови Кабінету Міністрів України від 8 серпня 2012 року № 766 “Про затвердження технічного завдання та конфігурації створення системи відеоспостереження” та Центральної виборчої комісії від від 13 вересня 2012 року № 892 “Про Порядок здійснення відеоспостереження на виборчих дільницях з використанням засобів відеоспостереження, доступу та контролю за функціонуванням системи відеоспостереження під час проведення виборів народних депутатів України 28 жовтня 2012 року”.

Така разова акція для показової демократичности виборчого процесу є чи не єдиним регулюванням роботи хоч якоїсь системи відеоспостереження на національному рівні. Водночас, в цілому реалізована система відеоспостереження на виборах була оцінена як зайва витрата коштів (близько мільярда гривень). В подальшому ця система не використовувалась, а в липні 2014 року була передана на баланс обласних державних адміністрацій, кожна з який вирішувала подальшу долю обладнання самостійно.

Акти органів місцевого самоврядування

Відсутність належного законодавчого регулювання, втім, не заважає органам місцевого самоврядування встановлювати системи відеоспостереження, збирати та обробляти значні масиви даних, зокрема, персональних.

В більшості населених пунктів системи встановлюються на підставі міських програм "Безпечне місто", програм щодо боротьби зі злочинністю, програм цифрового розвитку тощо. Такі програми ухвалюються місцевими радами на підставі пункту 22 частини першої статті 26 Закону України "Про місцеве самоврядування в Україні". Власне, ця стаття передбачає лише те, що місцеві ради вирішують питання щодо затвердження програм соціально-економічного та культурного розвитку відповідних адміністративно-територіальних одиниць, цільових програм з інших питань місцевого самоврядування.

Зазвичай мова йде про комплексні програми, однією з частин яких є встановлення систем відеоспостереження.

Тим не менше, програми не регламентують питання доступу до систем, обробки персональних даних тощо. Тому, для визначення цих питань, міські ради подекуди ухвалюють положення про системи відеоспостереження. Такі положення є у містах з найбільшими системами — у Києві та Одесі, але у Дніпрі та Вінниці, системи яких також входять до найбільших в Україні, таке регулювання відсутнє. В містах з меншими системами також іноді зустрічаються положення, проте, мало де вони принципово відрізняються від київського — врешті, чому б не використати вже готові практики, навіть незважаючи на наявні в них недоліки? Серед органів місцевого самоврядування, які не мають, на відміну від органів державної виконавчої влади, вертикального підпорядкування, поширеною є практика запозичення моделей рішень та нормативно-правових актів у інших органів місцевого самоврядування. Свого часу в київському положенні забули написати про можливість доступу до системи працівників ДБР та НАБУ, які також, як і поліція,

здійснюють досудове розслідування. В інших містах цієї помилки не помітили, і вона перекочувала до всіх інших положень.

Вирішенням цієї проблеми може стати затвердження типово порядку створення та використання комплексних систем відеоспостереження за публічним порядком. Належним суб'єктом затвердження такого типового порядку має бути Кабінет Міністрів України. Для реалізації цього сценарію відповідне повноваження Кабінету Міністрів України має бути закріплене на рівні закону.

Також, для детальнішого регулювання, органи місцевого самоврядування ухвалюють Регламенти діяльности систем, якими встановлюються детальні технічні та інфраструктурні питання встановлення та роботи систем відеоспостереження. Відомо про існування таких регламентів в Києві та Одесі, але питання їхньої відкритості виявилось проблемним — якщо в Одесі він опублікований на сайті комунальної установи, що здійснює обслуговування системи, регламент роботи київської системи вдалося отримати лише за запитом на доступ до публічної інформації, а у відкритих джерелах він відсутній.

ФУНКЦІОНАЛЬНЕ ПРИЗНАЧЕННЯ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

Як зазначалось вище, законодавчі підстави для створення ОМС комплексних систем відеоспостереження відсутні. Відтак, формально неможливо встановити законну ціль їхнього створення. Водночас, це вдалось встановити в ході дослідження на практиці.

Можна в цілому розділити функції систем на два блоки — пов'язані з опрацюванням інформації в режимі реального часу та пов'язані зі збереженими даними.

В реальному часі системи дозволяють моніторити обстановку в сфері публічної безпеки, зокрема щодо проведення масових заходів, роботи комунального транспорту, світлофорної мережі, діяльності муніципальних служб щодо озеленення, благоустрою, прибирання снігу тощо.

Очевидною в такому випадку є низька ефективність (результативність) операторів систем, які здійснюють цілодобове рутинне відстеження зображення з камер на моніторах (відеостінах), на які виводиться зображення одразу з десятків камер. Більш доцільним є запровадження автоматизованих процесів (відеоаналітики), які дозволяють без участі людини виявляти небезпечні ситуації або правопорушення.

Використання систем відеоспостереження для цілей контролю діяльності комунальних служб видається непропорційним, порівняно з рівнем втручання в приватне життя громадян. Керівники ОМС мають використовувати інакші механізми контролю, які не передбачатимуть надмірного (як для цілей використання систем) втручання.

Цілком доцільним і ефективним видається застосування систем для оперативного контролю та координації дій органів правопорядку та інших служб під час масових заходів або загострення оперативної обстановки. Для цієї цілі цілком виправданим може бути надання доступу до систем відеоспостереження для ОМС та інших державних органів у випадку надзвичайних ситуацій та ліквідації їхніх наслідків.

В роботі зі збереженими даними зацікавлені передовсім органи правопорядку, які використовують отримані дані в рамках проведення досудового розслідування.

ПОПЕРЕДЖЕННЯ ПРО ВІДЕОЗЙОМКУ

Відповідно до Резолюції ПАРЄ 1604 (2008) ("Відеоспостереження в публічних місцях") кожен, хто живе або проходить через зону відеоспостереження, має право знати про це і мати доступ до всіх записів із своїм зображенням.

З відвіданих міст тільки у Житомирі взято за правило розміщувати практично під кожною камерою попередження про відеоспостереження біля відеокамер. Також повідомлення про відеоспостереження здійснюється в Києві та Одесі. В цих містах таблички встановлюються не біля кожної камери, але загалом так, щоб на певному місці, за яким здійснюється відеонагляд, хоча б одна табличка була встановлена.

На жаль, в жодному з міст встановлення табличок нічим не регламентовано. Лише в Одесі в Положенні про систему зазначено, що інформація про здійснення відеоспостереження розміщується поблизу засобів відеофіксації та/або об'єктів відеоспостереження, зазначених у пункті 3.1 Положення (спосіб інформування визначається Регламентом). Втім, в Регламенті це питання не визначено, тому також, фактично, таблички встановлюються "під чесне слово".

У Тростянці та Маріуполі в деяких місцях встановлюються таблички, втім, вони не містять жодної довідкової інформації про суб'єкт здійснення відеоспостереження. В інших відвіданих містах повідомлення про відеоспостереження побачити не вдалось.

Як зазначалось вище, тільки один закон наділяє суб'єкт владних повноважень повноваженнями встановлювати системи відеоспостереження - Закону "Про Національну поліцію". І він містить вимогу щодо розміщення інформації про змонтовану/розміщену техніку на видному місці (частина друга статті 40). Отже, законодавець вважає за потрібне на рівні закону визначити обов'язок розміщувати попередження про відеоспостереження.

Окремо слід виділити практику міста Вінниця, де крім того, що не встановлюються жодні попередження про здійснення відеоспостереження, використовується декілька мобільних відеокамер, призначених для прихованого (наприклад, у гілках дерев) спостереження за місцями потенційного несанкціонованого скидання відходів. При чому, цей підхід, за твердженням чиновників, є ефективним. Приховане відеоспостереження в даному випадку спрямоване не на превенцію (для досягнення цієї цілі цілком підходять відкрито встановлені камери відеоспостереження), а на виявлення порушників. Є серйозні сумніви щодо законності такої практики, позаяк вона ідентична до одного з видів

негласних слідчих (розшукових) дій - спостереження за місцем (стаття 269 Кримінального процесуального кодексу України). Це абсолютно неприпустимо, оскільки спостереження за місцем як різновид НС(Р)Д може здійснюватись тільки в межах кримінального провадження належними суб'єктами НС(Р)Д і тільки під час досудового розслідування тяжкого або особливо тяжкого злочину, до яких несанкціоноване скидання відходів не належить. Тривожним є те, що вінницька практика інформаційно поширюється як приклад best practice і може бути взята на озброєння іншими населеними пунктами.

Прикладом практик інших органів влади щодо розміщення повідомлень про проведення відеоспостереження може бути ПАТ "Укрзалізниця", яке мало намір встановити систему відеоспостереження для гарантування безпеки при перевезенні пасажирів. У 2018 році Секретаріат Уповноваженого Верховної Ради України з прав людини надав роз'яснення ПАТ "Укрзалізниця" щодо обробки персональних даних при встановленні відеоспостереження.

Серед іншого, було наголошено на тому, що відеоспостереження повинно здійснюватись відкрито.

В Уповноваженого з прав людини наголошують на тому, що володілець персональних даних, який здійснює відеоспостереження, повинен повідомити суб'єкта персональних даних про факт здійснення відеоспостереження шляхом розміщення відповідного застереження. Таке застереження повинно бути видимим, розташованим на розумній відстані від місць зйомки та містити інформацію про володільця персональних даних (назву володільця, код ЄРДПОУ, контактну інформацію тощо).

ОБМІН ІНФОРМАЦІЄЮ МІЖ СУБ'ЄКТАМИ ВЛАДНИХ ПОВНОВАЖЕНЬ

Під час дослідження було виявлено різні способи обміну інформацією між розпорядниками/адміністраторами систем та іншими органами державної влади, підрозділами органів місцевого самоврядування. В тих населених пунктах де існують положення, порядок доступу різних органів та установ передбачений цими положеннями, в інших же містах — залежить від усталеної практики, власного розуміння чиновників, як має функціонувати система, та технічних можливостей.

Окремо слід звернути увагу на роботу інформаційної підсистеми "Гарпун" інформаційно-телекомунікаційної системи "Інформаційний портал Національної поліції України" (далі — система "Гарпун").

Система "Гарпун" збирає з камер відеоспостереження інформацію щодо пересування, розшуку транспортних засобів у форматі метаданих — зображення автомобіля та перелік інформації про його модель, колір, власника тощо. До системи "Гарпун" передається інформація з понад 2 тисяч камер, частина з яких перебувають у власності Нацполіції, а частина — камери, що формують системи відеоспостереження в населених пунктах.

Фактично кожне з міст, яке передає інформацію зі своєї системи відеоспостереження до системи "Гарпун" купляє або замовляє розробку програмних продуктів, які б експортували метадані, отримані програмним забезпеченням системи відеоспостереження, до системи "Гарпун" в прийнятному форматі.

В деяких містах інформація з систем відеоспостереження не передається до системи "Гарпун" через відсутність технічної можливості, в інших — через дискомунікацію між місцевою владою та органами Нацполіції. В містах з одними з найбільших систем відеоспостереження нам доводилось чути про те, що Національна поліція має платити за отримання таких даних — фактично, купляти в органів місцевого самоврядування інформаційний продукт, адже це вже використання системи не для охорони громадського порядку, а для здійснення оперативно-розшукової діяльності.

ЗАХИСТ ІНФОРМАЦІЇ

Системи відеоспостереження за своєю природою є інформаційно-телекомунікаційними системами, відтак, захист інформації в них має здійснюватись відповідно до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах".

Відповідно до частини другої статті 8 згаданого Закону 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 здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

Законом України "Про захист персональних даних" встановлена, вимога щодо захисту персональних даних. Зокрема, статтею 24 встановлено, що володільці, розпорядники персональних даних та треті особи зобов'язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних.

Враховуючи нерозуміння більшістю власників, розпорядників систем відеоспостереження того, що обличчя особи та номерні знаки автомобілів є персональними даними, належний захист інформації в системах відеоспостереження майже ніде не здійснюється.

Посадовці ДССЗЗІ під час розмови відзначили, що у відомство не може вимагати атестації КСЗІ для систем відеоспостереження через те, що законодавство не дає прямої відповіді на питання, чи є зображення особи її персональними даними. Але якщо відповідні норми будуть внесені до Закону України "Про захист персональних даних", то не буде сумнівів щодо потреби атестації.

Відповідно до даних Держспецзв'язку станом на липень 2019 року жодна з систем відеоспостереження в Україні не була атестована на відповідність КСЗІ вимогам законодавства.

За інформацією, наданою КУ "Центр-077" Одеської міської ради, 30 серпня 2019 року атестат відповідності КСЗІ інтегрованої системи відеоспостереження та відеоаналітики був зареєстрований у Держспецзв'язку, тобто, одеська система відеоспостереження стала першою атестованою в Україні. Також станом на кінець серпня система відеоспостереження у місті Києві проходила процес атестації.

Однією з проблем побудови та атестації КСЗІ є значна вартість таких послуг. Відповідно до даних в системі ProZorro побудова та

атестація КСЗІ в Одесі коштувала майже 400 тисяч гривень, а в Києві — майже мільйон, а насправді 2 мільйони — разом з КСЗІ дата-центру.

Очевидно, не всі місцеві ради навіть великих населених пунктів можуть виділити кошти на побудову та атестацію КСЗІ. Тому персональні дані в системах захищаються "підручними" засобами, які не завжди мають щось спільне з реальним захистом інформації.

Кричущим, але дуже показовим, є приклад однієї з міських рад, в якій доступ до системи з правами адміністратора (тобто, повний доступ) здійснюється за коротким і прогнозованим логіном та паролем, який входить до десятки найбільш поширених паролів в мережі Інтернет.

Проблему високої вартості сертифікації КСЗІ можна обійти, якщо запровадити модельні системи для систем відеоспостереження різного розміру. Відчутно зменшити навантаження на місцеві бюджети може створення інтегрованої загальнодержавної системи (дата-центру) для муніципальних систем відеоспостереження, сертифікація якої була б здійснена один раз і не за рахунок місцевих бюджетів.

Окремим потенційно проблемним моментом є те, що в переважній більшості ОМС для створення систем відеоспостереження закуповують обладнання китайської фірми HikVision, яка, судячи з усього, контролюється урядом КНР і перебуває у переліку торговельних санкцій США поруч з продукцією фірми Huawei. Причиною потрапляння до цього списку називають міркування національної безпеки США та інформація про існування механізмів прихованого отримання доступу до систем (бекдорів), закладених урядом Китаю. Дана інформація потребує додаткової перевірки та зважування всіх ризиків того, що чутлива інформація може бути доступна уряду іншої держави. На жаль, Служба безпеки України не відповіла на запит, направлений в рамках дослідження, і є єдиним державним органом, який проігнорував запити.

ВІДЕОЗАПИСИ ЯК ДОПУСТИМІ ДОКАЗИ

Одним з дуже поширених причин використання систем відеоспостереження є використання відеозаписів для цілей кримінального провадження або провадження у справах про адміністративні правопорушення. Справді, в умовах масового встановлення систем відеоспостереження злочинцям доволі важко уникнути потрапляння під приціл відеокамер.

В ході дослідження всі співрозмовники з органів місцевого самоврядування, комунальних підприємств та органів НПУ підтвердили, що записи з систем відеоспостереження без зауважень приймаються судами як допустимі докази.

Як було зазначено вище, встановлення систем відеоспостереження органами місцевого самоврядування не має належних законодавчих підстав, що становить порушення принципу законності. Відтак, презюмується, що вся інформація, отримана за допомогою таких систем, отримана не в межах і не у спосіб, визначений законом.

Також вже зазначалося, що, оскільки органи місцевого самоврядування не є органами державної влади, Національна поліція також не може законно використовувати дані, отримані з систем відеоспостереження, встановлених ОМС.

Виключення становлять лише системи відеоспостереження, які перебувають на балансі органів НПУ, однак лише за умови дотримання всіх інших вимог чинного законодавства України, зокрема законів "Про захист персональних даних" та "Про захист інформації в інформаційно-телекомунікаційних системах".

Лише питання часу, коли розумний адвокат переконає розумного суддю в тому, що докази, здобуті з систем відеоспостереження є неналежними. Перше ж таке рішення може спровокувати відповідну судову практику та позбавить системи відеоспостереження одного з їхніх козирів. Крім того, відповідно до концепції "плодів отруєного дерева", всі інші докази, здобуті на основі інформації, отриманої не в законний спосіб, будуть визнані також недопустимими.

Усе вищезазначене описано щодо кримінального провадження, але є цілком релевантним і для проваджень у справах про адміністративні правопорушення, оскільки стандарти доказів у цій частині принципово не відрізняються на практиці ні в контексті Кодексу України про адміністративні правопорушення, ані в контексті Кодексу адміністративного судочинства України.

РЕКОМЕНДАЦІЇ

Верховній Раді України

— створити законодавче підґрунтя функціонування систем відеоспостереження з урахуванням міжнародних стандартів та практики ЄСПЛ, залучивши до розробки відповідного законопроєкту представників зацікавлених державних органів, органів місцевого самоврядування та експертного середовища

— визначити в Законі України "Про захист персональних даних", що зображення обличчя/силуету особи є персональними даними

— здійснювати парламентський контроль за створенням та функціонуванням систем відеоспостереження

— внести зміни до Цивільного кодексу України задля регламентування встановлення систем відеоспостереження особами приватного права у публічних місцях

Уповноваженому Верховної Ради України з прав людини

— здійснити за участі представників громадськості моніторингові візити з перевіркою володільців та розпорядників персональних даних до міст із наймасштабнішими системами відеоспостереження та у разі виявлення порушень надати необхідні приписи про усунення порушень вимог законодавства про захист персональних даних та про доступ до публічної інформації

— проводити по мірі необхідності круглі столи за участі представників громадськості, державних органів та ОМС для узагальнення інформації щодо використання систем відеоспостереження та пошуку шляхів вирішення виявлених проблем

— напрацювати за участі представників громадськості та видати рекомендації щодо дотримання права на захист персональних даних та права на доступ до публічної інформації розпорядниками та користувачами систем відеоспостереження

Кабінету Міністрів України
та Міністерству внутрішніх справ України

— розглянути можливість створення національної інтегрованої системи відеоспостереження з державними дата-центрами (під контролем державного підприємства зі сфери управління МВС) та комунальними відеокамерами

Національній поліції України

— розглянути доцільність використання систем відеоспостереження для цілей ОРД/НС(Р)Д

Органам місцевого самоврядування

— у випадку, якщо в 2019-2020 роках парламент не створить законодавчі підстави для створення та використання ОМС систем відеоспостереження — передати відповідні системи на баланс органів Національної поліції

— відмовитись від використання систем відеоспостереження для цілей контролю за діяльністю комунальних служб

— не використовувати самостійно системи відеоспостереження для ОРД/НС(Р)Д

— здійснити атестацію КСЗІ систем відеоспостереження (за відсутності відповідних коштів — забезпечити власними силами максимально можливий рівень захисту інформації в системах)

— чітко розмежувати рівні доступу до інформації в системах відеоспостереження та забезпечити можливість персональної ідентифікації користувачів системи та логування всіх запитів до архіву відеозаписів

— розміщувати видиме застереження про факт здійснення відеоспостереження на розумній відстані від місць зйомки, що має містити інформацію про володільця персональних даних (назву володільця, код ЄРДПОУ, контактну інформацію тощо)

— надавати інформацію на запити відповідно до Закону України "Про захист персональних даних" (інформацію про себе) або Закону України "Про доступ до публічної інформації" із деперсоналізацією третіх осіб та державних номерних знаків транспортних засобів, при цьому не перенаправляючи такі запити до органів Нацполіції або інших користувачів систем.

Міжнародний фонд «Відродження» — одна з найбільших українських благодійних фундацій, що з 1990-го року допомагає розвивати в Україні відкрите суспільство на основі демократичних цінностей. За час своєї діяльності Фонд підтримав близько 20 тисяч проектів на суму понад 200 мільйонів доларів США. Фонд заснований філантропом Джорджем Соросом і є частиною міжнародної мережі Фундацій відкритого суспільства (Open Society Foundations).

Сайт: www.irf.ua

Facebook: www.fb.com/irf.ukraine

Асоціація українських моніторів дотримання прав людини в діяльності правоохоронних органів (Асоціація УМДПЛ) — неурядова правозахисна організація, що здійснює системний всеукраїнський моніторинг дотримання прав людини та основоположних свобод у діяльності правоохоронних органів.

Напрямки діяльності Асоціації УМДПЛ:

- експертно-аналітичний
- громадський контроль
- просвітництво
- пенітенціарний

Детальніше про організацію та результати роботи — www.umdpl.info

Підписано до друку 11.10.2019.
Надруковано на власному обладнанні Асоціації УМДПЛ.

Контактна інформація:
01001, Київ-1, а/с 496, тел.: (044) 253-40-36, association.umdpl@gmail.com