Закон № 4502-IX, який набрав чинності 16 січня 2026 року, став важливим етапом сучасного регулювання множинного громадянства. Він визначив це поняття та закріпив конкретні випадки, у яких наявність громадянства іншої держави визнається. Водночас такий підхід не означає необмеженого дозволу на множинне громадянство в усіх ситуаціях.

Сучасна політика України має поєднувати повагу до прав людини, підтримання зв'язку з українцями за кордоном і захист національної безпеки. Особливо важливо відрізняти добровільне набуття іноземного громадянства від ситуацій примусу на окупованих територіях. Подальший розвиток законодавства повинен забезпечувати правову визначеність, пропорційність обмежень, належний контроль та ефективний судовий захист.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Конституція України : Закон України від 28 червня 1996 року № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/ (дата звернення: 14.10.2026).
2. Про громадянство України : Закон України від 18 січня 2001 року № 2235-III. URL: https://zakon.rada.gov.ua/laws/show (дата звернення: 14.10.2026).
3. Про внесення змін до деяких законів України щодо забезпечення реалізації права на набуття та збереження громадянства України : Закон України від 18 червня 2025 року № 4502-IX. URL: https://zakon.rada.gov.ua/laws/show/4502-IX#Text (дата звернення: 14.10.2026).
4. Про громадянство України : Закон України від 8 жовтня 1991 року № 1636-XII. URL:https://zakon.rada.gov.ua/laws/show/1636-12/ed19911008.

Турдиєв А.Д., Сема Т.В., здобувачі
Науковий керівник: Ситніченко О.М.,
к.ю.н., доцент, доцент кафедри правового забезпечення безпеки бізнесу,
Державний торговельно-економічний університет

НОРМАТИВНО-ПРАВОВИЙ ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ В УМОВАХ ЦИФРОВІЗАЦІЇ

Коли ми купуємо щось в інтернеті або користуємося бонусною карткою магазину, то часто навіть не задумуємося, скільки інформації про себе залишаємо. Це може бути номер телефону, адреса доставки чи історія покупок. З одного боку, такі сервіси роблять наше життя зручнішим. З іншого – виникає питання: хто має доступ до цих даних і що буде, якщо вони потраплять до сторонніх осіб? У цій роботі ми хочемо розглянути, з якими ризиками стикається звичайний покупець, які права він має та коли за порушення цих прав може наставати кримінальна відповідальність.

Насамперед варто з'ясувати, які дані можуть опинитися під загрозою. Під час оформлення замовлення ми вказуємо ім'я, номер телефону, електронну адресу, а інколи й адресу проживання. Стаття 2 Закону України «Про захист персональних даних» визначає персональні дані як відомості про людину, за якими її можна ідентифікувати [1]. Тобто навіть звичайна інформація, яку ми залишаємо магазину та іншим інтернет платформ , за певних умов дозволяє встановити, хто саме зробив покупку. Це не означає, що магазин не має права її збирати, але для обробки даних потрібна законна підстава.

Далі важливо, як саме ці відомості зберігаються. Інформація про клієнтів є в базах магазинів, служб доставки та платіжних сервісів. Їй можуть загрожувати кібератаки, помилки в налаштуваннях захисту або неправомірні дії людей, які мають доступ до бази. Наприклад, уявімо повідомлення нібито від служби доставки, де правильно вказані ім'я покупця й номер його замовлення. Такому повідомленню легко повірити, хоча насправді його може надіслати шахрай. Це умовний приклад можливого ризику, а не опис конкретного доведеного кримінального правопорушення.

Отже, хто може використати наші дані не за призначенням? Це може бути сторонній зловмисник, який отримав незаконний доступ до системи, працівник компанії, що використав службову інформацію у власних цілях, або шахрай, який виманює дані обманом. Проте важливо не плутати звичайне збирання інформації з правопорушенням. Якщо покупець надає дані для доставки, а магазин обробляє їх на законних підставах і для визначеної мети, сам по собі такий процес не є незаконним [1].

Які ж права має покупець? Стаття 32 Конституції України захищає особисте й сімейне життя людини та встановлює правила поводження з конфіденційною інформацією про неї [2]. А стаття 8 Закону «Про захист персональних даних» дає право дізнатися, хто обробляє наші дані й навіщо, отримати доступ до них, вимагати виправлення недостовірної інформації або видалення даних, які обробляють незаконно, а також оскаржувати порушення [1]. Водночас обробка даних не завжди потребує саме згоди людини: підставою може бути, наприклад, виконання договору [1].

Припустімо, людина оформила картку постійного покупця, а пізніше почала отримувати повідомлення, не розуміючи, звідки магазин узяв її контакти та для чого використовує їх. У такому разі вона може звернутися до компанії й запитати про підстави обробки даних, попросити виправити помилки або припинити незаконне використання. Однак вимога видалити інформацію не завжди може бути виконана негайно, адже в окремих випадках закон зобов'язує зберігати певні відомості [1].

До кого звертатися, якщо права порушили? Спочатку можна направити звернення компанії, яка зберігає й обробляє дані. Контроль за дотриманням законодавства у цій сфері в межах своїх повноважень здійснює Уповноважений Верховної Ради України з прав людини. Крім того, свої права можна захищати в суді. Якщо ж є ознаки кримінального правопорушення, слід звертатися до правоохоронних органів [1; 3]. Тут потрібно пам'ятати: не кожне порушення правил обробки даних автоматично є кримінальним правопорушенням. Відповідальність залежить від того, що саме відбулося.

Кримінальний кодекс України передбачає відповідальність за окремі незаконні дії з персональною інформацією. Зокрема, стаття 182 стосується порушення недоторканності приватного життя, у тому числі визначених законом незаконних дій з конфіденційною інформацією про особу [3]. Якщо хтось без дозволу втручається в роботу інформаційної системи, може застосовуватися стаття 361 КК України. А стаття 361-2 може стосуватися незаконних дій з інформацією з обмеженим доступом, яка зберігається в комп'ютерних системах [3]. Тому, коли в новинах пишуть про «злам», треба з'ясувати, що саме зробили порушники, перш ніж називати конкретну статтю Кодексу.

Показовим є нещодавній випадок з мережею АТБ. 5 жовтня 2026 року Forbes Ukraine повідомив про кібератаку на сайт компанії. На сайті з'явилася вимога заплатити 400 тис. доларів, а автори повідомлення заявляли, що мають інформацію про 7,9 млн клієнтів [4]. Водночас представники АТБ підтвердили атаку, але заперечили витік персональних даних [4; 5]. Нам здається, цей приклад особливо важливий, тому що після гучної новини легко сприйняти заяву нападників як доведений факт, хоча це різні речі.

У випадку з АТБ потрібно розділяти три питання: чи була кібератака, чи справді хтось отримав доступ до персональних даних і чи були ці дані незаконно поширені. Одне не обов'язково означає інше. Навіть якщо витік інформації не підтвердився, незаконне втручання в роботу сайту за наявності передбачених законом ознак може становити окреме кримінальне правопорушення. Але й звинувачувати компанію в неналежному захисті даних тільки через повідомлення нападників було б неправильно. Для висновків потрібні докази й перевірка конкретних обставин.

Отже, захист персональних даних стосується кожного, хто користується інтернет-магазинами, доставкою чи іншими цифровими послугами. Українське законодавство дає людині право контролювати використання інформації про себе, звертатися зі скаргами та захищати свої права. В окремих випадках за незаконні дії з даними може наставати кримінальна відповідальність. На нашу думку, важливо не тільки карати винних після порушення, а й робити зрозумілими для покупців правила збирання і зберігання інформації. А історія з АТБ показує ще одну важливу річ: у правових питаннях треба відрізняти повідомлення про можливий витік від установленого факту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 13.10.2026).
2. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр (дата звернення: 13.10.2026).
3. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 13.10.2026).
4. Балашова Л., Мельник Т. «Мережу вони не поклали». Хакери зламали сайт АТБ і вимагали $400 000 викупу. Forbes Ukraine. 05.10.2026. URL: https://forbes.ua/innovations/merezu-voni-ne-poklali (дата звернення: 13.10.2026).
5. Сайт мережі АТБ зазнав хакерської атаки: що кажуть у компанії. УНІАН. 05.10.2026. URL: https://www.unian.ua/economics/other/atb-zaznalo-hakerskoji-ataki (дата звернення: 13.10.2026).

Тусаєва С.С., здобувач
Науковий керівник: угаєвська А.В.
к.ю.н., доцент, доцент кафедри публічного та міжнародного права
Київський національний економічний університет імені Вадима Гетьмана

СИСТЕМА КРИМІНАЛЬНИХ ПОКАРАНЬ В УКРАЇНІ ТА НІМЕЧЧИНІ: ПОРІВНЯЛЬНО-ПРАВОВИЙ АНАЛІЗ

Система кримінальних покарань є одним із основних інститутів кримінального права, оскільки від її побудови залежить можливість призначення справедливого, пропорційного та необхідного покарання за вчинення кримінального правопорушення. Реформування кримінального законодавства України є важливим напрямом європейської інтеграції, що зумовлює необхідність перегляду підходів до побудови та застосування системи кримінальних покарань відповідно до сучасних правових стандартів. У цьому контексті особливого значення набуває порівняння систем кримінальних покарань України та Німеччини з метою встановлення особливостей їх нормативно-правового закріплення.

Відповідно до статті 51 Кримінального кодексу України від 05.04.2001 р. №2341- III (далі КК України), система покарань передбачає 14 видів, але по факту, у пунктах 2 та 3 передбачається не один, а декілька видів покарань. Водночас застосування окремих із них на практиці порушує питання щодо їхньої фактичної суворості [1].

Питання місця штрафу в системі кримінальних покарань України залишається дискусійним. К. М. Оробець вказує, що фактична суворість цього покарання залежить від його розміру та можливості заміни іншим покаранням, що зумовлює необхідність перегляду його місця в системі або поділу на окремі види [2, с. 143-144].

Ю. А. Пономаренко підкреслив недоліки законодавчого регулювання випадків неможливості сплати штрафу, зокрема коли до засудженої особи не могли бути застосовані громадські або виправні роботи [3, с. 65]. Це свідчить про те, що під час визначення місця штрафу в системі покарань необхідно враховувати не лише його розмір, а й особливості виконання цього покарання.

У ч. 3 статті 212 КК України, що встановлює відповідальність за ухилення від сплати податків і зборів за наявності передбачених законом кваліфікуючих ознак, передбачено штраф у розмірі від п’ятнадцяти тисяч до двадцяти п’яти тисяч неоподатковуваних мінімумів доходів громадян, а також позбавлення права обіймати певні посади. При цьому позбавлення волі як вид покарання за цією статтею не передбачено. Варто зазначити, що відповідно до частини 4 статті 53 КК України допускається можливість розстрочки виплати штрафу до одного року. Проте загальний розмір санкції настільки великий, що навіть за наявності розстрочки не знімає