УДК 342.721

[https://doi.org/10.52058/2708-7530-2021-11\(17\)-176-184](https://doi.org/10.52058/2708-7530-2021-11(17)-176-184)

Капля Олександр Миколайович доктор юридичних наук, старший науковий співробітник, професор кафедри правоохоронної та антикорупційної діяльності ПрАТ «ВНЗ «Міжрегіональна «Академія управління персоналом», м. Київ, Україна, e-mail: kaplia.oleksandr@gmail.com, <https://orcid.org/0000-0001-8629-0771>

Муравйов Кирило Володимирович доктор юридичних наук, доцент, завідувач кафедри адміністративного, фінансового та банківського права ПрАТ «ВНЗ «Міжрегіональна «Академія управління персоналом», м. Київ, Україна, e-mail: donkirill@ukr.net, <https://orcid.org/0000-0002-4422-4116>

МЕХАНІЗМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ

Анотація. Стаття висвітлює проблеми застосування адміністративно-правових механізмів захисту персональних даних. Проведено дослідження нормативних документів з метою проведення класифікації правових засобів дотримання захисту персональних даних. Визначено необхідність деталізації інформаційних ресурсів, які можуть бути віднесені до категорії персональних даних, а також встановлення чітких критеріїв порушення законодавства у цій сфері. Проведено аналіз наукових праць вітчизняних та зарубіжних вчених, які висвітлюють проблеми порушення захисту персональних даних.

Для цього досліджено дієві механізми адміністративно-правового регулювання в області захисту персональних даних, які діють за кордоном. Для їх імплементації у вітчизняну правову сферу необхідно сформулювати такі нормативно-правові механізми, які б дозволили збільшити адміністративну відповідальності органів публічної влади за неналежний захист персональних даних громадян.

Стаття характеризує особливості практичних заходів Європейського Союзу спрямованих на захист персональних даних. Так, на відміну від вітчизняних нормативних документів, правові норми Європейського Союзу чітко регламентують перелік порушень у сфері захисту персональних даних, що тягнуть за собою відповідальність як фізичних, так і юридичних осіб.

Показано, що в умовах цифровізації майже кожна дія в цифровому середовищі пов'язана із реєстраціями на різних цифрових платформах. Це значною мірою впливає на характер надання персональних даних, який полягає в тому, що при реєстрації користувача на будь-якому сайті від нього беруть згоду на обробку персональних даних. В таких умовах, переважну кількість користувачів не цікавить, яким чином будуть використані їх персональні дані. Це спричиняє проблему неможливості контролювати, хто, і

як буде використовуватимуть їх персональні дані. Крім того, досить часто текст згоди на обробку персональних даних є однотипним та має лише одну опцію, пов'язану із погодженням на обробку та використанням персональних даних, яка є необхідною умовою для подальшого користування відповідними цифровими платформами.

Все це, та багато інших не вирішених питань пов'язаних із недосконалістю законодавства у сфері захисту персональних даних висвітлюється в даній статті.

Ключові слова: механізми, персональні дані, захист, Конституційні норми, адміністративне право, Кодекс України про адміністративні правопорушення, громадяни, працівники.

Kaplya Oleksandr Mykolaiovych Doctor of Science of Law, Senior Researcher, Professor Department of Law Enforcement and Anti-Corruption Activities PJSC «Higher education institution «Interregional Academy of Personnel Management», Kyiv, Ukraine, e-mail: kaplia.oleksandr@gmail.com, <https://orcid.org/0000-0001-8629-0771>

Muraviov Kyrylo Volodymyrovych Doctor of Science of Law, Associate Professor, Head of the Department of Administrative, Financial and Banking Law PJSC «Higher education institution «Interregional Academy of Personnel Management», Kyiv, Ukraine, e-mail: donkirill@ukr.net, <https://orcid.org/0000-0002-4422-4116>

MECHANISMS OF PERSONAL DATA PROTECTION IN UKRAINE

Abstract. The article highlights the problems of application of administrative and legal mechanisms for personal data protection. A study of regulatory documents was conducted in order to classify the legal means of compliance with personal data protection. The need for detailing information resources that can be classified as personal data, as well as the establishment of clear criteria for violations of legislation in this area. The analysis of scientific works of domestic and foreign scientists, which cover the problems of personal data protection violations, is carried out.

To this end, effective mechanisms of administrative and legal regulation in the field of personal data protection operating abroad have been studied. For their implementation in the domestic legal sphere, it is necessary to form such regulatory mechanisms that would increase the administrative responsibility of public authorities for improper protection of personal data of citizens.

The article characterizes the features of practical measures of the European Union aimed at the protection of personal data. Thus, in contrast to domestic regulations, the legal norms of the European Union clearly regulate the list of violations in the field of personal data protection, which entail the responsibility of

both individuals and legal entities.

It has been shown that in the context of digitization, almost every action in the digital environment is associated with registrations on different digital platforms. This greatly affects the nature of the provision of personal data, which is that when registering a user on any site from him consent to the processing of personal data. In such circumstances, the vast majority of users are not interested in how their personal data will be used. This causes the problem of not being able to control who and how will use their personal data. In addition, quite often the text of the consent to the processing of personal data is the same and has only one option related to the consent to the processing and use of personal data, which is a necessary condition for further use of the relevant digital platforms.

All this, and many other unresolved issues related to the imperfection of legislation in the field of personal data protection is covered in this article.

Keywords: personal data, protection, Constitutional norms, administrative law, Code of Ukraine on Administrative Offenses, citizens, employees.

Постановка проблеми. Адміністративно-правові механізми, як інші юридичні норми в Україні, мають вирішувати питання захисту персональних даних в контексті попередження порушень, які посягають на право громадян використовувати інформацію про свою особистість. Разом з тим, застосування таких даних в умовах цифрового суспільства має ряд не вирішених питань, зокрема: використання персональних даних, обробка, передача, тощо. Тому, першим кроком для визначення правових аспектів застосування норм закону в області захисту персональних даних є встановлення інформації, яка може бути віднесена до такої категорії та встановлення відповідальності, яка передбачена законодавством за порушення закону у цій сфері.

Аналіз останніх досліджень та публікацій. Проблематикою дослідження захисту персональних даних займалися багато вітчизняних та зарубіжних вчених – фахівців у галузі економіки, фінансів, державного управління, менеджменту, права та ін.

Мета статті: визначити дієві механізми адміністративно-правового регулювання в області захисту персональних даних; на основі міжнародного досвіду проаналізувати норми вітчизняного законодавства на предмет відповідності нормам міжнародного права; провести класифікацію видів інформації, яка застосовується в соціальних мережах та у сфері трудових відносин за окремими категоріями, що мають чітке розмежування за критеріями захищеності.

Виклад основного матеріалу. Зважаючи на те, що захист персональних даних, це конституційна норма, яка передбачена ст. 32, що забороняє втручатися в особисте життя людини, за виключенням випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [1], питання захисту персональних непокоїть значну кількість людей в Україні. Так, у зв'язку з можливістю незаконного поширення

персональних даних та їх використання є досить велика кількість звернень до суду.

Окрім зазначеної норми Конституції в Україні існує ще ряд нормативно-правових положень, які стосуються питань захисту персональних даних. Зокрема, Закон України «Про захист персональних даних», ст. 188-39 КУпАП, ст. 17 Міжнародного Пакту про громадянські і політичні права, ст. 12 Загальної Декларації прав людини, ст. Конвенції про захист прав людини і основоположних свобод. Також, до таких слід віднести положення Конвенції Ради Європи про захист осіб у зв'язку автоматичною обробкою персональних даних. Окрему увагу слід приділити витягу з Кримінального кодексу України (стаття 182 «Порушення недоторканності приватного життя»), де практика її застосування досить низька. В першу чергу це пов'язано із тим, що багато нових нормативних документів не повною мірою узгоджені із сучасними інформаційні системи. Затвердження типового порядку обробки персональних даних Уповноваженим Верховної Ради України з прав людини «Про затвердження документів у сфері захисту персональних даних» від 08.01.2014 № 1/02-14, також не висвітлює усіх проблем, що пов'язані із захистом персональних даних [2].

Зважаючи на те, що у 2012 р. було прийнято закон «Про захист персональних даних» та Велика Палата Верховного Суду сформулировала принципи обробки персональних даних, в основу яких лягли: прозорість, адекватність, відкритість, відповідальність, рівень захищеності персональних даних дуже низький.

Підставами для обробки, як зазначено у Постанові Верховної Ради України від 26 червня 1992 року № 2503-XI є згода суб'єкта персональних даних. Для більш детальних характеристик правозастосування слід дослідити нормативні документи та законодавчі рішення по ним [3].

Так, проблеми захисту персональних даних регламентуються Законом України «Про захист персональних даних». Цей закон був прийнятий у 2011 р. Разом з його прийняттям, з метою реалізації завдань вказаних у його редакції, створено окремий спеціальний орган в системі державного управління, який дістав назву Державна служба України з питань захисту персональних даних. Але його функціонування було не тривалим. Його ліквідували протягом двох років після створення, в свою чергу основні задачі з проблем захисту персональних даних поклали на Уповноваженого Верховної Ради України з прав людини та суди. Після не тривалого часу при Секретаріаті Уповноваженого Верховної Ради України з прав людини було створено Департамент з питань захисту персональних даних. Відповідний підрозділ не міг повною мірою охопити проблему забезпечення захисту персональних даних, оскільки в умовах цифровізації, коли кожна дія в цифровому середовищі пов'язана із реєстраціями на різних цифрових платформах, умова використання яких, це надання персональних даних. Тому, сьогодні можна

спостерігати, що при реєстрації користувача на будь-якому сайті від нього беруть згоду на обробку персональних даних.

В таких умовах, переважну кількість користувачів не цікавить яким чином будуть використані його персональні дані. І основна проблема полягає в тому, що кількість різних сервісів дуже велика. Громадяни не можуть навіть запам'ятати, хто, і як буде використовувати їх персональні дані. У зв'язку з цим виникає багато проблем. Найбільш поширеною і них є те, що текст згоди, що представлена на таких сайтах, переважно, є однотипним. Він не передбачає внесення окремих змін і має лише одну опцію пов'язану із погодженням на обробку та використання персональних даних.

Судова практика попередження випадків пов'язаних із таким відтоком персональних даних знайшла своє відображення у практиці Великої Палати Верховного Суду. У справі №806/3265/17 Верховний Суд показав, що закон не врегульовує питання наслідків відмови від обробки персональних даних громадян [4]. А відтак, відсутність альтернативи, як прийнято в цифровому середовищі показує низьку якість законів та порушення конституційних прав осіб, які відмовляються надавати персональні дані. Це в свою чергу вказує на те, що держава, або інший обробник персональних даних, не повинні примушувати людину давати згоду на обробку персональних даних, за винятком питань що стосуються безпеки. Таким чином, відповідна обробка повинна реалізовуватись в межах правовідносини між державою та громадянами, які визначені в законах та інших нормативних документах. Отже, на відміну від безальтернативних технологій мають бути інші рішення, які базуються на традиційних методах ідентифікації особи.

Ще одним юридично не врегульованим аспектом можна вважати незнання особи, куди будуть передаватися її персональні дані і як їх використовуватимуть. Норма закону, яка представлена у ст. 8 закону «Про захист персональних даних», вказує на те, що особа має можливість отримати таку інформацію. Крім того, відповідна стаття регламентує навіть порядок подальшої відмови від використання персональних даних [5].

Проблема сьогодення полягає в тому, що кількість випадків надання персональних даних настільки висока, що суб'єкт персональних даних навіть не має можливості відстежувати випадки передачі своїх персональних даних третім особам. Тому можна констатувати, що не достатня увага з боку держави до захисту персональних даних її громадян має глобальний характер. Майже кожен українець отримував дзвінки від телефонних аферистів, які заволодівши персональними даними мільйонів громадян, зокрема номерами мобільних телефонів з чітко прив'язаними ідентифікаційними даними особи. Так, за 2021 р., в Україні лише у Харківській області від дій телефонних зловмисників сума збитків склала 500 000 грн. [6]. Тенденції в центральних регіонах значно гірші. В Україні вже сформувався ринок персональних даних [7]. Закон «Про захист персональних даних» не містить в собі класифікацію персональних даних, яка б дала можливість відокремлювати дані загальнодоступні від персональних (ті,

які можуть бути об'єктом уваги злочинців). Відповідна невизначеність навіть не дозволяє предметно розслідувати справи пов'язані із порушенням закону у сфері персональних даних. Так, наприклад норма ст. 182 ККУ передбачає покарання у вигляді позбавлення волі за порушення недоторканості приватного життя, але її слід оновити у зв'язку з тим, що таке приватне життя сьогодні є і в мережі, де кожен має сторінку в соц. мережах, тощо.

Таким чином, можна констатувати факт, що реалізація прав на захист персональних даних є неефективною.

Не так давно відбувся витік персональних даних водійських посвідчень в Україні, через що підозра впала на додаток «Дія» [8]. Причину витіку даних і досі не встановлено. Фактів порушення захищеності персональних даних сьогодні достань для того, щоб визнати це глобальною загрозою привабливості особистого життя і власних даних громадян не лише на вітчизняному рівні, а й на міжнародному. Варто лише згадати масштабний витік персональних даних із соціальної мережі Facebook [9].

Враховуючи масштаби даної проблематики слід звернути увагу на запобіжники таким негативним явищам. Одним із них можна вважати норму закону «Про захист персональних даних», яка передбачає відмову від дозволу на використання персональних. Проте законом не реалізовану цю процедуру через звернення. Для використання даної норми суб'єкт персональних даних має звернутися до суду, або до Уповноваженого ВР. Проте, завантаженість відповідних інституцій не завжди дозволяє вирішити такі питання.

У справі №127/13877/19 суд першої інстанції, задовольняючи вимоги позивачів щодо зобов'язання видалення Акціонерним товариством «Укрпошта» персональних даних, вказав, що ідентифікація особи під час надання їй послуг може здійснюватися за паспортними даними без необхідності використання засобів автоматизації. Незважаючи на те, що позивачі у цій справі не надавали згоду на обробку їхніх персональних даних та внесення до електронних баз даних, відповідач не довів, що він не здійснював такої обробки.

Міжнародний досвід вирішення таких питань спонукає держави на рішучі дії. Так, наприклад, у США, шт. Каліфорнія у 2020 р. прийнято новий закон «Про захист персональних даних». Саме на території цього штату розташовані компанії Apple, Facebook, Google, які безпосередньо працюють із персональними даними всього світу. Він дозволяє користувачам персональних даних дізнатися хто використовує їх дані. Крім того законом передбачена можливість видалення персональних даних за заявкою користувача [10]. Законом передбачено значну адміністративну та кримінальну відповідальність за неконання його норм.

Європейська юридична практика також відзначається посиленням механізмів захисту персональних даних. Так, Європейський Союз прийняв Загальний регламент захисту даних (GDPR) висуває жорсткі вимоги для їх

обробників [11]. Процес зберігання також має обмеження по строку, що необхідний для їх опрацювання. Усе це на фоні серйозної відповідальності збільшує стан захищеності персональних даних в Європейських країнах. Звернувшись до статистики застосування стягнень, то завдяки порушенням GDPR за 2 роки його функціонування сума штрафів склала приблизно 360 млн. євро [12].

Розглядаючи вітчизняну практику слід відзначити значно меншу кількість справ, що пов'язано не із відсутністю порушень, а у зв'язку із низькою правовою культурою громадян. Також це відбувається і через незахищеність на нормативно-правовому рівні. Тому існує значна потреба у розробці ефективних захисних механізмів, які дозволять захистити права та свободи власників особистих даних.

Проведене дослідження представників Європейського союзу та Ради Європи з нагоди Міжнародного дня захисту персональних даних дозволило висвітлити, що в законі містяться лише загальні вимоги. Це значною мірою ускладнює їх практичне застосування. А сам закон «Про захист персональних даних» ухвалений ще з 2010 р., застарів.

Так, держава має забезпечити ефективні механізми адміністративно-правового захисту обігу та обробки персональних даних, які будуть мати превентивний характер задля припинення порушень, які спрямовані на порушення права на володіння та розпорядження персональними даними.

Такі заходи мають в першу чергу спрямовуватись на внесення доповнень та змін до ряду нормативних документів, які дозволять збільшити адміністративну відповідальність органів публічної влади за неналежний захист персональних даних громадян.

Висновки. Зважаючи на те, що законодавець чітко сформулював термін «персональні дані» та визначив порядок їх використання, Конституційний Суд України, надаючи офіційне роз'яснення щодо правозастосування ст. 32 Конституції, надав конкретний перелік інформації стосовно класифікації персональних даних, реалізація законодавчих положень ускладнена застарілістю самих норм закону про «Про захист персональних даних», а також ряду інших нормативних документів.

Це спричинило хвилю порушень, запобігти яким можна лише вносячи зміни в законодавство, зобов'язавши органи виконавчої влади контролювати та нести відповідальність за порушення захисту даних громадян. Відповідна практика вже давно присутня в країнах Європейського Союзу, де регламентовано чіткий перелік порушень, що тягнуть за собою відповідальність як фізичних, так і юридичних осіб.

Література:

1. Ст.32 Конституції України, (Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141), [Електронний ресурс], Режим доступу: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>

2. Уповноважений Верховної Ради України з прав людини, Наказ 08.01.2014 № 1/02-14 Про затвердження документів у сфері захисту персональних даних, url: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text

3. Постанова Верховної Ради України Про затвердження положень про паспорт громадянина України та про паспорт громадянина України для виїзду за кордон {Назва Постанови в редакції Постанови ВР N 719-V (719-16) від 23.02.2007 Закону N 5294-VI (5294-17) від 18.09.2012 } (Відомості Верховної Ради України (ВВР), 1992, N 37, ст.545), url: <https://zakon.rada.gov.ua/laws/show/2503-12#Text>

4. Постанова Верховного Суду від 19 вересня 2018 року, Справа N 806/3265/17 (Пз/9901/2/18), м. Київ, [Електронний ресурс], Режим доступу: <https://verdictum.ligazakon.net/document/76822787>

5. Про захист персональних даних, Документ 2297-VI, чинний, поточна редакція — Редакція від 02.10.2021, підстава - 1723-IX, url: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

6. В Україні – «загострення» телефонного шахрайства. [Електронний ресурс] // Укр Інформ. – 2021. – Режим доступу до ресурсу: <https://www.ukrinform.ua/rubric-society/3219995-v-ukraini-zagostrenna-telefonogo-sahrajstva-vtim-ne-lise-v-ukraini.html>.

7. Скільки коштують персональні дані українців і чи легко їх купити? [Електронний ресурс] // Радіо Свобода. – 2021. – Режим доступу до ресурсу: <https://www.radiosvoboda.org/a/personalni-dani-na-prodazh/31074560.html>.

8. Злив персональних даних українців: що сталося і як захиститися [Електронний ресурс] // Радіо Свобода. – 2021. – Режим доступу до ресурсу: <https://www.radiosvoboda.org/a/zlyv-danyx-i-diya/30610626.html>.

9. Масштабний витік даних: Facebook не сповіщатиме постраждалих [Електронний ресурс] // Укр Інформ. – 2021. – Режим доступу до ресурсу: <https://www.ukrinform.ua/rubric-technology/3223520-masstabnij-vitik-danih-facebook-ne-spovisatime-postrazdalih-koristuvaciv.html>.

10. 2019 is the Year of ... CCPA? [Infographic]". The National Law Review. January 8, 2019. Retrieved 2019-01-30.

11. Frimin, Michael (29 March 2018). "Five benefits GDPR compliance will bring to your business". Forbes. Archived from the original on 12 September 2018. Retrieved 11 September 2018.

12. Самые крупные многомиллионные штрафы за нарушение GDPR в 2019 году [Електронний ресурс] // Panda Mediacenter. – 2019. – Режим доступу до ресурсу: <https://www.cloudav.ru/mediacenter/security/gdpr-fines-summary/>.

References:

1. St.32 Konstitucii Ukraïni [Article 32 of the Constitution of Ukraine]. (n.d.). zakon.rada.gov.ua. Retrieved from <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text> [in Ukrainian]

2. Nakaz “Pro zatverdzhennja dokumentiv u sferi zahistu personal'nih danih” [Order “On approval of documents in the field of personal data protection,”]. (n.d.). zakon.rada.gov.ua. Retrieved from https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text [in Ukrainian]

3. Postanova Verhovnoï Radi Ukraïni “Pro zatverdzhennja polozhen' pro pasport gromadjanina Ukraïni ta pro pasport gromadjanina Ukraïni dlja viïzdu za kordon” [Resolution of the Verkhovna Rada of Ukraine” On Approval of the Provisions on the Passport of a Citizen of Ukraine and on the Passport of a Citizen of Ukraine for Traveling Abroad”]. (n.d.). zakon.rada.gov.ua. Retrieved from <https://zakon.rada.gov.ua/laws/show/2503-12#Text> [in Ukrainian]

4. Postanova Verhovnogo Sudu Sprava N 806/3265/17 (Pz/9901/2/18) [Resolution of the Supreme Court Case No. 806/3265/17 (Pz / 9901/2/18).]. (n.d.). verdictum.ligazakon.net. Retrieved from <https://verdictum.ligazakon.net/document/76822787> [in Ukrainian]

5. Zakon Ukrainy «Pro zahist personal'nih danih» [The Law of Ukraine «On personal data protection»]. (n.d.). *zakon.rada.gov.ua*. Retrieved from <https://zakon.rada.gov.ua/laws/show/2297-17#Text> [in Ukrainian]
6. *V Ukraïni – «zagostrennja» telefonnogo shahrajstva*. [In Ukraine - "exacerbation" of telephone fraud]. URL: <https://www.ukrinform.ua/rubric-society/3219995-v-ukraini-zagostrenna-telefonnogo-sahrajstva-vtim-ne-lise-v-ukraini.html> [in Ukrainian]
7. *Skil'ki koshtujut' personal'ni dani ukraïnciv i chi legko ih kupiti?* [How much are personal data of Ukrainians and is it easy to buy them?]. URL: <https://www.radiosvoboda.org/a/personalni-dani-na-prodazh/31074560.html> [in Ukrainian]
8. *Zliv personal'nih danih ukraïnciv: shho stalosja i jak zahistitisja* [Drain of personal data of Ukrainians: what happened and how to protect yourself]. URL: <https://www.radiosvoboda.org/a/zlyv-danyx-i-diya/30610626.html> [in Ukrainian]
9. *Masshtabnij vitik danih: Facebook ne spovishhatime postrazhdalih* [Drain of personal data of Ukrainians: what happened and how to protect yourself]. URL: <https://www.ukrinform.ua/rubric-technology/3223520-mashtabnij-vitik-danih-facebook-ne-spovishatime-postrazhdalih-koristuvaciv.html> [in Ukrainian]
10. 2019 is the Year of ... CCPA? [Infographic]". The National Law Review. January 8, 2019. Retrieved 2019-01-30 [in English]
11. Frimin, Michael (29 March 2018). "Five benefits GDPR compliance will bring to your business". Forbes. Archived from the original on 12 September 2018. Retrieved 11 September 2018 [in English]
12. *Samye krupnye mnogomillionnye shtrafy za narushenie GDPR v 2019 godu* [The largest multimillion fines for violating the GDPR in 2019]. URL: <https://www.cloudav.ru/mediacenter/security/gdpr-fines-summary/> [in Ukrainian]