ДОСЛІДНИЦЬКА СЛУЖБА
ВЕРХОВНОЇ РАДИ УКРАЇНИ

Парламентське дослідження щодо стандартів Європейського Союзу та Ради Європи із захисту та обробки персональних даних у правоохоронній діяльності

2026

Парламентське дослідження щодо стандартів Європейського Союзу та Ради Європи із захисту та обробки персональних даних у правоохоронній діяльності*

Анотація. *Парламентське дослідження містить аналіз стандартів Ради Європи та Європейського Союзу у сфері захисту персональних даних у межах діяльності поліції та органів кримінальної юстиції. Матеріал систематизує міжнародно-правові акти та практику Європейського суду з прав людини (ЄСПЛ), що формують єдиний європейський правовий простір захисту інформаційної приватності.*

Розкрито сутність втручання у право на приватність через «трискладовий тест» та встановлено обов'язок володільців персональних даних диференціювати дані за категоріями осіб (підозрювані, засуджені, потерпілі, свідки) і характером інформації («тверді» факти проти «м'яких» оцінок). Деталізовано особливий (чутливий) статус даних про кримінальні вироки, наголошено на реабілітаційній меті обробки даних та неприпустимості довічної стигматизації засудженого. Обґрунтовано вимогу щодо диференційованих строків зберігання біометричних даних залежно від тяжкості правопорушення. На основі позицій ЄСПЛ доведено юридичну недопустимість автоматичних обмежень прав осіб (зокрема, ув'язнених) суто на підставі їхнього формального статусу без персоналізованого аналізу поточної небезпеки.

Окреслено критерії незалежності наглядових органів, їх слідчі та корегувальні повноваження, а також право громадян на ефективний судовий захист і компенсацію матеріальної та моральної шкоди. Надано рекомендації щодо удосконалення національного законодавства, зокрема в частині чіткого розмежування загального та правоохоронного регулювання захисту й обробки персональних даних і впровадження принципу підзвітності (accountability) органів влади.

Ключові слова: *правомірність втручання, «тверді» та «м'які» персональні дані, індивідуалізована оцінка ризиків, обробка даних про засудження, оцінка впливу на захист даних, спеціаліст із захисту даних, ДНК-профіль, відбитки пальців, наглядовий орган.*

Зміст

Вступ

Швидкий розвиток інформаційних технологій і тотальна цифровізація суспільних відносин зумовили докорінну зміну підходів до захисту приватності. У сучасних умовах персональні дані стали стратегічним ресурсом, а їх обробка правоохоронними органами та органами кримінальної юстиції набула безпрецедентних масштабів, що створює нові виклики для захисту основоположних прав і свобод людини. Європейський простір сьогодні очолює світовий рух за встановлення суворих стандартів «інформаційної приватності», базуючись на принципах підзвітності та прозорості.

Актуальність дослідження зумовлена статусом України як кандидата на членство в Європейському Союзі (далі – ЄС), що покладає на державу зобов'язання щодо повної гармонізації національного законодавства з *acquis communautaire* ЄС. Особливої гостроти означене питання набуває у сфері діяльності поліції та органів кримінального судочинства, де втручання у приватне життя особи є найбільш інтенсивним і вимагає чіткого балансу між інтересами громадської безпеки та людською гідністю. Впровадження таких інструментів, як Директива (ЄС) 2016/680 (Police Directive)[1] та Модернізована Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108+)[2], визначає нову юридичну реальність, у якій правоохоронні органи зобов'язані доводити легітимність кожного акту обробки даних на всіх етапах їх життєвого циклу. Окремим пріоритетом у межах Дорожньої карти з питань верховенства права[3] є імплементація системи ECRIS (Європейська інформаційна система кримінальних проваджень) та ECRIS-TCN (для громадян третіх країн), що базуються на Рамковому рішенні 2009/315/JHA[4], Регламенті (ЄС) 2019/816[5] та Директиві (ЄС) 2019/884[6]. Ці акти визначають правила транскордонного обміну даними про засудження особи.

Також у контексті виконання міжнародно-правових зобов'язань щодо адаптації законодавства України до положень права Європейського Союзу (acquis ЄС) та реалізації стратегічного курсу на європейську інтеграцію пунктом

---

[1] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. URL: https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng

[2] Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108+). URL: https://zakon.rada.gov.ua/laws/show/994_326#Text

[3] Дорожня карта з питань верховентсва права. URL: https://eu-ua.kmu.gov.ua/wp-content/uploads/UA_Dorozhnya_karta_z_pytan_verhovenstva_prava_2.pdf

[4] COUNCIL FRAMEWORK DECISION 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States. URL: https://eur-lex.europa.eu/eli/dec_framw/2009/315/oj/eng

[5] REGULATION (EU) 2019/816 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726. URL: https://eur-lex.europa.eu/eli/reg/2019/816/oj/eng

[6] DIRECTIVE (EU) 2019/884 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third-country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA. URL: https://eur-lex.europa.eu/eli/reg/2019/884/oj/eng

322 Плану законопроєктної роботи Верховної Ради України на 2026 рік[7] передбачено розроблення проєкту Закону про інформаційно-аналітичну систему «Облік відомостей про притягнення особи до кримінальної відповідальності та наявності судимості». Зазначена законодавча ініціатива має на меті практичне запровадження європейських стандартів обробки даних про засудження особи за вчинення кримінального правопорушення, що зумовлює необхідність ґрунтовного аналізу положень зазначеного вище законодавства ЄС для забезпечення легітимності майбутнього регулювання відносин у сфері захисту та обробки персональних даних.

Деякі питання захисту персональних даних розкрито в таких інформаційно-аналітичних матеріалах Дослідницької служби як Інформаційна довідка щодо забезпечення захисту персональних даних відповідно до міжнародних стандартів прав людини[8] та Аналітична записка з питань порівняльного законодавства щодо збору біометричних даних осіб та відображення їх у паспортних документах в Європейському Союзі та державах-членах ЄС[9].

Метою цього дослідження є створення комплексного аналітичного підґрунтя для розробки та вдосконалення національних нормативно-правових актів у сфері захисту персональних даних задля формування сучасної системи захисту даних, яка би передбачала:

- чітке розмежування загального регулювання та спеціальних правил для правоохоронного сектору;
- запровадження дієвих механізмів підзвітності (accountability) володільців персональних даних;
- забезпечення інституційної незалежності наглядового органу відповідно до європейських стандартів;
- імплементацію правових позицій ЄСПЛ щодо індивідуалізованої оцінки ризиків та пропорційності строків зберігання чутливої інформації.

Предмет дослідження – стандарти Європейського Союзу та Ради Європи із захисту та обробки персональних даних у правоохоронній діяльності.

Нове законодавство у сфері захисту персональних даних та їх обробки дозволить Україні не лише виконати міжнародні зобов'язання, а й гарантуватиме громадянам рівень захисту прав, співмірний із найкращими європейськими практиками.

Європейські стандарти захисту персональних даних, включаючи акти Ради Європи та ЄС, їх вплив на національне законодавство, перспективи

---

[7] План законопроектної роботи Верховної Ради України на 2026 рік, затверджений Постановою Верховної Ради України від 10 лютого 2026 року № 4774-IX. URL: https://zakon.rada.gov.ua/laws/show/4774-20#n16

[8] Інформаційна довідка щодо забезпечення захисту персональних даних відповідно до міжнародних стандартів прав людини. *Дослідницька служба Верховної Ради України*. URL: https://research.rada.gov.ua/documents/analyticRSmaterialsDocs/hum_social_policy/inform_references-hsp/76146.html

[9] Аналітична записка з питань порівняльного законодавства щодо збору біометричних даних осіб та відображення їх у паспортних документах в Європейському Союзі та державах-членах ЄС. *Дослідницька служба Верховної Ради України*. URL: https://research.rada.gov.ua/documents/analyticRSmaterialsDocs/industry_policy/analytical_notes-indst/73855.html?search

гармонізації є предметом наукового пошуку українських[10] та закордонних[11] науковців.

Окрім того, порушена тематика перебуває у фокусі пріоритетних напрямів роботи Комітету Верховної Ради України з питань правоохоронної діяльності.

Основна частина

1. Система нормативно-правових актів (джерела права) у сфері захисту та обробки персональних даних.

Нормативно-правова база захисту персональних даних (далі також – ПД) у правоохоронній сфері ґрунтується на архітектурі актів Ради Європи (РЄ) та законодавства Європейського Союзу, що формують єдиний європейський простір захисту основоположних прав.

Акти Ради Європи, якими врегульовано захист і обробку персональних даних.

Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108+) є єдиним юридично зобов'язальним міжнародним договором, що охоплює обробку ПД як у державному, так і в приватному секторах. Стаття 6 Конвенції спеціально регулює обробку чутливих даних, включаючи дані про правопорушення та кримінальні вироки, дозволяючи її лише за наявності належних законодавчих гарантій[12].

Європейська конвенція з прав людини (ЄКПЛ) – це фундаментальний акт, стаття 8 якого захищає право на повагу до приватного і сімейного життя. Судова практика ЄСПЛ розглядає захист даних як невід'ємну складову «інформаційної приватності»[13].

Рекомендація № R(87)15 Комітету Міністрів РЄ – спеціалізований документ, що встановлює принципи використання ПД у поліцейському секторі.

---

[10] Різенко О. В. Європейські правові стандарти захисту персональних даних. *Аналітично-порівняльне правознавство.* № 6 (2024). DOI: https://doi.org/10.24144/2788-6018.2024.06.105; Рубля О. С. Нормативно-правове регулювання захисту персональних даних органами публічної влади. *Наукові записки.* Серія: Право. № 19. 2025. DOI: https://doi.org/10.36550/2522-9230-2025-19-348-352; Шевчук О. О. Правове регулювання охорони персональних даних в Європейському Союзі : дис. ... канд. юрид. наук : 12.00.11 / Київський національний університет імені Тараса Шевченка. Київ, 2021. 214 с. URL: https://scc.knu.ua/upload/iblock/4a6/dis_Shevchuk%20O.%20O..pdf; Мервінський О., Мельник К. Правові аспекти організації захисту персональних даних у сфері правоохоронної діяльності відповідно до міжнародних стандартів. *Наукові вісті НТУУ "КПІ".* 2015. № 5. С. 34–41. URL: https://ela.kpi.ua/server/api/core/bitstreams/29a199d7-5abc-43e0-845d-a989fb0b1339/content;Пальчик М. Л., Шкрібляка К. П., Березецький Ю. М. Захист персональних даних як елемент національної безпеки в умовах воєнного стану. Юридичний науковий електронний журнал. 2025. № 12. С. 280–284. URL: https://app-journal.in.ua/wp-content/uploads/2025/12/71-1.pdf та ін.

[11] Juraj Sajfert, Teresa Quintel. Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3285873&utm ; Leiser, M.R. and Custers, B.H.M. (2019) The Law Enforcement Directive: Conceptual Issues of EU Directive 2016/680, European Data Protection Law Review. Vol. 5, nr. 3, p. 367-378. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4014545&utm ; Cécile de Terwangne. Council of Europe convention 108+: A modernised international treaty for the protection of personal data. URL: https://www.sciencedirect.com/science/article/abs/pii/S0267364920301023?utm; Sajfert J., Quintel T. Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities. ResearchGate. 2019. URL: https://orbilu.uni.lu/bitstream/10993/38833/1/SSRN-id3285873%20%282%29.pdf та ін.

[12] Convention for the protection of individuals with regard to the processing of personal data. URL: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

[13] European Convention on Human Rights. URL: https://www.echr.coe.int/documents/d/echr/convention_eng

Він вимагає чіткого розрізнення між даними, що ґрунтуються на фактах, та даними, що базуються на підозрах або оцінках[14].

Конвенція про кіберзлочинність (Будапештська конвенція) – регулює процесуальні повноваження щодо збору електронних доказів. Стаття 15 зобов'язує сторони забезпечити належний захист прав людини та ПД під час застосування цих повноважень[15].

Законодавство Європейського Союзу у сфері захисту персональних даних.

Хартія основоположних прав Європейського Союзу – її стаття 7 гарантує право на приватність, а стаття 8 виокремлює захист персональних даних (ПД) як самостійне основоположне право. Вона вимагає, щоб обробка була чесною, здійснювалася для визначених цілей та перебувала під контролем незалежного органу[16].

Договір про функціонування Європейського Союзу (ДФЄС) – стаття 16 надає ЄС прямі повноваження встановлювати правила захисту ПД у всіх сферах діяльності Союзу, включаючи правоохоронне та судове співробітництво в кримінальних справах[17].

Регламент (ЄС) 2016/679 (General Data Protection Regulation – GDPR) (Загальний регламент про захист персональних даних) – є основним актом для цивільного та комерційного секторів. Стаття 10 встановлює суворі умови для обробки даних про кримінальні вироки поза правоохоронною сферою (тільки під контролем державних органів або за наявності спеціальних гарантій)[18].

Регламент (ЄС) 2018/1725 (Про захист фізичних осіб у зв'язку з обробкою персональних даних інституціями, органами, офісами та агентствами Союзу) – цей акт гармонізує правила захисту даних всередині структур ЄС (зокрема, агентства eu-LISA) із принципами GDPR та Директиви 2016/680[19].

Регламент (ЄС) 2023/2854 (Data Act) (Закон Європейського Союзу про дані) – регулює доступ до даних пристроїв Інтернету речей (IoT). Пункт 10 Преамбули уточнює, що цей акт не зачіпає повноваження правоохоронних органів щодо збору електронних доказів[20].

---

[14] Recommendation no.r (87) 15 of the Committee of Ministers to Member States Regulating the Use of Personal Data in the Police Sector. URL: https://rm.coe.int/0900001680929718

[15] Convention on Cybercrime, Budapest, 23.XI.2001. URL: https://rm.coe.int/1680081561

[16] Charter of Fundamental Rights of the European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

[17] Consolidated version of the Treaty on the Functioning of the European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT

[18] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1770645156485

[19] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1725

[20] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). URL: https://eur-lex.europa.eu/eli/reg/2023/2854/oj

Директива (ЄС) 2016/680 (Police Directive) (Про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами з метою запобігання, розслідування, виявлення чи переслідування за вчинення кримінальних правопорушень) – її стаття 4 закріплює принципи обробки, а стаття 10 – особливі умови для обробки генетичних, біометричних даних та даних про судимості[21].

Регламент (ЄС) 2019/816 (ECRIS-TCN Regulation) (Про створення централізованої системи для ідентифікації держав-членів, що володіють інформацією про засудження громадян третіх країн та осіб без громадянства (ECRIS-TCN)) – документ регулює обробку біометричних даних (відбитків пальців та зображень обличчя) і вимагає суворого ведення логів[22].

Директива (ЄС) 2019/884 (Про внесення змін до Рамкового рішення 2009/315/ ЈНА щодо обміну інформацією про громадян третіх країн та щодо Європейської інформаційної системи кримінальних проваджень (ECRIS)) – гармонізує транскордонний обмін даними про судимість із сучасними стандартами захисту ПД[23].

Рамкове рішення Ради 2009/315/ЈНА (Про організацію та зміст обміну інформацією з реєстрів судимостей між державами-членами) – це базовий акт, на якому побудована вся система ECRIS[24].

2. Сутність права на приватність та правова природа персональних даних.

Концепція втручання у право на приватність.

Збирання та використання персональних даних поліцією для правоохоронних цілей становить пряме втручання у право на приватне життя, гарантоване статтею 8 ЄКПЛ та статтею 7 Хартії ЄС. У сфері кримінальної юстиції будь-яке збирання чи зберігання персональних даних поліцією розглядається як втручання, оскільки воно передбачає вилучення особистої інформації з приватної сфери індивіда для публічних цілей.[25] Таке втручання є правомірним лише за умови *дотримання «трискладового тесту»: воно має*

---

[21] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680

[22] REGULATION (EU) 2019/816 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726. URL: https://eur-lex.europa.eu/eli/reg/2019/816/oj/eng

[23] Directive (EU) 2019/884 of the European Parliament and of the Council of 17 April 2019 amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third-country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA. URL: https://eur-lex.europa.eu/eli/reg/2019/884/oj/eng

[24] COUNCIL FRAMEWORK DECISION 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States. https://eur-lex.europa.eu/eli/dec_framw/2009/315/oj/eng

[25] Посібник з європейського права у сфері захисту персональних даних. URL: https://rm.coe.int/handbook-on-european-data-protection-law-ukr/1680a0689b

бути передбачено законом, переслідувати легітимну мету й бути необхідним у демократичному суспільстві.

Людська гідність є фундаментом, що вимагає, аби засуджені не розглядалися як об'єкти обробки даних, а їхні права поважалися навіть в умовах позбавлення волі[26].

Юридичне визначення персональних даних та категорії осіб.

Персональні дані – це будь-яка інформація, що стосується ідентифікованої або такої, яку можна ідентифікувати, фізичної особи. Органи кримінальної юстиції зобов'язані чітко розрізняти ПД таких категорій суб'єктів: підозрюваних, засуджених, потерпілих та свідків[27].

Також необхідно чітко диференціювати «тверді» дані (факти) та «м'які» дані (особисті оцінки, підозри, розвідка). Персональні дані про засудження належать до чутливих категорій, що вимагають посиленого захисту[28].

3. Принципи та підстави обробки персональних даних компетентними органами.

Фундаментальні принципи обробки даних.

Обробка персональних даних має відповідати принципам, визначеним у Директиві (ЄС) 2016/680 (стаття 4) [29] та Конвенції 108+ (стаття 5)[30]: *законність та чесність* (обробка має ґрунтуватися на праві ЄС або держави-члена); *обмеження мети* (збір для чітких легітимних цілей без несумісної подальшої обробки); *мінімізація* (ПД мають бути адекватними та обмеженими суворою необхідністю); *точність* (обов'язок виправляти або видаляти неточні дані без затримки); *обмеження зберігання* (дані не зберігаються довше, ніж це необхідно для цілей обробки); *безпека* (захист від несанкціонованої обробки технічними заходами); *підзвітність* (володілець персональних даних відповідальний за дотримання принципів і повинен це продемонструвати).

Підстави обробки даних.

Юридична правомірність обробки персональних даних вимагає дотримання таких встановлених законом підстав:

виконання завдань у суспільних інтересах – обробка законна лише тоді, коли вона необхідна для виконання завдання компетентним органом на підставі права;

дисбаланс сил та недійсність згоди – у правоохоронній сфері згода суб'єкта персональних даних зазвичай не розглядається як дійсна правова

---

[26] Посібник із судової практики ЄКПЛ: Права ув'язнених. URL: https://ks.echr.coe.int/documents/d/echr-ks/guide_prisoners_rights_ukr

[27] Директива (ЄС) 2016/680. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680

[28] Конвенція 108+. URL: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

[29] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680

[30] Конвенція 108+. URL: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

підстава. Це зумовлено нерівністю між державою та особою, де остання часто зобов'язана надати дані за законом;

здійснення офіційних повноважень – компетентні органи діють як володільці персональних даних, наділені владними повноваженнями вимагати виконання законних вимог[31].

Особливості обробки даних про засудження та реабілітаційна мета. Обробка даних про засуджених має специфічні стандарти:

1. *Спеціальний статус:* дані про засудження належать до чутливих категорій; їх обробка дозволяється лише під контролем офіційного органу влади або за наявності чітких законодавчих гарантій згідно зі статтею 10 GDPR[32].

Відповідно до Регламенту (ЄС) 2019/816 функціонування централізованої системи ECRIS-TCN передбачає створення державами-членами детальних записів про засуджених громадян третіх країн та осіб без громадянства, що включають алфавітно-цифрові дані (прізвища, імена, дату та місце народження, громадянство, стать), а також відбитки пальців та, за наявності технічної можливості й дозволу національного права, зображення обличчя.

Обробка такої інформації вимагає суворого дотримання принципів якості та точності даних, що реалізується через такі механізми:

обов'язок перевірки та верифікації: компетентні органи зобов'язані вживати всіх розумних заходів для забезпечення точності та актуальності даних у момент їх внесення, а агентство eu-LISA має впроваджувати автоматизовані механізми контролю якості та регулярного звітування;

динамічна модифікація та синхронізація: будь-яка зміна інформації в національному реєстрі судимостей, яка стала підставою для створення запису в ECRIS-TCN, тягне за собою ідентичну модифікацію даних у центральній системі державою, що винесла вирок, без неналежної затримки;

безумовне видалення у разі скасування вироку: у разі скасування судового рішення або виправдання особи, дані повинні бути негайно виправлені або повністю видалені з центральної системи для забезпечення принципу точності;

процедура оскарження неточностей: якщо будь-яка держава-член має підстави вважати дані в системі неточними або такими, що обробляються незаконно, вона зобов'язана негайно поінформувати державу, що винесла вирок, яка, своєю чергою, має невідкладно розпочати процедуру перевірки;

автоматизація обмеження строків зберігання: записи зберігаються в системі лише доти, доки відповідна інформація міститься в національному реєстрі судимостей, а після закінчення цього строку дані (включаючи біометрію) повинні бути видалені автоматично або не пізніше ніж через місяць.

---

[31] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[32] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Окремим елементом підзвітності є обов'язкове ведення логів (logging) усіх операцій збору, зміни та видалення даних, що дозволяє ідентифікувати посадову особу, час та обґрунтування кожного акту обробки. Такий підхід гарантує суб'єкту даних право на ефективний захист, включаючи право на отримання письмового підтвердження про вжиті заходи щодо виправлення чи видалення його персональних відомостей[33].

2. *Реабілітаційна мета:* європейська пенітенціарна політика наголошує, що обробка персональних даних має сприяти соціальній реінтеграції засудженого. Будь-яке тримання персональних даних у реєстрах не повинно перетворюватися на довічну стигматизацію[34].

3. *Біометрія та ДНК:* зберігання профілів ДНК та відбитків пальців засуджених суворо обмежене принципом необхідності; безстрокове зберігання даних осіб, які були виправдані або не засуджені, є порушенням статті 8 ЄКПЛ[35].

4. *Корекція за зміною статусу:* у разі скасування вироку чи виправдання особи володілець персональних даних зобов'язаний видалити або виправити записи негайно для забезпечення принципу точності.

Визначення балансу між безпекою та приватністю (правові позиції ЄСПЛ).

Принцип індивідуалізованої оцінки ризиків є фундаментальною вимогою ЄСПЛ, він гарантує, що права ув'язнених не обмежуються автоматично лише на підставі їхнього статусу чи тяжкості вчиненого злочину. Згідно з практикою Суду дія Конвенції не припиняється «біля воріт в'язниці», і будь-які обмеження мають бути суворо обґрунтовані конкретними обставинами справи[36].

Індивідуальна оцінка ризиків запобігає автоматизму в таких аспектах.

Відмова від обмежень за статусом: ЄСПЛ неодноразово визнавав неприпустимими норми, які запроваджують автоматичні обмеження (наприклад, на кількість побачень) для всіх засуджених певної категорії, таких як довічно ув'язнені[37]. У справі *«Хорошенко проти Росії»* Суд установив, що суворий режим, який застосовувався до заявника протягом десяти років лише через його статус, без урахування особистої поведінки, порушив право на сімейне життя[38].

Забезпечення пропорційності: індивідуальний підхід вимагає від влади розробляти системи оцінки для балансування особистих і громадських інтересів. Наприклад, при організації побачень влада має враховувати конкретну ситуацію (відстань до дому, наявність дітей), а не просто посилатися на загальний розклад.

---

[33] REGULATION (EU) 2019/816 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726. URL: https://eur-lex.europa.eu/eli/reg/2019/816/oj/eng

[34] Посібник із судової практики ЄКПЛ: Права ув'язнених. URL: https://ks.echr.coe.int/documents/d/echr-ks/guide_prisoners_rights_ukr

[35] Рішення ЄСПЛ у справі S. and Marper v. the United Kingdom. URL: http://hudoc.echr.coe.int/eng?i=001-89958

[36] Посібник із судової практики ЄКПЛ: права ув'язнених. URL: https://ks.echr.coe.int/documents/d/echr-ks/guide_prisoners_rights_ukr

[37] Там само.

[38] Рішення ЄСПЛ у справі Khoroshenko v. Russia. URL: http://hudoc.echr.coe.int/eng?i=001-155632

Регулярний перегляд заходів: особливі режими безпеки не можуть застосовуватися нескінченно. Влада зобов'язана проводити повторну експертизу, враховуючи зміни у поведінці особи.

Захист уразливих категорій: принцип індивідуалізації критично важливий для осіб із психічними розладами. Для них недостатньо діагнозу; влада має надати індивідуальну програму лікування, спрямовану на реабілітацію.

Стримування застосування сили: використання засобів стримування (наручників) не повинно бути рутинною практикою. Індивідуальна оцінка потребує конкретних підстав вважати, що ув'язнений може втекти чи проявити агресію.

Свобода совісті та релігії: формальний підхід, що ігнорує індивідуальну ситуацію ув'язненого при обмеженні релігійних обрядів, є неприпустимим.

Судова практика щодо обробки даних про засуджених:

1) S. and Marper v. the United Kingdom: ЄСПЛ установив, що «всеосяжний і нерозбірливий» характер повноважень щодо зберігання ДНК-профілів та відбитків пальців осіб, які були підозрюваними, але не були засуджені, не забезпечує справедливого балансу інтересів. Суд підкреслив, що безстрокове зберігання таких чутливих даних осіб, чия винуватість не доведена, становить порушення статті 8 ЄКПЛ[39];

2) B.B. v. France: ЄСПЛ визнав законним включення засуджених за сексуальні злочини до національної бази даних, оскільки воно супроводжувалося належними гарантіями: правом суб'єкта вимагати видалення, обмеженим доступом та встановленими строками зберігання. Це підтверджує, що втручання є пропорційним, якщо існують механізми перегляду необхідності зберігання даних[40];

3) Brunet v. France: ЄСПЛ установив порушення через 20-річний строк зберігання ПД особи у базі поліції, кримінальне провадження щодо якої було закрито без вироку. Суд визнав такий строк надмірним за відсутності реальної можливості видалення даних і належного судового контролю[41];

4) Aycaguer v. France: ЄСПЛ постановив, що відмова видалити персональні дані ДНК-профілів навіть засуджених осіб без диференціації за тяжкістю злочину та без визначення конкретної тривалості зберігання є порушенням статті 8 ЄКПЛ[42].

4. Права та обов'язки суб'єктів під час обробки їх персональних даних.

У європейському правопорядку суб'єкт даних (зокрема, підозрюваний або засуджений) наділений комплексом прав, що дозволяють йому зберігати контроль над власною інформацією, тоді як на правоохоронні органи покладаються суворі обов'язки щодо підзвітності[43].

Права суб'єкта даних (включаючи засуджених).

---

[39] Рішення ЄСПЛ у справі «S. and Marper v. the United Kingdom». URL: http://hudoc.echr.coe.int/eng?i=001-89958
[40] Рішення ЄСПЛ у справі «B.B. v. France». URL: http://hudoc.echr.coe.int/eng?i=001-96350
[41] Рішення ЄСПЛ у справі «Brunet v. France». URL: http://hudoc.echr.coe.int/eng?i=001-146382
[42] Рішення ЄСПЛ у справі «Aycaguer v. France». URL: http://hudoc.echr.coe.int/eng?i=001-174434
[43] Посібник з європейського права у сфері захисту персональних даних (2018). URL: https://rm.coe.int/handbook-on-european-data-protection-law-ukr/1680a0689b

Згідно з розділом III Директиви (ЄС) 2016/680[44] та статтею 9 Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних суб'єкт даних має такі права.

Право на інформацію та прозорість (стаття 13 Директиви): володілець персональних даних зобов'язаний надати інформацію про обробку у стислій, прозорій та доступній формі. Це включає: ідентичність і контактні дані володільця персональних даних; контактні дані спеціаліста із захисту даних (DPO); цілі та юридичні підстави обробки ПД; строк зберігання даних або критерії його визначення; наявність права подати скаргу до наглядового органу.

Право на доступ (стаття 14 Директиви): суб'єкт даних має право отримати підтвердження факту обробки та копію своїх ПД. Зокрема, він має право знати про категорії даних, одержувачів (кому дані передані) та наявність автоматизованого прийняття рішень, включаючи профайлінг (із наданням змістовної інформації про логіку такого процесу).

Право на виправлення, видалення та обмеження (стаття 16 Директиви). Виправлення: володілець персональних даних повинен без надмірної затримки виправити неточні або доповнити неповні ПД. Видалення («право бути забутим»): дані мають бути видалені, якщо обробка порушує закон або якщо дані більше не потрібні для цілей кримінального правосуддя. Обмеження обробки: замість видалення суб'єкт даних може вимагати обмежити використання даних, якщо їх точність оскаржується або вони мають зберігатися як докази.

Специфічні права ув'язнених: навіть в умовах позбавлення волі засуджені зберігають право на конфіденційність медичних даних та кореспонденції з адвокатом. Будь-яке обмеження цих прав має бути індивідуалізованим та обґрунтованим.

Обов'язки володільців персональних даних (поліції та органів юстиції).

Правоохоронні органи як володільці персональних даних несуть відповідальність за дотримання стандартів обробки (принцип підзвітності).

Ведення логів (стаття 25 Директиви): у всіх автоматизованих системах обробки обов'язково фіксуються операції: збір, зміна, ознайомлення, розкриття (включаючи передачу), поєднання та видалення. Логи мають дозволяти ідентифікувати особу, яка зверталася до даних, час операції та обґрунтування запиту. Логи використовуються виключно для перевірки законності обробки та гарантування цілісності даних.[45]

Для систем обміну інформацією про судимості (ECRIS-TCN) встановлено обов'язок зберігати логи всіх операцій із даними відповідно до статті 31 Регламенту (ЄС) 2019/816. Логи мають фіксувати факт доступу, ідентифікацію особи, що зверталася, дату, час та обґрунтування запиту.

Оцінка впливу на захист даних (Data Protection Impact Assessment, DPIA) (стаття 27 Директиви): якщо тип обробки (особливо з використанням нових

[44] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680

[45] Директива (ЄС) 2016/680. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680

технологій, таких як розпізнавання облич) може призвести до високого ризику для прав осіб, володілець персональних даних зобов'язаний провести попередню оцінку впливу. Вона включає систематичний опис операцій, аналіз їх необхідності та пропорційності, а також заходи безпеки для пом'якшення ризиків[46].

Попередня консультація (стаття 28 Директиви): у разі, якщо DPIA вказує на наявність високого ризику, який володілець персональних даних не може самостійно пом'якшити, він зобов'язаний проконсультуватися з наглядовим органом до початку обробки.

Спеціаліст із захисту даних (DPO) (стаття 32 Директиви): призначення DPO є обов'язковим для правоохоронних органів. Ця особа діє незалежно, не отримує вказівок від керівництва щодо виконання своїх завдань і є контактною для суб'єктів даних та наглядового органу. DPO моніторить відповідність закону та надає поради персоналу.

Безпека та конфіденційність (стаття 29 Директиви): володілець персональних даних повинен впроваджувати технічні заходи (шифрування, псевдонімізацію) та організаційні заходи (доступ лише уповноваженим особам) для захисту від незаконного доступу чи втрати даних.

Основні європейські стандарти захисту персональних даних представлені на Рис. 1*.

[46] Практичний посібник з використання персональних даних у поліцейському секторі. URL: https://rm.coe.int/practical-guide-on-the-use-of-personal-data-in-the-police-sector/1680792701)

* Рисунок згенеровано за допомогою ШІ.


ОСНОВНІ ЄВРОПЕЙСЬКІ СТАНДАРТИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ
1. ЗАКОННІСТЬ ТА СПРАВЕДЛИВІСТЬ
Обробка ПД може здійснюватися лише на підставі закону, є необхідною та пропорційною для досягнення конкретних цілей кримінальної юстиції та правоохоронної діяльності.
2. ОБМЕЖЕННЯ ЦІЛЕЙ
ПД збираються для чітко визначених, законних цілей і не можуть оброблятися далі у спосіб, несумісний з цими цілями.
3. МІНІМІЗАЦІЯ ДАНИХ
Обробляються лише ті ПД, які є адекватними, релевантними та необхідними для досягнення зазначених цілей.
4. ОБМЕЖЕННЯ ЗБЕРІГАННЯ
ПД зберігаються у формі, що дозволяє ідентифікувати особу, не довше, ніж це необхідно для цілей обробки, після чого підлягають видаленню або анонімізації.
ЗАХИСТ ПРАВ І СВОБОД ФІЗИЧНИХ ОСІБ ПРИ ОБРОБЦІ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ КРИМІНАЛЬНОЇ ЮСТИЦІЇ ТА ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ
5. ЦІЛІСНІСТЬ ТА КОНФІДЕНЦІЙНІСТЬ
ПД обробляються з дотриманням належного рівня безпеки, включаючи захист від несанкціонованого доступу, втрати, зміни або розкриття.
6. ПРАВА СУБ'ЄКТА ДАНИХ
Особа має право на інформацію, доступ, виправлення, видалення або обмеження обробки своїх ПД, а також право подати скаргу до наглядового органу.
ДОДАТКОВІ ЄВРОПЕЙСЬКІ СТАНДАРТИ
7. ПІДЗВІТНІСТЬ (Відповідальність)
Володілець ПД зобов'язаний демонструвати відповідність принципам захисту даних та забезпечувати їх дотримання.
8. ОЦІНКА ВПЛИВУ (DPIA)
Перед впровадженням обробки з високим ризиком для прав осіб проводиться оцінка впливу на захист даних.
9. НЕЗАЛЕЖНИЙ НАГЛЯД
Незалежні наглядові органи здійснюють контроль та мають ефективні корегувальні повноваження.
10. ЕФЕКТИВНИЙ ЗАХИСТ ТА САНКЦІЇ
Особи мають право на судовий захист та компенсацію шкоди, а порушення тягнуть за собою ефективні, пропорційні та стримувальні санкції.
Ці стандарти ґрунтуються на Конвенції Ради Європи 108+, Директиві (ЄС) 2016/680 (Police Directive), Регламенті (ЄС) 2016/679 (GDPR) та практиці Європейського суду з прав людини.

Рис. 1.

5. Контроль, нагляд та відповідальність у сфері захисту даних.

Незалежний нагляд є фундаментальною гарантією європейського правопорядку, що забезпечує й гарантування захисту прав фізичних осіб у цифрову еру, особливо в системі кримінальної юстиції, де ризики втручання є найвищими.

Незалежний нагляд: статус та повноваження органів. Згідно зі статтею 8(3) Хартії основоположних прав ЄС та статтею 16(2) ДФЄС контроль за дотриманням правил захисту ПД повинен здійснюватися незалежним органом[48]. Кожна держава-член зобов'язана створити один або декілька незалежних наглядових органів (DPAs). На рівні інституцій, органів та агентств ЄС (зокрема, Європолу та Євроюсту) нагляд здійснює Європейський інспектор із захисту даних (EDPS).[49]

Критерій «повної незалежності»: наглядові органи повинні діяти абсолютно об'єктивно, бути вільними від будь-якого зовнішнього (прямого чи опосередкованого) впливу та не запитувати і не приймати інструкцій від урядів чи інших суб'єктів[50].

Судова практика: Суд ЄС у справах *Комісія проти Німеччини (C-518/07)* та *Комісія проти Австрії (C-614/10)* підтвердив, що державний нагляд за наглядовим органом або призначення персоналу через міністерства порушує вимогу незалежності[51].

Функціональні повноваження: органи нагляду наділені комплексом інструментів:

слідчі повноваження – право отримувати доступ до всіх ПД та інформації, необхідної для виконання завдань, а також доступ до будь-яких приміщень володільця персональних даних[52];

корегувальні повноваження – винесення попереджень, доган, наказів про приведення обробки у відповідність до вимог, встановлення тимчасової або остаточної заборони на обробку, наказ про виправлення або видалення даних[53];

дорадчі повноваження – надання висновків парламенту та уряду щодо законодавчих заходів, які стосуються захисту ПД.

Згідно зі статтею 29(2) Регламенту (ЄС) 2019/816 Європейський інспектор із захисту даних (EDPS) зобов'язаний забезпечувати проведення регулярного незалежного аудиту діяльності агентства eu-LISA щодо обробки персональних даних у межах системи ECRIS-TCN.

Для забезпечення високої якості та прозорості контролю цей процес включає такі специфічні вимоги:

періодичність і стандарти: аудит має проводитися не рідше ніж один раз на три роки відповідно до визнаних міжнародних стандартів аудиту;

---

[48] Хартія основоположних прав ЄС. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

[49] Директива (ЄС) 2016/680 (Police Directive). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680 ; Регламент (ЄС) 2018/1725. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1725

[50] Модернізована Конвенція 108+. URL: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

[51] Посібник з європейського права у сфері захисту персональних даних (2018). URL: https://rm.coe.int/handbook-on-european-data-protection-law-ukr/1680a0689b

[52] Директива (ЄС) 2016/680. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680

[53] Загальний регламент про захист даних (GDPR). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

підзвітність і розповсюдження результатів: за результатами перевірки готується детальний звіт, який направляється Європейському Парламенту, Раді ЄС, Європейській Комісії, самому агентству eu-LISA, а також національним наглядовим органам держав-членів;

процесуальні гарантії: перед остаточним ухваленням звіту агентству eu-LISA обов'язково надається можливість ознайомитися з його змістом та надати свої коментарі;

обсяг наглядових повноважень: для ефективного виконання цієї функції EDPS має право у будь-який час отримувати від eu-LISA всю необхідну інформацію, мати безперешкодний доступ до всіх документів, системних логів (відповідно до статті 31 Регламенту) та до всіх приміщень агентства;

координований нагляд: цей аудит є частиною ширшої системи контролю, де EDPS і національні наглядові органи активно співпрацюють у межах своїх компетенцій для забезпечення законності функціонування великомасштабних IT-систем ЄС. Такий посилений механізм контролю гарантує, що обробка алфавітно-цифрових та біометричних даних засуджених осіб у центральній системі повністю відповідає європейським стандартам безпеки та захисту прав людини;

виняток для судової влади: органи нагляду не є компетентними щодо контролю за обробкою ПД судами, коли останні діють у межах своїх судових повноважень, щоб не зашкодити незалежності судової влади[54].

Відповідальність, санкції та засоби юридичного захисту. Система кримінальної юстиції вимагає наявності реальних механізмів реагування на порушення, особливо у випадках незаконного стеження чи зберігання біометричних даних[55].

Право на подання скарги: будь-який суб'єкт даних (у тому числі засуджений) має право подати скаргу до наглядового органу, якщо вважає обробку своїх ПД незаконною. Орган зобов'язаний повідомити про хід та результати розгляду протягом розумного строку[56].

Ефективний судовий захист:

- *проти володільця персональних даних/оператора:* право на позов до суду у разі порушення прав, гарантованих законодавством про захист даних[57];
- *проти наглядового органу:* право на судовий перегляд юридично зобов'язальних рішень органу нагляду або у разі нерозгляду скарги протягом встановленого строку[58].

Відповідальність та право на компенсацію: кожна особа, якій заподіяно матеріальну або нематеріальну шкоду (включаючи моральні страждання та

---

[54] Пояснювальна записка до Модернізованої Конвенції 108+. URL: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

[55] Посібник із судової практики ЄКПЛ: Права ув'язнених (2024). URL: https://ks.echr.coe.int/documents/d/echr-ks/guide_prisoners_rights_ukr

[56] Директива (ЄС) 2016/680 (Police Directive). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680

[57] Загальний регламент про захист даних (GDPR). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

[58] Модернізована Конвенція 108+. URL: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

стигматизацію через неправомірне розкриття даних про судимість), має право на отримання повної компенсації від володільца персональних даних або будь-якого іншого компетентного органу[59].

Санкції та штрафи: держави встановлюють правила щодо санкцій, які повинні бути *ефективними, пропорційними та стримувальними*. GDPR передбачає адміністративні штрафи до 20 000 000 євро за найсерйозніші порушення[60]. У правоохоронній сфері переважають дисциплінарна відповідальність посадових осіб та примусові заходи щодо зупинення незаконної обробки[61].

Висновки

Аналіз стандартів Ради Європи та Європейського Союзу свідчить, що захист персональних даних у сфері кримінальної юстиції еволюціонував від загальних декларацій до створення високотехнологічних систем транскордонного обміну із жорстким режимом підзвітності. Для України критично важливим є врахування таких фундаментальних аспектів європейського правопорядку.

1. Архітектура транскордонного співробітництва та системи ECRIS / ECRIS-TCN. Європейський простір правосуддя ґрунтується на обов'язку держав забезпечувати обмін інформацією про засудження особи через децентралізовану систему ECRIS (Рамкове рішення 2009/315/JHA) та централізовану систему ідентифікації громадян третіх країн ECRIS-TCN (Регламент (ЄС) 2019/816). Це вимагає від держави не лише технічного підключення, а й дотримання суворого принципу: держава винесення вироку є відповідальною за збереження актуальності й точності даних у масштабах усього Союзу. Будь-яке розходження між національним реєстром та європейською базою даних є порушенням права на приватність.

2. Спеціальний юридичний режим «чутливих» даних про судимість. Згідно зі статтею 6 Конвенції 108+, статтею 10 GDPR та статтею 10 Директиви (ЄС) 2016/680 дані про кримінальні правопорушення мають статус особливих категорій даних. Їх обробка дозволяється виключно за умови наявності суворих законодавчих гарантій і лише тоді, коли це абсолютно необхідно для виконання завдань кримінальної юстиції. Будь-який комплексний реєстр судимостей повинен вестися під повним контролем офіційного органу влади.

3. Принцип динамічної синхронізації та якості даних. Відповідно до Директиви (ЄС) 2019/884 та Регламенту (ЄС) 2019/816 держави зобов'язані впроваджувати механізми негайного виправлення або видалення даних у центральній системі у разі скасування вироку, амністії чи помилування на

---

[59] Директива (ЄС) 2016/680 (Police Directive). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680; Практичний посібник з використання персональних даних у поліцейському секторі. URL: https://rm.coe.int/practical-guide-on-the-use-of-personal-data-in-the-police-sector/1680792701

[60] Загальний регламент про захист даних (GDPR). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

[61] Директива (ЄС) 2016/680 (Police Directive). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680

національному рівні. Недопустимою є «довічна стигматизація» особи через застарілу інформацію в реєстрах, що прямо випливає з практики ЄСПЛ.

4. Посилена підзвітність через системне логування (Logging). Для систем обміну судимостями встановлено вищі стандарти прозорості операцій. Згідно зі статтею 31 Регламенту (ЄС) 2019/816 логи мають фіксувати не лише факт доступу, а й ідентифікатор службової особи, точний час, мету запиту та юридичне обґрунтування. Логи використовуються виключно для перевірки законності обробки та гарантування цілісності даних.

5. Пропорційність біометричної ідентифікації. Використання відбитків пальців та зображень обличчя в системі ECRIS-TCN обмежується суворою необхідністю для ідентифікації особи і не повинно перевищувати мету, визначену законом. Обробка біометрії засуджених має бути диференційованою за тяжкістю злочину, що відповідає вимогам індивідуалізованої оцінки ризиків ЄСПЛ.

Рекомендації для удосконалення законодавства України:

1) чітко відокремити загальний режим захисту ПД (за аналогією GDPR) від спеціального правоохоронного режиму (згідно з аналогічним врегулюванням у Директиві 2016/680);

2) створити наглядовий орган із повним фінансовим та операційним суверенітетом, наділений повноваженнями проводити незалежні аудити баз даних правоохоронців не рідше ніж раз на три роки (за аналогією з аудитами EDPS щодо ECRIS-TCN);

3) установити обов'язкову процедуру *оцінки впливу на захист даних* перед впровадженням будь-яких аналітичних систем чи технологій розпізнавання облич у поліцейській діяльності.

4) забезпечити особі право на письмове підтвердження виправлення чи видалення її даних у реєстрах та право на повну компенсацію шкоди у разі незаконної обробки.

Отже, побудова інформаційно-аналітичної системи обліку судимостей в Україні має базуватися на європейському стандарті «підзвітного управління даними», де легітимність кожного акту збирання інформації повинна бути доведена володільцем персональних даних на всіх етапах життєвого циклу даних.

Дослідницька служба
Верховної Ради України