УДК 342.7

https://doi.org/10.52058/3041-1254-2026-1(23)-97-106

Гаделія Віталій Романович аспірант Інституту держави і права імені В.М.Корецького НАН України, керівник адвокатського бюро "Віталій Гаделія та партнери", https://orcid.org/0009-0003-8435-7989

ПРОБЛЕМИ КОНСТИТУЦІЙНО-ПРАВОВОГО РЕГУЛЮВАННЯ ВПРОВАДЖЕННЯ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ ОРГАНАМИ МІСЦЕВОГО САМОВРЯДУВАННЯ

Анотація

Вступ. Автономність місцевого самоврядування закладена Європейської хартією місцевого самврядування [1]. Однак, в своїй діяльності органи місцевого самоврядування збирають, обробляють, розповсюджують безліч персональних даних, зокрема відеозображення особи. В той же час, так обробка персональних даних повинна здійснюватись у відповідності до законодавства України і практики Європейського суду з прав людини.

Мета. Метою даною статті є дослідження діяльності органів місцевого самоврядування в сфері запровадження комплексних систем відеоспостереження.

Матеріали і методи. Матеріалами дослідження є: 1) нормативно-правове забезпечення щодо регулювання конституційно-правового забезпечення приватності, в тому числі і зарубіжні джерела; 2) праці вітчизняних та зарубіжних авторів, що провадять свої науково-практичні дослідження приватності та воєнного стану.

В процесі здійснення дослідження було використано наступні наукові методи: теоретичного узагальнення та групування (для характеристики порядку збору, обробки, розповсюдження та використання персональних даних при здійсненні органами влади своїх повноважень); формалізації, аналізу та синтезу; логічного узагальнення результатів (формулювання висновків).

Результати. У науковій статті розкрито проблемні питання втручання в приватність органами органами місцевого самоврядування, а також надані рекомендації щодо їх вирішення.

Перспективи. В подальших наукових дослідженнях пропонується зосередити увагу на проблемних питання порядку збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди іншими органами державної влади та приватними юридичними особами, а також шляхів їх вирішення.

Ключові слова: право на приватність, конфіденційність, право на недоторканність приватного життя, право на недоторканність особистого і сімейного життя, персональні дані, конфіденційні дані, ідентифікація, органи місцевого самоврядування**.**

Hadelia Vitalii Romanovych Postgraduate student at the V.M. Koretsky Institute of State and Law of the National Academy of Sciences of Ukraine, Head of the law firm "Vitalii Hadelia and Partners", https://orcid.org/0009-0003-8435-7989

PROBLEMS OF CONSTITUTIONAL AND LEGAL REGULATION OF THE IMPLEMENTATION OF VIDEO SURVEILLANCE SYSTEMS BY LOCAL GOVERNMENTS

Abstract

Introduction. The autonomy of local self-government is established by the European Charter of Local Self-Government. However, in their activities, local self-government bodies collect, process, and disseminate a vast amount of personal data. At the same time, such processing of personal data must be carried out in accordance with the legislation of Ukraine and the practice of the European Court of Human Rights.

Objective. The objective of this article is to investigate the activities of local self-government bodies in the field of personal data processing.

Materials and Methods. The research materials are: 1) legal framework regulating the constitutional and legal safeguarding of privacy, including foreign sources; 2) works of domestic and foreign authors conducting scientific and practical research on privacy and martial law. In the process of conducting the research, the following scientific methods were used: theoretical generalization and grouping (to characterize the procedure for collecting, processing, disseminating, and using personal data during the exercise of powers by government bodies); formalization, analysis, and synthesis; logical generalization of results (formulating conclusions).

Results. The scholarly article reveals the problematic issues of interference with privacy by local self-government bodies, and provides recommendations for their resolution.

Perspectives. Future scholarly research is proposed to focus attention on the problematic issues related to the procedure for collecting, storing, using, and disseminating confidential information about an individual without their consent by other state authorities and private legal entities, as well as ways to resolve them.

Keywords: right to privacy, confidentiality, right to inviolability of private life, right to inviolability of personal and family life, personal data, confidential data, identification, local self-government bodies.

Постановка проблеми. Автономність органів місцевого самоврядування, яке є гарантованим Європейською хартією місцевого самоврядування і статтею 7 Конституції України [2].

Однак, в той же час, органи місцевого самоврядування повинні діяти на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України.

Однією з конституційних вимог, є саме законодавче регулювання баз даних, які стосуються конфіденційних даних. Запровадження комплексних систем відеоспостереження в містах вимагає наявності закону, який регулює порядок збирання, обробки, зберігання, розповсюдження та видалення такого специфічного виду персональних даних як відеозображення особи. Такі дані можуть допомогти органам правопорядку розслідувати кримінальні правопорушення. Однак, в той же час, неврегульованість даного питання, несе в собі ризики визнання зібраних доказів недопустимими.

В той же час, органи місцевого самоврядування приймають локальні нормативно-правові акти, які замінюють собою конституційну вимогу наявності саме регулювання у формі закону.

На вищевказану правову проблему вказано і в роз'ясненні Уповноваженого Верховної Ради України з прав людини, де зокрема також підкреслено що “існують проблеми правового регулювання щодо встановлення систем відеоспостереження з боку місцевої влади, оскільки у профільному Законі України «Про місцеве самоврядування в Україні» [3] відсутні прямі повноваження щодо встановлення технологій стеження за населенням” [4].

Аналіз останніх досліджень і публікацій.

Правовими проблемами відеоспостереження, які організуються органами місцевого самоврядування, досліджували, зокрема, Ольга Шпакович та Мартін Скурек в своїй роботі The Legal Regulation of the Facial Recognition and Real-Time Remote Biometric Identification Systems in Ukraine and the Czech Republic [15] описали логіку прийняття законодавства в сфері масового відеоспостереження в Україні та Чеській Республіці. Джон Фасман в своїй книзі *We See It All: Liberty and Justice in an Age of Perpetual Surveillance* [20] дослідив загрози приватності в сучасному світі, зокрема і в сфері масового відеоспостереження.

Метою статті є дослідження конституційно-правових проблем в сфері приватності, які стосуються запровадженням комплексних систем відеоспостереження органами місцевого самоврядування.

Виклад основного матеріалу.

Однією з конституційних проблем в сфері місцевого самоврядування є те, що **випадки** збирання, зберігання, використання та поширення конфіденційної інформації про особу визначитись повинні саме **законом** (стаття 32 Конституції України).

А якщо взяти до уваги, що в сукупності з пунктом пунктом 12 частини 1 статті 92 Конституції України виключно законами України визначаються організація і діяльність органів виконавчої влади, основи державної служби, організації державної статистики та **інформатики**, то порядок і підстави збирання конфіденційної інформації про особу повинне мати конкретне саме законодавче підґрунтя.

Таким чином, наразі впровадження систем відеоспостереження відбувається без однієї з ключових "тріад правомірності втручання в приватність", а саме: законності.

Наразі, багато міст України прийняли локальні нормативно-правові акти щодо безпеки міст, зокрема положення про комплексні системи відеоспостереження міст (наприклад, рішення Київської міської ради від 5 липня 2018 року N 1195/5259 [5]).

Дане рішення було прийнято на підставі законів України "Про місцеве самоврядування в Україні", "Про місцеві державні адміністрації"[2] [6], "Про інформацію" [7], "Про електронні комунікації" [8], "Про захист інформації в інформаційно-комунікаційних системах" [9], "Про захист персональних даних" [10], "Про електронні документи та електронний документообіг" [11].

Однак, в жодному з цих законів немає прямих повноважень ні органів місцевого самоврядування, ні державних адміністрацій вести публічне відеоспостереження за місцевістю, збирати, зберігати та розповсюджувати такі конфіденційні дані про осіб.

В рішенні від 11 грудня 2014 року у справі František Ryneš C-212/13 (пункт 22) Суд справедливості ЄС дійшов висновку, що зображення особи, записане системою камер, є персональними даними, відповідно до статті 2(a) Директиви 95/46 [12]. Отже, збір таких даних є втручанням в приватну сферу і для правомірності, крім принципу законності, ще потрібно дотримуватися принципу пропорційності.

Отримати доступ на підставі вмотивованого звернення можуть :

- **Місцева влада:** Посадовці Київради, КМДА, райдержадміністрацій та комунальних підприємств Києва.
- **Органи правопорядку:** СБУ (центральне управління та ГУ у м. Києві), МВС, Нацполіція (апарат та ГУ у м. Києві), Нацгвардія .
- **Охоронні організації:** Управління державної охорони (УДО) та ліцензовані охоронні фірми, які охороняють конкретні об'єкти (тільки за письмовим зверненням керівника) .
- **Рятувальники:** ДСНС України та ГУ ДСНС у м. Києві .

[2] Закон України Про місцеві державні адміністрації, URL:https://zakon.rada.gov.ua/laws/show/586-14#Text

- **Страховики:** Представники МТСБУ (Моторне (транспортне) страхове бюро України).

Однак, в більшості профільних законів, які регулюють діяльність перелічених органів, відсутні законодавчі повноваження на отримання такого доступу. В зазначеному порядку також відсутні гарантії від необгрунтованого втручання чи зловживаннях, адже не передбачено незалежний орган, котрий міг би перевіряти такий доступ, а також перелік випадків, коли такий доступ буде правомірним (наприклад, тяжкість розслідування злочину).

Покращити правове регулювання даної сфери міг стати законопроект №11031 від 20.02.2024 Про єдину систему відеомоніторингу стану публічної безпеки [13].

Проєктом Закону передбачалось унормувати:

"*єдині функціональні та технічні вимоги до побудови та функціонування систем відеомоніторингу стану публічної безпеки центрального, регіонального та місцевого рівнів, відомчих систем відеомоніторингу підприємств, установ організацій (незалежно від форм власності) та фізичних осіб, установлених у публічних місцях, порядок доступу до інформації, а також складу відеоданих, метаданих, аналітичних даних, відеоархівів, сигналів тривог, що створюються ними; забезпечення єдиних правил інформаційного обміну на державному, регіональному та місцевому рівнях між суб'єктами єдиної системи відеомоніторингу стану публічної безпеки через єдиний інформаційний простір з урахуванням розмежування прав доступу до інформації; захисту інформації, у тому числі персональних даних у системах відеомоніторингу стану публічної безпеки центрального, регіонального та місцевого рівнів та відомчих системах відеомоніторингу підприємств, установ організацій (незалежно від форм власності) та фізичних осіб, установлених у публічних місця*" [14].

В той же час, Комітет ВРУ з питань інтеграції України до Європейського Союзу встановив, що законопроєкт №11031 має фундаментальні вади: він дозволяє надмірне збирання та довгострокове (до 15 років) зберігання персональних і біометричних даних, не містить прозорого опису процесів ідентифікації та роботи алгоритмів, не забезпечує принципи мінімізації, пропорційності й обмеження цілей, не встановлює технічних стандартів, процедурних гарантій, механізмів незалежного контролю та нагляду, допускає потенційно незаконне використання технологій розпізнавання обличчя, у тому числі в реальному часі, що суперечить законодавству ЄС та створює ризик масового стеження, зловживань і «охолоджуючого ефекту» щодо свободи зібрань і вираження поглядів; у підсумку Комітет визнав проєкт несумісним із європейським правом і міжнародними зобов'язаннями України. Пізніше, даний законопроект був відкликаний.

Щодо даного законопроекту є досить цікавим зауваження Мартіна Скурека та Ольги Шпакович. В своїй статті вони, зокрема, зазначили, що на прикладі в

Чеської Республіки, зроблено висновок, що AI Act дозволяє використання систем дистанційної біометричної ідентифікації в реальному часі, але за певних умов. Основною з них є те, що використання такої системи для пошуку конкретної особи чи осіб має бути санкціоноване судом або іншим незалежним органом. Фактично це означає, що рішення про включення конкретної особи до довідкової бази даних має ухвалюватися судом. Однак, щодо цієї дуже важливої гарантії проти зловживання системою, Закон № 110/2019 Зб. про обробку персональних даних пропонує, що це правило не застосовується до певних відносно нечітко визначених груп осіб. Таким чином, на їх думку, цей Закон фактично нівелює цей фундаментальний механізм контролю в певних випадках [15].

Ще одним з законопроектів, який покликаний унормувати дане питання, є законопроект про захист персональних даних номер 8153 від 25.10.2022 [16]. Однак, в даній статті так само не унормовано повноваження органів місцевого самоврядування на відеоспостереження.

Як зазначено у правовому висновку Ради Європи на проєкт закону “про захист персональних даних (№8153 від 25 жовтня 2022 року) є ряд зауважень, які вказують на незрозумілість терміну «особа, яка здійснює відеоспостереження» у проєкті Закону [17].

Верховний комісар ООН з прав людини, Фолькер Тюрк, зазначив, що такі технології можуть призвести до «масового стеження за нашими публічними просторами, знищуючи будь-яке поняття приватності» [18]. Обробка біометричних даних з використанням технологій розпізнавання обличчя в реальному часі за відсутності належної правової основи та законної мети може порушувати право на приватність, гарантоване статтею 32 Конституції України, яка захищає кожного громадянина від втручання в його приватне та сімейне життя.

В той же час, в Конституції України відсутні гарантії щодо пропорційного втручання в приватне життя, що може призвести до надмірного збору персональних даних.

Джон Фасман, наприклад, вважає, що відбувається "розмивання мети" (Mission Creep), оскільки технології, придбані для боротьби з тероризмом, згодом починають використовуватися для переслідування за дрібні провини.

Можливість “відмотати назад” результат масового відеоспостереження, дозволяє реконструювати приватне життя конкретної людини, дізнатись уподобання людини, коло спілкування, звички. Тому відсутність “розумних строків” зберігання такої інформації створює ризики утворення надмірного масиву даних, які дозволяли б створити цифровий портрет особи і знайти шляхи для впливу на неї.

Таким чином, без дотримання принципу необхідності в демократичному суспільстві (пропорційності), існує ризик формування суспільства, в якому “все на увазі, карається і ніщо не забувається”.

Amnesty International, неурядова організація, що об'єднує понад 7 мільйонів людей по всьому світу та присвячена запобіганню серйозним порушенням прав людини, також розпочала глобальну компанію за заборону використання систем розпізнавання обличчя для масового спостереження. На думку цієї організації, невибіркове масове спостереження ніколи не є пропорційним втручанням [19].

В той же час, стаття 32 Конституції України створює певне поле для дискусії, оскільки дозволяє збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди лише в інтересах національної безпеки, економічного добробуту та прав людини. Яким чином визначається інтерес національної безпеці, економічного добробуту та прав людини?

Якщо припустити, що розмежування йде за видом кримінального правопорушення, наприклад загрози національній безпеці згруповані в розділі I Особливої частини Кримінального кодексу України «Кримінальні правопорушення проти основ національної безпеки України» (статті 109–114² Кримінального кодексу України), а загрозу правам людини становлять злочини проти життя, свободи, гідності, рівності, приватності та політичних прав (розділи II–V ККУ), то що, наприклад, робити зі складами кримінальних правопорушень, які формально не входять в ці розділи?

Наприклад, частина 4 статті 321 Кримінального кодексу України формально не відноситься ні до кримінальних правопорушень у сфері національної безпеки, ні до злочинів які становлять загрозу економічному добробуту чи правам людини. Чи дозволено тоді збір конфіденційної інформації про особу відповідно до положень статті 32 Конституції України? Вбачається, що такий підхід у вигляді розмежування випадків правомірності втручання у приватність в залежності від виду правпорушення суперечиться європейському підходу у вигляді розмежування у вигляді тяжкості вчиненого правопорушення.

Отже, наразі питання комплексного відеоспостереження міст є невирішеним законодавчо, що є прямим порушенням Конституції України і створює безліч ризиків порушення права на повагу до приватності органами місцевого самоврядування і місцевих державних адміністрацій. Також, така неунормованість несе загрозу визнання зібраних доказів недопустими і впливає напряму на забезпечення ефективного досудового розслідування і покарання винних. В той же час, потрібно чітко визначитись на законодавчому рівні: що є пропорційним втручанням в приватність у випадку масового відеоспостереження.

Література:

1. Європейська хартія місцевого самоврядування [Електронний ресурс]. Рада Європи, Страсбург, 15.10.1985 р. URL: https://zakon.rada.gov.ua/laws/show/994_036#Text .

2. Конституція України [Електронний ресурс] : Закон України від 28.06.1996 № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.

3. Про місцеве самоврядування в Україні [Електронний ресурс] : Закон України від 21.05.1997 № 280/97-ВР. *Відомості Верховної Ради України*. 1997. № 24. Ст. 170. URL: https://zakon.rada.gov.ua/laws/show/280/97-%D0%B2%D1%80#Text.

4. [Роз'яснення Уповноваженого Верховної Ради України з прав людини] [Електронний ресурс]. URL: https://ombudsman.gov.ua/storage/app/media/%D0%97%D0%9F%D0%94/rozyasnennya.pdf

5. Про затвердження Положення про Комплексну систему відеоспостереження міста Києва [Електронний ресурс] : Рішення Київської міської ради від 05.07.2018 № 1195/5259. URL: https://ips.ligazakon.net/document/MR181017.

6. Про місцеві державні адміністрації [Електронний ресурс] : Закон України від 09.04.1999 № 586-XIV. *Відомості Верховної Ради України*. 1999. № 20–21. Ст. 190. URL: https://zakon.rada.gov.ua/laws/show/586-14#Text.

7. Про інформацію [Електронний ресурс] : Закон України від 02.10.1992 № 2657-XII. *Відомості Верховної Ради України*. 1999. № 27. Ст. 238. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

8. Про електронні комунікації [Електронний ресурс] : Закон України від 16.12.2020 № 1089-IX. *Відомості Верховної Ради України*. 2021. № 3. Ст. 20. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text.

9. Про захист інформації в інформаційно-комунікаційних системах [Електронний ресурс] : Закон України від 05.07.1994 № 80/94-ВР. *Відомості Верховної Ради України*. 1994. № 31. Ст. 282. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

10. Про захист персональних даних [Електронний ресурс] : Закон України від 01.06.2010 № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

11. Про електронні документи та електронний документообіг [Електронний ресурс] : Закон України від 22.05.2003 № 851-IV. *Відомості Верховної Ради України*. 2003. № 36. Ст. 275. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text.

12. František Ryneš v Úřad pro ochranu osobních údajů [Електронний ресурс] : Case C-212/13. Court of Justice of the European Union, Grand Chamber. 11.12.2014. URL: https://curia.europa.eu/juris/document/document.jsf?docid=160561&doclang=EN .

13. Про єдину систему відеомоніторингу стану публічної безпеки [Електронний ресурс]: Проєкт Закону України № 11031 від 20.02.2024. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/43733.

14. [Пояснювальна записка до Проєкту Закону № 11031] [Електронний ресурс]. URL: https://itd.rada.gov.ua/billinfo/Bills/pubFile/2219955.

15. The Legal Regulation of the Facial Recognition and Real-Time Remote Biometric Identification Systems in Ukraine and the Czech Republic [Електронний ресурс]. URL: https://www.researchgate.net/publication/396808270_The_Legal_Regulation_of_the_Facial_Recogniti_on_and_Real-Time_Remote_Biometric_Identification_Systems_in_Ukraine_and_the_Czech_Republi_C .

16. Про захист персональних даних [Електронний ресурс] : Проєкт Закону України № 8153 від 25.10.2022. URL: https://itd.rada.gov.ua/billinfo/Bills/CardByRn?regNum=8153&conv=9.

17. Правовий висновок Ради Європи до проєкту Закону України «Про захист персональних даних» (реєстр. № 8153) [Електронний ресурс]. URL: https://itd.rada.gov.ua/billinfo/Bills/pubFile/1804763.

18. UN High Commissioner says facial recognition could lead to 'destruction of privacy' [Електронний ресурс] : [стаття] / В. Тюрк. 2023. URL: https://www.biometricupdate.com/202307/un-high-commissioner-says-facial-recognition-could-lead-to-destruction-of-privacy?fbclid=IwAR0gXV41kaFwdSP27miiuYBMVQwDJUW0CCIJYe0wZ_qdKgOk6N_Ff4tfkkeA .

19. Ban dangerous facial recognition technology that amplifies racist policing [Електронний ресурс] : [стаття] / Amnesty International. 2021. URL: https://www.amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/

20. Fasman, Jon**.** *We See It All: Liberty and Justice in an Age of Perpetual Surveillance*. PublicAffairs, 2021

21. Кримінальний кодекс України [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2341-14#n2227

References:

1. Council of Europe. (1985, October 15). *Yevropeis'ka khartiia mistsevoho samovriadvannia* [European Charter of Local Self-Government]. URL: https://zakon.rada.gov.ua/laws/show/994_036#Text.

2. Verkhovna Rada of Ukraine. (1996, June 28). *Konstytutsiia Ukrainy* [The Constitution of Ukraine] (Law No. 254k/96-VR). *Vidomosti Verkhovnoi Rady Ukrainy*, *1996*(30), Art. 141. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.

3. Verkhovna Rada of Ukraine. (1997, May 21). *Pro mistseve samovriadvannia v Ukraini* [On Local Self-Government in Ukraine] (Law No. 280/97-VR). *Vidomosti Verkhovnoi Rady Ukrainy*, *1997*(24), Art. 170. URL: https://zakon.rada.gov.ua/laws/show/280/97-%D0%B2%D1%80#Text.

4. Ukrainian Parliament Commissioner for Human Rights. (*n.d.*). [*Roz'iasnennia Upovnovazhenoho Verkhovnoi Rady Ukrainy z prav liudyny*] [Clarification of the Ukrainian Parliament Commissioner for Human Rights]. URL: https://ombudsman.gov.ua/storage/app/media/%D0%97%D0%9F%D0%94/rozyasnennya.pdf.

5. Kyiv City Council. (2018, July 5). *Pro zatverdzhennia Polozhennia pro Kompleksnu systemu videosposterzhennia mista Kyieva* [On the Approval of the Regulation on the Integrated Video Surveillance System of the City of Kyiv] (Decision No. 1195/5259). URL: https://ips.ligazakon.net/document/MR181017.

6. Verkhovna Rada of Ukraine. (1999, April 9). *Pro mistsevi derzhavni administratsii* [On Local State Administrations] (Law No. 586-XIV). *Vidomosti Verkhovnoi Rady Ukrainy*, *1999*(20–21), Art. 190. URL: https://zakon.rada.gov.ua/laws/show/586-14#Text.

7. Verkhovna Rada of Ukraine. (1992, October 2). *Pro informatsiiu* [On Information] (Law No. 2657-XII). *Vidomosti Verkhovnoi Rady Ukrainy*, *1999*(27), Art. 238. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

8. Verkhovna Rada of Ukraine. (2020, December 16). *Pro elektronni komunikatsii* [On Electronic Communications] (Law No. 1089-IX). *Vidomosti Verkhovnoi Rady Ukrainy*, *2021*(3), Art. 20. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text.

9. Verkhovna Rada of Ukraine. (1994, July 5). *Pro zakhyst informatsii v informatsiino-komunikatsiinykh systemakh* [On Protection of Information in Information and Communication Systems] (Law No. 80/94-VR). *Vidomosti Verkhovnoi Rady Ukrainy*, *1994*(31), Art. 282. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

10. Verkhovna Rada of Ukraine. (2010, June 1). *Pro zakhyst personalnykh danykh* [On Personal Data Protection] (Law No. 2297-VI). *Vidomosti Verkhovnoi Rady Ukrainy*, *2010*(34), Art. 481. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

11. Verkhovna Rada of Ukraine. (2003, May 22). *Pro elektronni dokumenty ta elektronnyi dokumentoobih* [On Electronic Documents and Electronic Document Management] (Law No. 851-IV). *Vidomosti Verkhovnoi Rady Ukrainy*, *2003*(36), Art. 275. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text.

12. Court of Justice of the European Union. (2014, December 11). *František Ryneš v Úřad pro ochranu osobních údajiv* (Case C-212/13). URL: https://curia.europa.eu/juris/document/document.jsf?docid=160561&doclang=EN.

13. Verkhovna Rada of Ukraine. (2024, February 20). *Proekt Zakonu Ukrainy Pro yedynu systemu videomonitorynhu stanu publichnoi bezpeky* [Draft Law of Ukraine On the Unified Public Security Video Monitoring System] (Draft Law No. 11031). URL: https://itd.rada.gov.ua/billinfo/Bills/Card/43733.

14. Verkhovna Rada of Ukraine. (2024). *Poiasniuvalna zapyska do Proektu Zakonu № 11031* [Explanatory Note to Draft Law No. 11031]. URL: https://itd.rada.gov.ua/billinfo/Bills/pubFile/2219955.

15. The Legal Regulation of the Facial Recognition and Real-Time Remote Biometric Identification Systems in Ukraine and the Czech Republic. (*n.d.*). URL: https://www.researchgate.net/publication/396808270_The_Legal_Regulation_of_the_Facial_Recogniti_on_and_Real-Time_Remote_Biometric_Identification_Systems_in_Ukraine_and_the_Czech_Republi_C.

16. Verkhovna Rada of Ukraine. (2022, October 25). *Proekt Zakonu Ukrainy Pro zakhyst personalnykh danykh* [Draft Law of Ukraine On Personal Data Protection] (Draft Law No. 8153). URL: https://itd.rada.gov.ua/billinfo/Bills/CardByRn?regNum=8153&conv=9.

17. Verkhovna Rada of Ukraine. (2023). *Pravovyi vysnovok Rady Yevropy do proektu Zakonu Ukrainy «Pro zakhyst personalnykh danykh»* [Legal Opinion of the Council of Europe on the Draft Law of Ukraine "On Personal Data Protection"] (Draft Law No. 8153). URL: https://itd.rada.gov.ua/billinfo/Bills/pubFile/1804763.

18. Turk, V. (2023). *UN High Commissioner says facial recognition could lead to 'destruction of privacy'* [Article]. URL: https://www.biometricupdate.com/202307/un-high-commissioner-says-facial-recognition-could-lead-to-destruction-of-privacy?fbclid=IwAR0gXV41kaFwdSP27miiuYBMVQwDJUW0CCIJYe0wZ_qdKgOk6N_Ff4tfkkeA.

19. Amnesty International. (2021). *Ban dangerous facial recognition technology that amplifies racist policing*. URL: https://www.amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/.

20. Fasman, Jon. *We See It All: Liberty and Justice in an Age of Perpetual Surveillance*. PublicAffairs, 2021

21. Kryminalnyi kodeks Ukrainy [Criminal Code of Ukraine]. Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#n2227