АДМІНІСТРАТИВНЕ ПРАВО І ПРОЦЕС; ФІНАНСОВЕ ПРАВО; ІНФОРМАЦІЙНЕ ПРАВО

УДК 342.98
DOI https://doi.org/10.32844/2618-1258.2022.6.12

БЛІНОВА Г.О., МАМЕДОВА Е.А.

ПРАВОВІ АСПЕКТИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У РОБОТІ ПАТРУЛЬНОГО ПОЛІЦЕЙСЬКОГО

LEGAL ASPECTS OF PERSONAL DATA PROTECTION IN THE WORK OF A PATROL POLICE OFFICER

У статті проаналізовано правові засади захисту персональних даних фізичних осіб працівниками патрульної поліції в процесі використання відеореєстраторів та бодікамер. Виявлено такі позитивні аспекти використання технічних пристроїв фіксації в роботі патрульної поліції як: відеоматеріали можна використовувати як доказову базу у кримінальних розслідуваннях та судових процесах; вони можуть допомогти встановити обставини злочину, ідентифікувати злочинців і захистити права потерпілих; знижується рівень корупції з боку працівників поліції, оскільки наявність відеозаписів може допомогти запобігти зловживанням з боку поліцейських, а також зменшити можливість випадкових або необґрунтованих затримань чи застосування надмірної сили; відеозаписи можуть стати ефективним інструментом захисту прав громадян у випадках порушення правил поведінки поліцейськими або випадків прояву недобросовісності з боку правоохоронців. Виокремлено потенційні негативні аспекти використання електронної техніки, що здійснює постійний відеозапис, а саме це може порушувати приватність та конфіденційність життя громадян; існує ризик зловживання відеозаписами поліції, зокрема, їх неправомірного використання, поширення або викривлення фактів; використання техніки нагляду може супроводжуватись технічними проблемами, такими як помилки запису, збої системи, втрати даних, що може вплинути на достовірність та надійність відеозаписів. Для недопущення реалізації таких ризиків необхідно встановлювати чіткі правила та обмеження щодо збереження, доступу та використання отриманої відеоінформації в патрульній поліції; розробити механізми контролю та внутрішні правила, щоб уникнути можливих зловживань; підвищувати рівень технічного супроводження цих процесів.

Ключові слова: *кібербезпека, патрульна поліція, персональні дані, право на приватність, конфіденційна інформація, розголошення.*

The article analyzes the legal principles of protection of personal data of individuals by patrol police officers in the process of using video recorders and body cameras. Such positive aspects of the use of technical fixation devices in the work of the patrol police were identified as: video materials can be used as an evidence base in criminal

© БЛІНОВА Г.О. – доктор юридичних наук, доцент, професор кафедри цивільного, господарського та екологічного права (Національний технічний університет «Дніпровська політехніка»)

© МАМЕДОВА Е.А. – ад'юнкт кафедри адміністративного права, процесу та адміністративної діяльності (Дніпропетровський державний університет внутрішніх справ)

investigations and court proceedings; they can help establish the circumstances of the crime, identify criminals and protect the rights of victims; the level of police corruption is reduced, as the availability of video footage can help prevent abuse by police officers and reduce the possibility of accidental or unjustified arrests or the use of excessive force; video recordings can become an effective tool for protecting the rights of citizens in cases of violations of the rules of conduct by police officers or cases of dishonesty on the part of law enforcement officers. The potential negative aspects of the use of electronic equipment that makes permanent video recording are singled out, namely that it can violate the privacy and confidentiality of citizens' lives; there is a risk of abuse of police video recordings, in particular, their illegal use, distribution or distortion of facts; the use of surveillance technology may be accompanied by technical problems, such as recording errors, system failures, data loss, which may affect the reliability and reliability of video recordings. In order to prevent the realization of such risks, it is necessary to establish clear rules and restrictions regarding the preservation, access and use of received video information in the patrol police; develop control mechanisms and internal rules to avoid possible abuses; to increase the level of technical support of these processes.

Key words: *cyber security, patrol police, personal data, right to privacy, confidential information, disclosure.*

Постановка проблеми. Під час збройної агресії проти України ще більше посилюється питання необхідності захисту персональних даних в роботі поліції, оскільки загроза виникає не лише праву на приватність особистого життя, а в першу чергу може спричинити загрозу особистій безпеці громадянина.

Патрульна поліція України, будучи підрозділом Національної поліції, який працює на користь громадян займається роботою з персональними даними осіб, відеофіксацією правопорушень та дорожньо-транспортних пригод. Діяльність патрульної поліції, пов'язана з захистом та обробкою персональних даних, здійснюється відповідно до Конституції України, Закону України «Про національну поліцію», «Про захист персональних даних» та інших відповідних законів України.

З огляду на швидке поширення інформаційних технологій у громадському житті в Україні та діяльності державних органів, все більшу важливість набуває забезпечення права громадян на недоторканність особистого та сімейного життя, яке гарантується статтею 32 Конституції України [1]. Однак, в процесі свого життя громадяни України, як члени суспільства, зобов'язані передавати деяку особисту інформацію державним органам для забезпечення реалізації їхніх прав державою. З свого боку, органи владних повноважень мають застосовувати заходи для захисту цих даних від розголошення. Ці заходи повинні бути в силі з моменту отримання відповідних даних і до їх знищення або їх знеособлення, або до отримання згоди особи, якій належать ці дані, на їх розголошення. Проте на практиці з'ясовуються деякі особливості застосування цих норм правоохоронними органами.

Так, протягом 2022 року Уповноваженим Верховної ради із захисту прав людини фіксувались такі порушення законодавства про захист персональних даних: неправомірна обробка персональних даних, зокрема їх неправомірне поширення та використання, незабезпечення надання суб'єкту персональних даних повної інформації щодо володільця персональних даних, неналежне оформлення згоди на обробку персональних даних, ненадання доступу до своїх персональних даних (інформації про себе), оприлюднення в мережі Інтернет персональних даних українських військових та іноземних громадян, які надають військову допомогу Україні на період дії воєнного стану, надмірний збір персональних даних надавачами гуманітарної, волонтерської та іншої благодійної допомоги населенню [2]. Деякі із зазначених проблем мали прояв і в інформаційному просторі патрульної поліції.

Національна поліція України, у тому числі патрульна поліція накопичують в межах своїх інформаційних систем та баз даних значні обсяги персональних даних: як роботодавці вони збирають, зберігають та використовують персональні дані своїх найманих працівників; як суб'єкти владних повноважень – персональні дані осіб, яким надають адміністративні послуги та персональні дані про осіб, щодо яких складаються протоколи про вчинені адміністративні правопорушення, та притягнутих до адміністративної відповідальності осіб.

Тому потребує постійного моніторингу діяльність з використання персональних даних в діяльності патрульної поліції, оскільки працівники цієї служби першими отримують

персональні дані свідків, правопорушників та потерпілих при виїзді на місце події.

Стан дослідження проблеми. Дослідженням питань правового регулювання забезпечення кібербезпеки поліції в Україні та окремих аспектів використання персональних даних поліцейськими займались такі вчені, як В. Батчев, Т. Білобров, О. Бочковий, В. Венгер, К. Галинська, Л. Єрьоміна, Н. Коваленко, А. Кошман, С.О. Прокопов, У. Шатська, О. Шевчук та інші. Проте на сьогодні відсутня сучасна узгоджена концепція правового регулювання кібербезпеки Національної поліції України загалом, та патрульної поліції зокрема, а питання забезпечення правил використання персональних даних в роботі патрульного поліцейського висвітлюються в науковій літературі фрагментарно.

Метою статті є визначення передбачених законодавством правил використання персональних даних громадян працівниками патрульної поліції при використанні відеореєстраторів та бодікамер; з'ясування в результаті аналізу практичної діяльності патрульної поліції позитивних та негативних аспектів використання таких засобів та напрацювання напрямів організаційно-правового удосконалення захисту персональних даних громадян в роботі патрульної поліції.

Виклад основного матеріалу. Відповідно до пункту 9 частини 1 статті 31 Закону України «Про Національну поліцію», одним із заходів превентивного характеру є використання технічних приладів і засобів, що мають функції фото- та відеозйомки. Відеореєстратори та бодікамери патрульних поліцейських є такими засобами. Відповідно до ст. 40 Закону України «Про Національну поліцію», «поліція для забезпечення публічної безпеки і порядку може закріплювати на форменому одязі такий пристрій, з метою «попередження, виявлення або фіксування правопорушення, охорони громадської безпеки та власності, забезпечення безпеки осіб» [3]. Наявність таких нагрудними камер розглядається працівниками патрульної поліції як засіб захистити себе від упереджених заяв щодо їхньої поведінки.

На сьогодні, констатує В. Батчев, поліція фіксує дії громадян використовуючи портативний нагрудний реєстратор, відеореєстратор у службовому авто, стаціонарні відеосистеми. При використанні цих засобів поліцейським забороняється: 1) самовільне видалення відеозаписів з носіїв, заміна цих носіїв, зміна їх системної дати та часу; 2) примусове виключення відеореєстраторів, у тому числі на вимогу сторонніх осіб; 3) перешкоджання здійсненню відеозапису; 4) використання відеореєстраторів у випадках, не пов'язаних із здійсненням повноважень поліції; 5) копіювання, передання інформації з відеореєстраторів стороннім особам. За фактами втрати або пошкодження відеореєстратора чи карти пам'яті, складових частин стаціонарної системи, проводиться службове розслідування [4].

Відповідно до п. 8 Інструкції із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису, передавання відеозаписів, отриманих з портативних та відеореєстраторів, установлених на службових транспортних засобах, БпЛА, автомобільних та стаціонарних систем для використання засобами масової інформації, а також поширення в мережі Інтернет, здійснюється з дозволу керівника органу, підрозділу поліції з дотриманням Закону України «Про захист персональних даних». Таке передавання здійснюється виключно з метою забезпечення безпеки та захисту інтересів громадян, суспільства і держави, а також з метою захисту гідності та честі працівника поліції [5]. Проте у законодавстві такі підстави не конкретизовані.

Відповідно до ч. 2 ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України» Національна поліція України забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від кримінально протиправних посягань у кіберпросторі; здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі [6]. Таким чином Національна поліція України є суб'єктом, що реалізує державну політику у сфері захисту персональних даних громадян. Цьому обов'язку протирічать факти поширення в соціальних мережах та в Інтернет відеозаписів із бодікамер патрульних поліцейських.

Вказані обмеження та вимоги щодо передавання відеозаписів з відеореєстраторів поліцейських, наголошує В. Батчев, є важливими для забезпечення захисту приватності громадян і уникнення можливого зловживання інформацією. Рішення на передавання відеозаписів для використання засобами масової інформації або поширення в Інтернеті залежить від дозволу керівника органу поліції. Це забезпечує контроль та відповідальність за використання цих записів та захист інтересів громадян, суспільства і працівників поліції. Головною метою передавання відеозаписів у цих випадках є забезпечення безпеки, захист інтересів громадян і громадського порядку, а також захист гідності і честі працівника поліції. Ці обмеження та процедури є важливими для

забезпечення балансу між ефективним використанням відеозаписів в розслідуванні злочинів та захистом приватності і прав громадян [4]. Додержання цих вимог сприяє підвищенню довіри до правоохоронних органів та забезпеченню належного захисту прав людини у контексті використання технологій нагляду та збору інформації.

Згідно з поглядами деяких юристів, захист, який забезпечується шляхом використання відеореєстраторів поліцією, може суперечити праву на приватність. В даний час, коли записи з цих реєстраторів публікуються самою поліцією на платформах, таких як YouTube, або передаються ЗМІ, інколи ці записи є фрагментарними, що може створювати упереджене уявлення про особу і порушувати презумпцію невинуватості. Крім того, правове регулювання автоматичної зйомки без згоди особи вважається недостатньо розробленим і може суперечити чинному законодавству. Зазначене правове регулювання також вважається недостатньо прозорим, оскільки вивчити його шляхом аналізу опублікованих нормативно-правових актів є неможливим. Неопубліковані службові акти Національної поліції, які визначають порядок застосування пристроїв, зберігання та режим доступу до відеозаписів, вважаються загрозою для дотримання поліцією прав людини на приватність [6].

У нашому законодавстві поняття «персональні дані» та «конфіденційна інформація» відіграють важливу роль щодо захисту права на приватність, а їх зміст та особливості використання визначені у Законах України «Про захист персональних даних», «Про доступ до публічної інформації», «Про інформацію» [8; 9; 10, с. 93; 11]. Конституційний суд та Міністерство юстиції України давали роз'яснення щодо конкретизації змісту цих даних та правил їх обігу [11; 12; 13; 14]. Таким чином, дані про національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження належать до конфіденційної інформації про фізичну особу. Збирання, зберігання та використання цих даних підлягають обмеженням і можуть здійснюватись лише згідно з вимогами закону та з відповідними

Відповідно до Наказу № 73 МВС, патрульна поліція України реалізувала інформаційно-аналітичну діяльність з метою забезпечення ефективності своєї роботи [15]. Ця діяльність включає створення власних баз даних, які є частиною єдиної інформаційної системи Національної поліції України та Міністерства внутрішніх справ України. Патрульна поліція має доступ до баз даних Національної поліції України, Міністерства внутрішніх справ України та інших державних органів. Це дозволяє патрульній поліції отримувати необхідну інформацію для виконання своїх функцій та забезпечувати безпеку громадян. Однак, використання персональних даних в роботі патрульної поліції підлягає відповідному регулюванню з метою забезпечення захисту приватності та прав людини відповідно до законодавства України.

На практиці мають місце порушення законодавства про захист персональних даних. Наприклад, за свідченнями колишніх працівників поліції є хибна практика працівників патрульної поліції на вимогу своїх безпосередніх керівників фотографувати всіх людей та їх документи, з якими працівники поліції взаємодіють під час несення служби для підтвердження показників по кількості опитаних громадян та громадян з якими проведено бесіди. Ця інформація передається у «Telegram» групи керівникові [16]. Це є грубим порушенням вимог Закону України «Про захист персональних даних». Патрульним поліцейським слід пам'ятати про заборону «виконувати злочинні чи явно незаконні розпорядження та накази», що зазначено у ст. 8 Закону України «Про Національну поліцію» [17].

Не лише Законом України «Про захист персональних даних» та Типовим порядком обробки персональних даних у базах персональних даних [18] закріплюється обов'язок працівників правоохоронних органів дотримуватись правил використання персональних даних, за якими можна ідентифікувати особу, і які мають характер конфіденційної інформації, як їх володільців чи розпорядників. Обов'язок осіб, уповноважених на виконання функцій держави не розголошувати і не використовувати в інший спосіб конфіденційну інформацію, що стала їм відома у зв'язку з виконанням своїх службових повноважень, крім випадків, встановлених законом, визначаються також як нами раніше зазначалось і етичними кодексами окремих відомств [19, с. 55].

Обов'язок патрульних поліцейських не розголошувати та не використовувати конфіденційну інформацію, включаючи персональні дані, які стали їм відомі у зв'язку з виконанням їхніх службових обов'язків, визначається Правилами етичної поведінки поліцейських [20]. Отже, патрульні поліцейські мають обов'язок поважати конфіденційність персональних даних, які стали їм відомі у ході виконання своїх службових обов'язків, і не використовувати їх неправомірно або розголошувати без належної підстави.

На сьогодні відеозаписи, отримані з відеореєстраторів і опубліковані без згоди на це особи, котра була об'єктом відеозапису, є порушенням норм Закону України «Про захист персональних даних». Така ситуація буде продовжуватись до внесення відповідних змін до Закону України «Про Національну поліцію» [10; с. 94].

Основним шляхом вирішення проблеми є врегулювання суперечностей законодавчої бази з цього питання. Однак це не має бути просте узгодження правових норм без зміни концепції автоматичної відеофіксації. Враховуючи принципи прав людини, зокрема права на приватність та практику Європейського суду з прав людини (*Peck v. the United Kingdom; Sciacca v. Italy*), доцільним було б застосовувати деперсоніфікацію. Тобто закриття обличчя особи, інформацію про П.І.Б. (зокрема озвученої патрульними), номерних знаків транспортних засобів, серії та номери документів, що посвідчують особу тощо. Крім того, мова може йти про інші особливості особи (татуювання, зачіска тощо) [3]. При цьому, така деперсоніфікація має бути здійснена ще до передачі такого відео третім особам, тобто вона має бути зроблена самою Національною поліцією України [10, с. 94].

Відсутність можливості деперсоналізації відеозапису створює перепони у використанні їх як доказів в судових справах. Наприклад, Дніпропетровський окружний адміністративний суд розглядав справу 160/11214/20 про визнання дій протиправними та зобов`язання вчинити певні дії за позовом фізичної особи до департаменту патрульної поліції Національної поліції України в частині надання неповної інформації згідно звернення (запиту) позивача від 12.02.2020 року, зареєстрованого за №М-1431, а саме: ненадання запису відеореєстратора в період з 11:28 до 15:00 20.01.2020 року, зі службового автомобіля, який прибув за викликом позивача на спеціальну лінію «102» здійсненого близько о 11:28 20.01.2020 року, (транспортний засіб 11*3781).

Позовні вимоги обґрунтовані тим, що позивач не погоджується з бездіяльністю відповідача щодо надання неповної інформації, запитуваної у зверненні від 12.02.2020 року. Відповідач заперечує можливість надання відеозапису оскільки він містить конфіденційну інформацію про третіх осіб, а відтак інформацію з обмеженим доступом. На підставі наведеного, враховуючи відсутність у відповідача технічної можливості деперсоніфікації зафіксованих на відеозаписах третіх осіб (тобто відсутність можливості вилучити з відеозапису інформацію з обмеженим доступом), з метою забезпечення прав та інтересів осіб, щодо яких вказані відомості містять таку інформацію, обмеженню підлягає доступ до відеозапису в цілому. На запитуваних відеозаписах з відеореєстратора, установленого у службовому автомобілі, а також з портативного відеореєстратора, закріпленого на одностроїстаршого лейтенанта поліції під час реагування на повідомлення міститься інформація про третіх осіб, а саме: відомості про таємницю особистого та сімейного життя, гарантовані Конституцією України та нормами законодавства щодо захисту персональних даних. Зважаючи на те, що у ДПП немає технічної можливості деперсоніфікації зафіксованих на відеозаписах третіх осіб, надання таких відеозаписів без їх згоди може завдати шкоду особистим правам та інтересам таких осіб. Зазначене обґрунтування суд визнав достатнім, також врахував строки зберігання таких відеозаписів та відмовив у задоволенні позову [21].

Судова практика також має приклади хибного сприйняття громадянами права на заборону використання їхніх персональних даних, а в окремих випадках – навіть зловживання відповідним правом [22]. Показовою тут може бути справа № 465/4390/17, у якій позивач (фізична особа) оскаржує дії начальника Управління патрульної поліції у м. Львові щодо надання його (позивача) персональних даних інженерові відділу з паркування Львівського комунального підприємства «Львівавтодор» для складення стосовно нього (позивача) протоколу про адміністративне правопорушення за порушення правил паркування. Суди першої [23], апеляційної [24] та касаційної інстанції дали належну правову оцінку цій ситуації та встановили, що порушень законодавства про захист персональних даних з боку начальника Управління патрульної поліції у м. Львові не було [25].

Упродовж 2022 року працівниками Секретаріату Уповноваженого було проведено 85 перевірок, спрямованих на дотримання законодавства про захист персональних даних. Перевірки охоплювали різні органи та установи, зокрема міністерства, центральні органи виконавчої влади, державні агентства, служби, органи місцевого самоврядування, органи соціального захисту населення, центри надання адміністративних послуг, авіапідприємства, підприємства житлово-комунального сектору, медичні заклади, благодійні фонди, бюро кредитних історій, інтернет-провайдери, бюро перекладів та інші. Під час перевірок здійснювалось дослідження стану дотримання прав людини на захист персональних даних.

За результатами проведених перевірок видано 75 приписів про усунення порушень, які є обов'язковими для виконання. Узагальнивши результати перевірок, можна виокремити такі типові порушення вимог законодавства про захист персональних даних: 1) не затверджено розпорядчий документ, яким визначено загальні вимоги до обробки та захисту персональних даних, або розпорядчий документ затверджено, проте він не відповідає вимогам законодавства, зокрема, у документі не визначено категорії суб'єктів персональних даних; склад персональних даних, який збирається щодо суб'єктів персональних даних; порядок обробки і захисту персональних даних; 2) неправильно визначено правові підстави для обробки персональних даних; 3) не всі суб'єкти персональних даних повідомляються про володільця персональних даних, склад та зміст зібраних персональних даних, їхні права, визначені законодавством, мету збору персональних даних та осіб, яким передаються їхні персональні дані; 4) не визначено план дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій; 5) не визначено процедуру знищення/видалення персональних даних, строк зберігання яких закінчився; 6) не ведеться облік операцій, пов'язаних з обробкою персональних даних [2].

Серед причин порушень безпеки обробки персональних даних У. Шадська виокремлює наступні: 1) відсутність розроблених і затверджених положень щодо безпеки персональних даних, які б відповідали потребам даного відомства/структурного підрозділу, а також національним і міжнародним стандартам у сфері захисту персональних даних; 2) низький кваліфікаційний рівень співробітників у сфері захисту персональних даних; 3) передача персональних даних по незахищених каналах зв'язку; 4) відсутність осіб, відповідальних за захист персональних даних; 5) не ведеться належний облік зібраної або переглянутої інформації, а також того, з якою метою і на яких законних підставах збираються і проглядаються дані [26].

За результатами опитування 231 патрульних поліцейських у Дніпропетровській області було з'ясовано, що майже 70% з них вважають, що персональні дані громадян складають основу наповнення баз даних, яку використовує патрульна поліція. Водночас, більшість респондентів вважають, що персональні дані громадян у базі даних патрульної поліції захищені – 79,7% і відповідно 20,3% вважають, що незахищені персональні дані громадян. Серед причин вказані такі: передавання із рук в руки; не доброчесність окремих працівників поліції; доступність персональних даних для корумпованих та зацікавлених співробітників; витоки інформації через технічні прилади; у зв'язку з паперовим обігом інформації. Серед опитаних патрульних поліцейських 70,1% вважають, що персональні дані патрульних в інформаційних системах патрульної поліції захищені, а 29,9% переконані, що незахищені. Серед причин «незахищеності» персональних даних вказана проблема в недобросовісних колегах [27]. Таким чином наведені факти вказують на необхідність конкретизації проблем у сфері забезпечення безпеки персональних даних в роботі патрульної поліції та шляхів їх вирішення.

Висновки. В ситуації з збройною агресією проти України захист персональних даних стає ще більш важливим і актуальним завданням. Витік персональних даних може мати серйозні наслідки не лише для приватного життя особи, але й для її особистої безпеки. Використання електронної техніки, що забезпечує безперервний відеозапис, у роботі поліції дійсно має як позитивні, так і потенційно негативні аспекти з позицій захисту прав людини. Важливо збалансувати ці аспекти та забезпечити належний рівень захисту особистої приватності та конфіденційності громадян.

З позитивних аспектів можна виділити наступне: 1) відеоматеріали можна використовувати як доказову базу у кримінальних розслідуваннях та судових процесах; вони можуть допомогти встановити обставини злочину, ідентифікувати злочинців і захистити права потерпілих; 2) знижується рівень корупції з боку працівників поліції, оскільки наявність відеозаписів може допомогти запобігти зловживанням з боку поліцейських, а також зменшити можливість випадкових або необґрунтованих затримань чи застосування надмірної сили; 3) відеозаписи можуть стати ефективним інструментом захисту прав громадян у випадках порушення правил поведінки поліцейськими або випадків прояву недобросовісності з боку правоохоронців.

Однак, є потенційні негативні аспекти, які необхідно також враховувати: 1) використання електронної техніки, що здійснює постійний відеозапис, може порушувати приватність та конфіденційність життя громадян, а тому необхідно встановлювати чіткі правила та обмеження щодо збереження, доступу та використання отриманої відеоінформації; 2) існує ризик зловживання відеозаписами поліції, зокрема, їх неправомірного використання, поширення або викривлення фактів, тому необхідно розробити механізми контролю та внутрішні правила, щоб уникнути

можливих зловживань; 3) використання техніки нагляду може супроводжуватись технічними проблемами, такими як помилки запису, збої системи, втрати даних тощо, що може вплинути на достовірність та надійність відеозаписів, тому необхідні підвищувати рівень технічного супроводження цих процесів.

Основними недоліками в організації та реалізації захисту персональних даних в патрульній поліції є : 1) незатверджений розпорядчий документ або розпорядчий документ, який не відповідає вимогам законодавства, тобто патрульна поліція не має затверджених документів, які б визначали загальні вимоги до обробки та захисту персональних даних; а наявні положення та інструкції не включають необхідну інформацію, зокрема, категорії суб'єктів персональних даних, склад збираних даних, порядок обробки та захисту; 2) неправильно визначені правові підстави для обробки, передання, оприлюднення, зберігання та знищення персональних даних; 3) відсутність у посадових інструкціях працівників патрульної поліції зобов'язання не розголошувати персональні дані; 4) відсутність методичних роз'яснень та інструкцій про алгоритми дотримання режимів інформації з обмеженим доступом, у тому числі персональних даних, в роботі патрульної поліції; 5) недостатня інформація для суб'єктів персональних даних, коли не всі суб'єкти персональних даних повідомляються про володільця персональних даних, склад і зміст зібраних даних, їхні права, мету збору та осіб, яким передаються їхні дані, відповідно до вимог законодавства; 6) відсутність плану дій на випадок несанкціонованого доступу, пошкодження технічного обладнання або надзвичайних ситуацій, що може підірвати безпеку персональних даних; 7) невизначена процедура знищення/видалення персональних даних, строк зберігання яких вже закінчився; 8) оприлюднення відеозаписів з бодікамер та автореєстраторів без згоди на поширення персональних даних (зображення) всіх учасників; 9) відсутність конкретизації дисциплінарної відповідальності за порушення правил захисту персональних даних патрульними поліцейськими та керівним складом.

Уповноважений ВР України рекомендував за результатами перевірок дотримання законодавства про захист персональних даних суб'єктам національної системи кібербезпеки, у тому числі Національній поліції України розробити і реалізувати запобіжні, організаційні, освітні заходи у сфері кібербезпеки, кібероборони та кіберзахисту з метою запобігання несанкціонованого доступу до персональних даних, зокрема, у зв'язку із збройною агресією Російської Федерації проти України, а Департаменту кіберполіції Національної поліції України опублікувати рекомендації серед громадян щодо безпеки в інтернеті від шахрайських дій [2].

На наш погляд, в першу чергу такі рекомендації повинні бути чітко доведені на відповідних тренінгах до працівників поліції, у тому числі працівників патрульної поліції. Це обумовлено необхідністю оперативного реагування працівників патрульної поліції як на інциденти пов'язані із кібербезпекою як самих працівників патрульної поліції, так і з оперативним наданням роз'яснень громадянам, які звертаються за допомогою при виявленні кіберзлочинів, вчинених щодо них.

Список використаних джерел:

1. Конституція України: Закон України від 28.06.96 р. Відомості Верховної Ради України. 1996. № 30. Стаття 141.

2. Доповідь про стан додержання та захисту прав і свобод людини і громадянина в Україні у 2022 році. Омбудсман України. URL: https://ombudsman.gov.ua/report-2022/images/documents/annual-report-2022.pdf

3. Нагрудна камера поліцейського – порушення права на приватність. URL: https://protocol.ua/ua/nagrudna_kamera_politseyskogo

4. Батчев В. Використання поліцією відеореєстраторів: що треба знати. URL: https://antydot.info/authors/vykorystannya-politsijeyu-videorejestratoriv-scho-treba-znaty/

5. Інструкція із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису: Наказ Міністерства внутрішніх справ України 18 грудня 2018 року № 1026. URL: https://zakon.rada.gov.ua/laws/show/z0028-19#Text

6. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. Голос України від 09.11.2017. № 208.

7. Нагрудна камера (відеореєстратор) патрульного: правове регулювання і порушення права на приватність. URL: http://umdpl.info/police-experts.info/2016/04/14/article-videofixation/

8. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI (у редакції від 19.10.2017). Відомості Верховної Ради України. 2010. № 34. Стор. 1188. Стаття 481.

9. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. Відомості Верховної Ради України. 2011. № 32. Стаття 314.

10. Інформаційне забезпечення діяльності патрульної поліції : наук.-практ. рекоменд. / О.В. Бочковий, Г.О. Блінова, С.О. Прокопов, Е.А. Мамедова. Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2020. 98 с.

11. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. Відомості Верховної Ради України. 1992. № 48. Стаття 650.

12. Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К. Г. Устименка) від 30 жовтня 1997 року № 5-зп. у справі 18/203-97. [Електронний ресурс]. URL: zakon.rada.gov.ua/laws/show/v005p710-97.

13. Рішення Конституційного Суду України 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 № 1-9/2012 від 20 січня 2012 року № 2-рп/2012. [Електронний ресурс]. URL: zakon.rada.gov.ua/go/v002p710-12.

14. Деякі питання практичного застосування Закону України «Про захист персональних даних»: Роз'яснення Міністерства юстиції України від 21.12.2011 р. [Електронний ресурс]. URL: http://zakon2.rada.gov.ua/laws/show/n0076323-11.

15. Наказ № 73, від 06.11.2015 «Про затвердження Положення про Департамент патрульної поліції»,

16. Захист прав поліцейських. [Електронний ресурс]. URL: https://www.facebook.com/groups/1535431980081968

17. Про Національну поліції: Закон України від 02 липня 2015 року № 580-VIII. Відомості Верховної Ради України. 2015. № 40-41. ст.379.

18. Типовий порядок обробки персональних даних: Наказ Уповноваженого Верховної Ради України з прав людини 08.01.2014 № 1/02-14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text

19. Блінова Г.О. Адміністративно-правові засади інформаційного забезпечення органів публічної адміністрації в Україні: актуальні питання теорії та практики. Дис. на здобут. наук. ступ. докт. Юрид. наук. Запоріжжя. 2019. 458 с.

20. Про затвердження Правил етичної поведінки поліцейських. Наказ Міністерства внутрішніх справ України 09.11.2016 № 1179. URL: https://zakon.rada.gov.ua/laws/show/z1576-16#Text

21. Рішення Дніпропетровського окружного адміністративного суду № 93431021 від 07.12.2020. URL: https://youcontrol.com.ua/ru/catalog/court-document/93431021/

22. Венгер В., Кошман А., Шевчук О. Аналіз судової практики щодо застосування законодавства України про захист персональних даних. URL: https://rm.coe.int/report-dp-2021-2web-/1680aa5225

23. Рішення Франківського районного суду м. Львова у справі № 465/4390/17 від 26.12.2017 року. URL: https://reyestr.court. gov.ua/Review/71439748.

24. Постанова Львівського апеляційного адміністративного суду у справі № 465/4390/17 від 14 травня 2018 року. URL: https://reyestr.court.gov.ua/Review/74098229.

25. Постанова Верховного Суду у справі № 465/4390/17 від 13 жовтня 2020 року. URL: https://reyestr.court.gov.ua/ Review/92173101.

26. Шадська У. Захист персональних даних в діяльності Національної поліції України. Експертний центр з прав людини. URL: https://ecpl.com.ua/comments/zahyst-personalnyh-danyh-v-diyalnosti-natsionalnoji-politsiji-ukrajiny/

27. Аналітичний звіт «Адміністративно-правові засади забезпечення кібербезпеки патрульної поліції України» за результатами опитування патрульних поліцейських. Наукова лабораторія соціологічних та кримінально-правових досліджень ННІ ЗНПК. Дніпро 2023. 37 с.